

Regelwerke & Standards im IT-Governance Umfeld

von Jörg Schlösser, Sascha Thies, Joachim Fremmer

Einleitung

IT-Governance ist die Organisation, Steuerung und Kontrolle der IT eines Unternehmens durch die Unternehmensführung zur konsequenten Ausrichtung der IT-Prozesse an der Unternehmensstrategie.

Diese Steuerung (engl. "Governance") durch die Unternehmensführung ist notwendig, da die Informationsfunktion in Unternehmen eine wichtige Rolle spielt und somit der reibungslose Ablauf und die konsequente Verbesserung der IT-Prozesse ein wesentlicher Erfolgsfaktor für Unternehmen darstellt. Ziel ist es, die IT-Geschäftsziele zu unterstützen, Investitionen in die IT zu optimieren und ein angemessenes IT-bezogenes Risiko- & Change Management zu betreiben. IT-Governance verfolgt im Wesentlichen 5 Ziele:

- Strategic Alignment: fortwährende Ausrichtung der IT an den Unternehmenszielen und -prozessen und Unterstützung des Unternehmen bei der Erreichung der Geschäftsziele
- Resource Management: verantwortungsvoller und nachhaltiger Einsatz der IT-Ressourcen (Mitarbeiter, Systeme, Finanzen)
- Risk Management: IT-Risiken erkennen, beurteilen und managen
- Performance Measurement: Messung der Performance der IT-Prozesse und Services
- Value Delivery: Bewertung des Wertbeitrags der IT

IT-Governance ist ein wesentlicher Bestandteil eines erfolgreichen Business IT-Alignment, dessen Umsetzung durch leistungsfähige und international akzeptierte Standards und Regelwerke (z.B. COSO, SAS 70, ISO 20000, COBIT, ITIL) unterstützt wird.

Im Folgenden werden die wesentlichen Regelwerke und Standards für erfolgreiche Managementsysteme dargestellt, welche u. a. von der ISO (International Organisation for Standardization) und der IEC (International Electrotechnical Commission), sowie dem BSI (British Standards Institute) und dem DIN (Deutsches Institut für Normung) herausgegeben werden.

Inhalte

In diesem Artikel finden Sie Beiträge zu folgenden Regelwerken und Standards:

- ITIL v2
- ITIL v3
- ISO/IEC 20000
- ISO/IEC 15504
- ISO/IEC 17799
- ISO/IEC 27001
- IT-GSHB
- RISK MGMT
- SOX
- COBIT 4

exagon consulting & solutions gmbh
Heinrich-Hertz strasse 13
50170 Kerpen

Tel. +49 2273 98330
Fax. +49 2273 983311

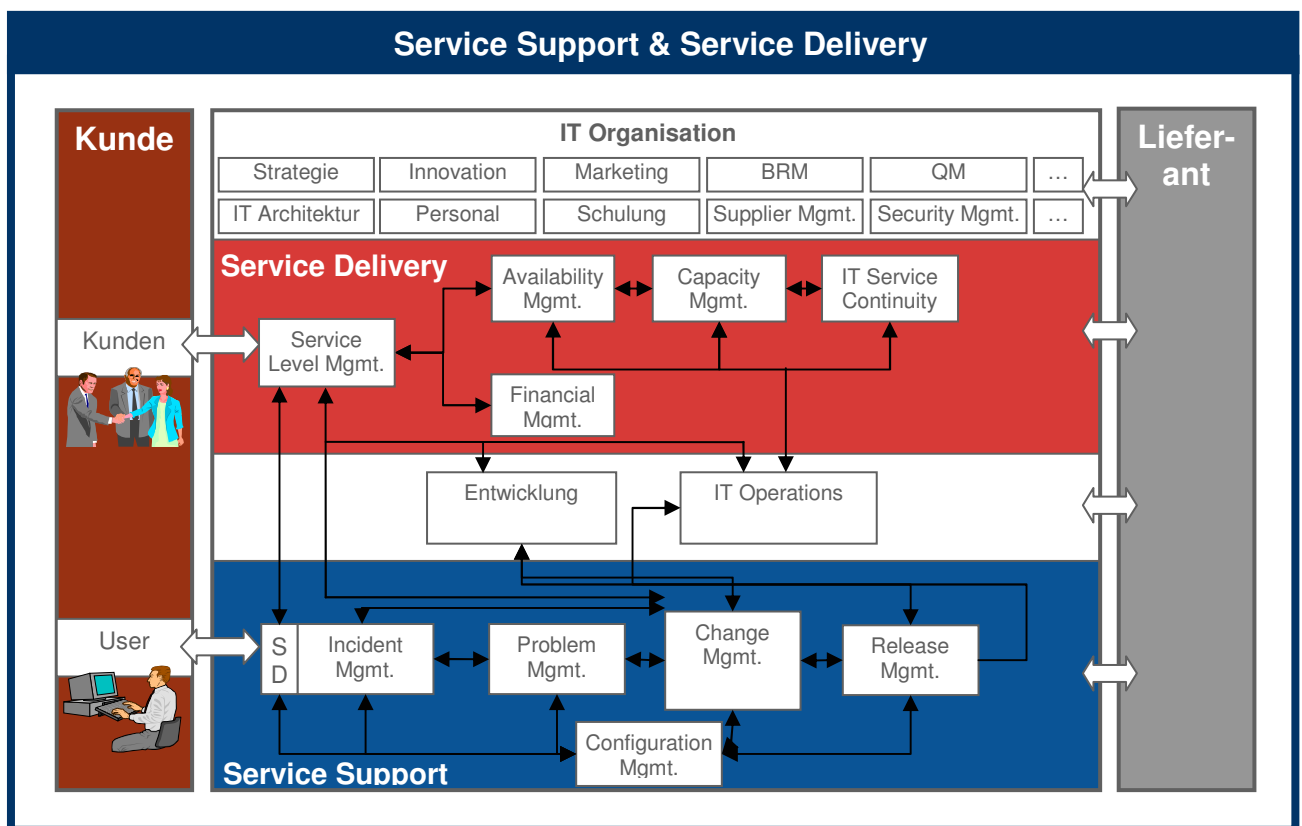
www.exagon.de

ITIL V2

Die IT Infrastructure Library (ITIL) ist ein Regelwerk, das die für den Betrieb und Steuerung einer IT-Infrastruktur notwendigen Prozesse beschreibt. Diese richten sich nach den durch die IT-Organisation erbrachten Services bzw. den Dienstleistungen.

ITIL wurde von der Central Computing and Telecommunications Agency (CCTA, jetzt OGC) entwickelt, einer Regierungsbehörde in Großbritannien, und ist in einer Reihe von Büchern definiert, die vom Office of Government Commerce (OGC), einer Stabstelle der Regierung von Großbritannien, seit 1989 herausgegeben werden.

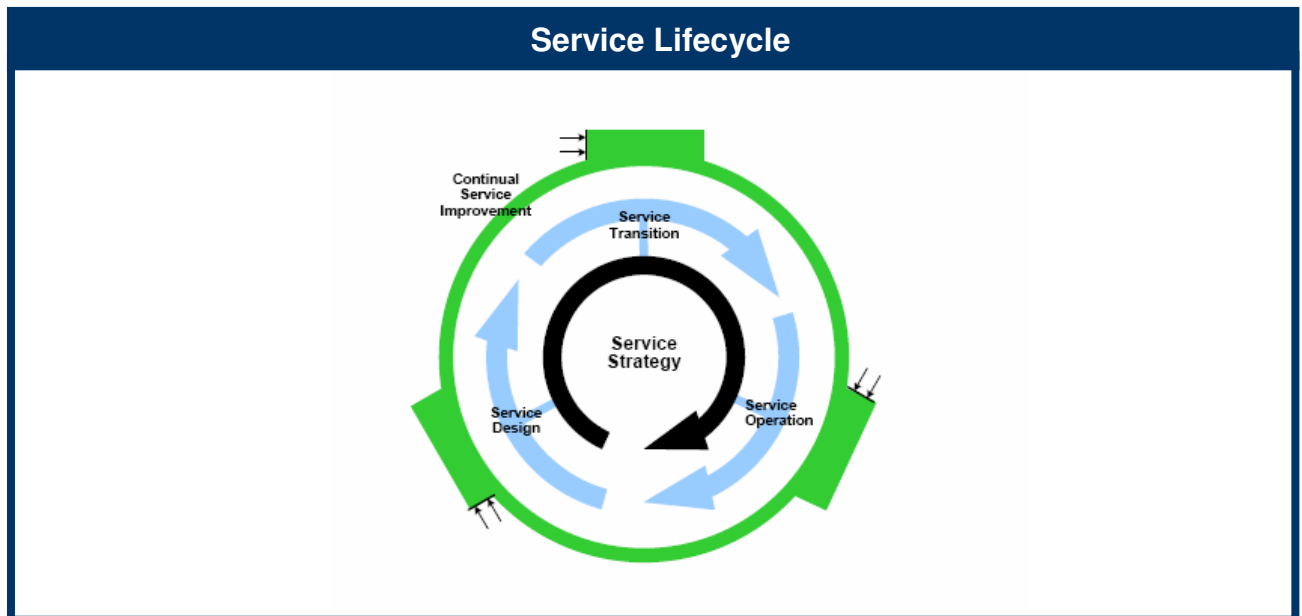
ITIL beschreibt einen Best-Practice Ansatz anhand von Modellen und Organisationsformen aus der Praxis. Diese Best-Practices kann jede Organisation beliebig adaptieren und auf ihre Bedürfnisse anpassen. ITIL beschreibt nicht, wie etwas getan werden muss, sondern, was getan werden sollte. Durch die so gebotene Flexibilität ergeben sich Ungenauigkeiten in der Beschreibung, so dass bei Umsetzung konkretisierende Sekundärliteratur oder zusätzliches Know-How hinzugezogen werden muss. Die Kernbereiche sind Service Support und Service Delivery:



ITIL soll nicht die Einführung einer IT-Infrastruktur organisieren, sondern vielmehr deren dauerhaften und ständig verbesserten Betrieb sicherstellen. Das zentrale Konzept ist der Service, der vom IT-Dienstleister in definierter Qualität erbracht wird. Dies wird auch interessant für Situationen, in denen der Betrieb dieser Infrastruktur beispielsweise ausgelagert werden soll (IT-Outsourcing) oder intern im Rahmen von Centeransätzen organisiert werden soll.

ITIL V3

ITIL in der Version 3 ist in der Überarbeitung im Sommer 2007 erschienen. In der neuen Version ist eine wesentliche Neuerung die Lifecycle Ausrichtung. Dies spiegelt sich auch in der neuen Strukturierung der 5 Abschnitte wieder:



Während in Version 2 die Ausrichtung der IT und des Business berücksichtigt wurden, betont Version 3 die Integration von Business und IT.

Dabei wird die Sichtweise in Unternehmens- oder IT-Prozessen durch eine Sichtweise in Dienstleistungen und Mehrwertidentifizierung und -umsetzung ergänzt.

Ein wichtiges Kriterium kann dabei sein, ob Unternehmen bestimmten gesetzlichen Auflagen unterliegen und diese in Audits überprüft werden. Insbesondere gilt dies beispielsweise für Unternehmen aus der Pharma-Branche, die von solchen Regulativen betroffen sind (z.B. Lebensmittel- und Arzneimittelgesetze, FDA (Food an Drug Association, Börsen und Banken). In diesem Kontext kann das ITIL Rahmenwerk helfen, nicht nur die vollständige IT-Leistungserbringung sicherzustellen, sondern auch die gesamte Unternehmenswertschöpfung zu unterstützen.

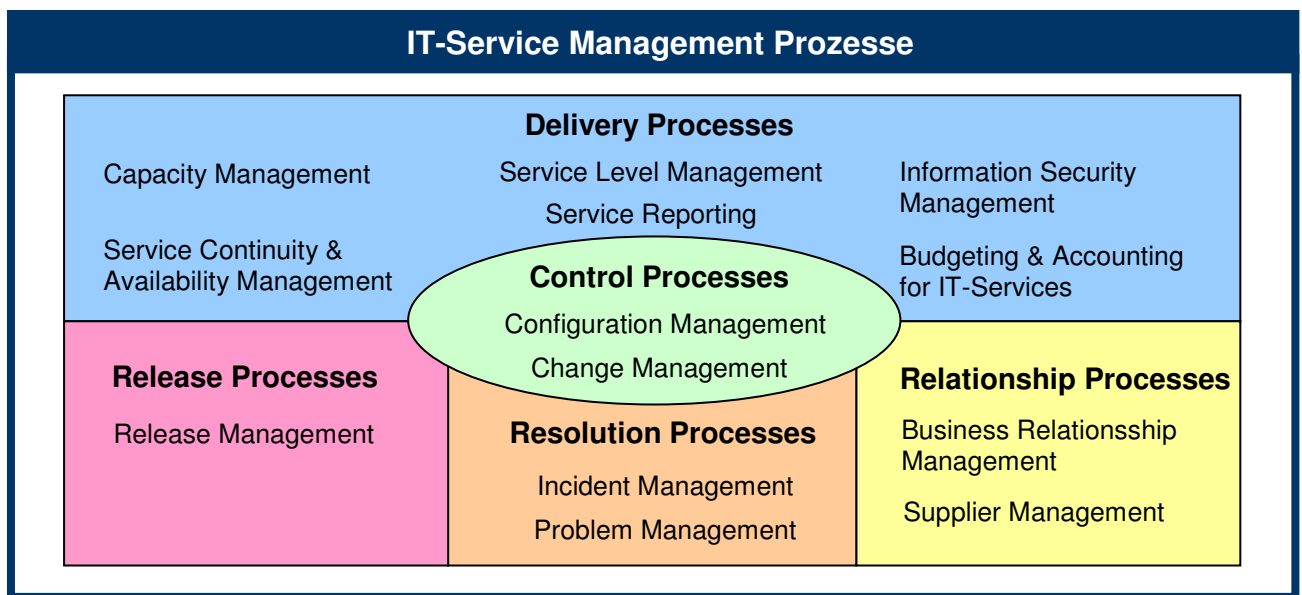
Insgesamt rückt bei der ITIL Version 3 der Service-Gedanke und die ganzheitliche Sicht auf das Unternehmen weiter in den Mittelpunkt. Bisher standen der IT-Betrieb und das Infrastruktur-Umfeld im Fokus von ITIL.

ISO/IEC 20000

Die ISO/IEC 20000 geht auf den alten British Standard BS 15000 zurück und dokumentiert als international anerkannter Standard zum IT-Service Management die Anforderungen für ein professionelles IT-Service Management.

Die ISO/IEC 20000 dient als messbarer Qualitätsstandard für das IT Service Management (ITSM). Dazu werden in der ISO/IEC 20000 die notwendigen Mindestanforderungen an Prozesse beschrieben, die eine Organisation etablieren muss, um IT-Services in definierter Qualität bereitstellen und managen zu können.

Die ISO/IEC 20000 ist ausgerichtet an den Prozessen, wie sie durch die IT Infrastructure Library beschrieben sind, und ergänzt diese komplementär.



Die ISO/IEC 20000 besteht aus folgenden Dokumenten:

ISO/IEC 20000 Part 1 – „Service Management: Specification“

Die ISO 20000-1 enthält die „Muss-Kriterien“ des Standards zu den Prozessgruppen Delivery, Control, Release, Resolution und Relationship. Es sind die Vorgaben dokumentiert, die eine Organisation einhalten, sicherstellen und nachweisen muss, um eine Zertifizierung zu erhalten.

ISO/IEC 20000 Part 2 – „Service Management: Code of Practice“

Innerhalb des zweiten Teils bietet die ISO/IEC 20000 Leitlinien und Empfehlungen für IT Service Management Prozesse („Kann-Kriterien“) und ergänzt die Anforderungen des ersten Teils um Erläuterungen der Best-Practices.

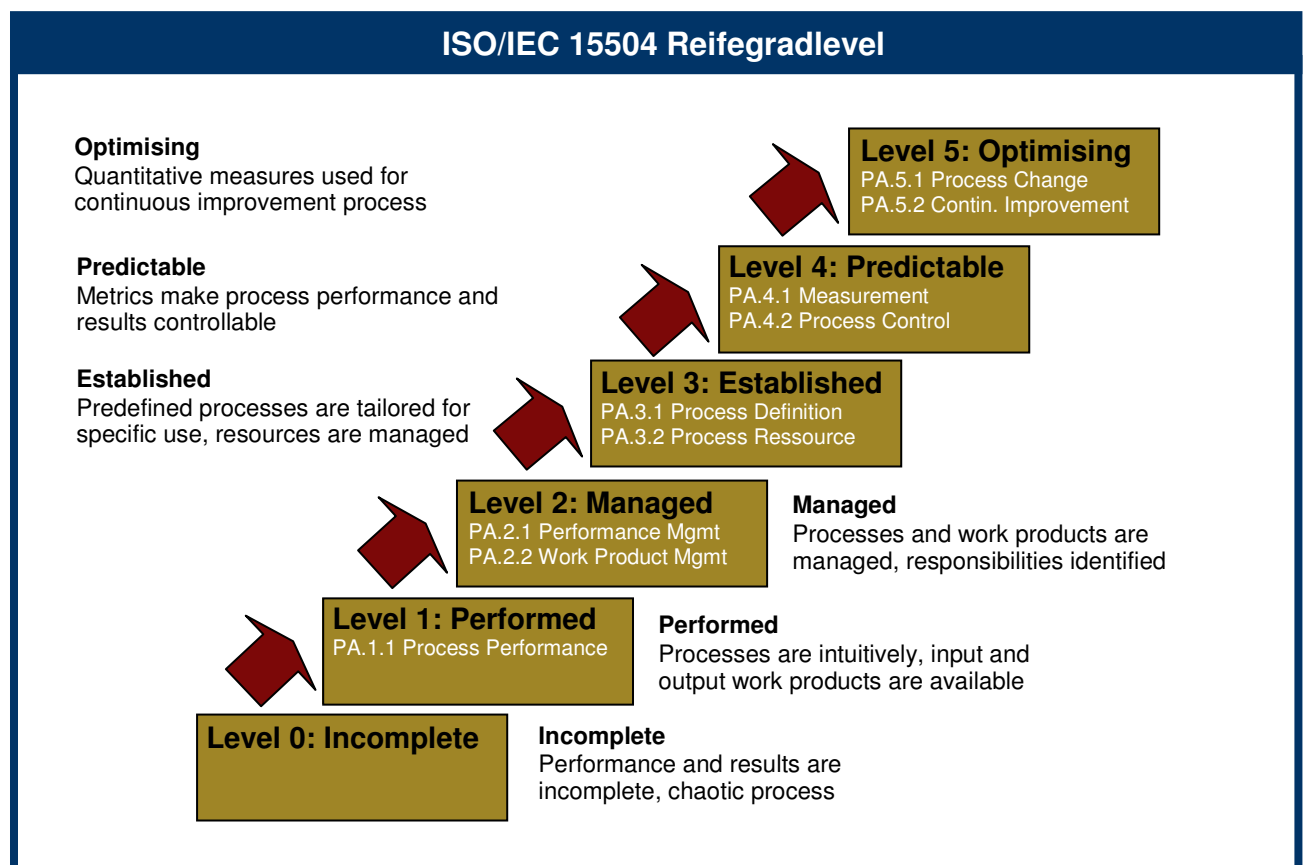
Die erfolgreiche Umsetzung der ISO/IEC 20000 kann zertifiziert werden. Damit besteht die Möglichkeit, die Implementierung eines IT Service Management anhand eines internationalen Standards objektiv zu messen (Anmerkung: eine ITIL Zertifizierung für eine IT-Organisation ist nicht möglich, da ITIL keine Norm ist). Die Zertifizierungsgrundlage ist Teil I, dessen Forderungen mit den Prozesskriterien aus ITIL in einem Self-Assessment Workbook PD0015 zusammengeführt wurden und das in Zertifizierungsverfahren angewendet wird.

ISO/IEC 15504

Die ISO/IEC 15504 wurde 1998 als Technischer Report verabschiedet und seit 2006 als Internationaler Standard veröffentlicht. Häufig wird SPICE (Software Process Improvement and Capability Determination) mit der ISO-Norm gleichgesetzt. Dies ist allerdings nicht korrekt, da das SPICE-Projekt eine konkrete Ausprägung der Norm für den Aspekt der Softwareentwicklung darstellt.

Die ISO/IEC 15504 stellt kein Vorgehensmodell dar, sondern bietet einen Rahmen für die Prozessbewertung. Die Verbesserung von Prozessen (Process Improvement) einerseits und die Bestimmung des Prozessreifegrads (Capability Determination) andererseits bilden die Kernpunkte dieses Modells. Der Internationale Standard formuliert Anforderungen an Prozessmodelle, so dass verschiedene Prozessmodelle zur Konstruktion eines Prozess Assessment Modells herangezogen werden können.

Die Prozess Assessments werden anhand des zweidimensionalen Referenz- und Assessment Modells durchgeführt. Die Prozess-Dimension auf der einen Seite dient zur Kennzeichnung der Vollständigkeit von Prozessen, die Reifegrad-Dimension auf der anderen Seite dient der Bestimmung ihrer Leistungsfähigkeit. Die jeweils relevanten Prozesse werden mit Hilfe der unternehmenseigenen Prozesslandkarte und des dazugehörigen Rahmenwerkes bestimmt. Den Reifegradstufen sind Prozessattribute (PA) zugeordnet, welche jeweils durch zugrunde liegende Managementaktivitäten beschrieben werden und der Beurteilung der Prozesse dienen. Es wird nicht nur die Existenz einer Prozessaktivität beurteilt, sondern auch die adäquate Durchführung der Aktivität bewertet. Für jeden Prozess kann unabhängig ein Reifegrad ermittelt werden. So kann die gewünschte Prozessverbesserung gezielt auf die neuralgischen Punkte gelenkt werden.



ISO/IEC 17799, ISO/IEC 27001, Grundschutzhandbuch

Die ISO/IEC 17799:2005 (Information technology -- Code of practice for information security management) ist ein internationaler Standard, der Kontrollmechanismen für die Informationssicherheit beinhaltet und inhaltlich auf dem British Standard Nr. 7799, Teil 1 (BS 7799-1:1999) aufbaut. Ausgangspunkt für die Standardisierung war eine Sammlung von Erfahrungen, Verfahren und Methoden aus der Praxis - ähnlich ITIL - um einen Best-Practice Ansatz zu erreichen.

Eine Zertifizierung nach ISO/IEC 17799 ist grundsätzlich nicht möglich, da es sich bei der Norm um eine Sammlung von Vorschlägen ("soll", im Englischen: "should") und nicht Forderungen ("muss", im Englischen: "shall") handelt. Soll ein Informationssicherheits-Managementsystem (ISMS) zertifiziert werden, ist dies nach ISO/IEC 27001 möglich.

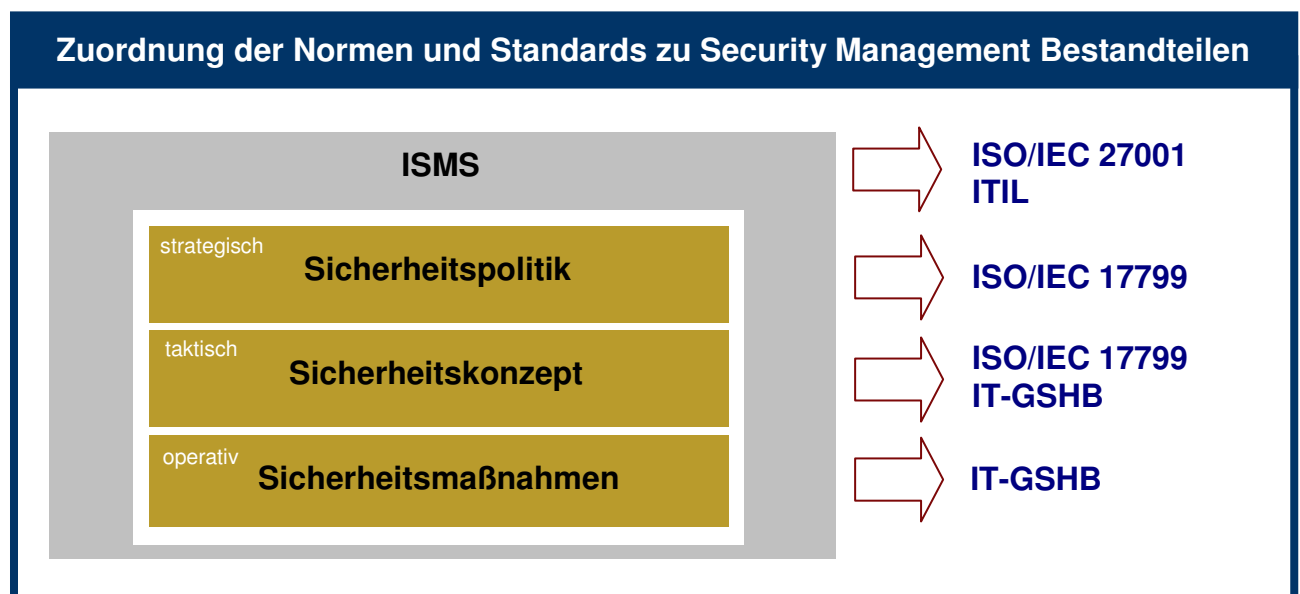
Die ISO/IEC 27001:2005 beschreibt die Anforderungen für die Implementierung von geeigneten Sicherheitsmechanismen (Herstellung, Einführung, Betrieb, Überwachung, Wartung, und Verbesserung). Der Zweck ist die Auswahl geeigneter Sicherheitsmechanismen, um den Schutz aller IT-Assets zu gewährleisten. Darüber hinaus wird ein Risikomanagementsystem gefordert, das neben der Identifikation zu schützender Unternehmenswerte und einer entsprechenden Risikobewertung die Ableitung von Maßnahmen zur nachhaltigen Risikominderung vorsieht.

Die Abgrenzung des IT-Grundschutzhandbuches (IT-GSHB) des BSI (Bundesamt für Sicherheit in der Informationstechnik) und eines Informationssicherheits-Managementsystems nach ISO/IEC 17799 lässt sich folgendermaßen darstellen:

ISO17799 berücksichtigt die gesamte Unternehmenssicherheit, das IT-GSHB die Sicherheit von einzelnen IT-Komponenten.

ISO 17799 basiert auf einer prozessorientierten Risikoanalyse, das IT GSHB auf einem stark technikzentrierten Ansatz.

Das IT-GSHB bildet also eine Grundlage als systematische Basis-Sicherheitsprüfung zur Risikoreduzierung bei IT-Komponenten. Die ISO/IEC 17799 geht hier wesentlich weiter.



Risikomanagement

Risikomanagement beschreibt den planvollen Umgang mit Risiken jeder Art (z. B. allgemeine unternehmerische Risiken, spezielle finanzielle Risiken). Auch technische Risiken können in einem Managementsystem behandelt werden (z. B. als Bestandteil des Arbeitsschutzes), wie z.B. Basel II technische Risiken, wie Risiken des Herstellungsprozesses und der Arbeitssicherheit aufgreift.

Die in den letzten Jahren entwickelten systemorientierten Regelwerke und Standards zum Risikomanagement, geben allgemein anwendbare Prinzipien zur Einrichtung und Anwendung von Risikomanagement-Standards vor. Derzeit existieren weltweit über 80 Frameworks und Normen zum Risikomanagement, wie z.B.:

- CAN/CSA Q850 Risk Management: Guideline for Decision-Makers (Kanada 1997)
- BS-6079-3:2000 Project management. Guide to the management of business related project risk (Großbritannien 2000)
- JIS Q 2001:2001 Guidelines for development and implementation of a risk management system (Japan 2001)
- COSO ERM Enterprise Risk Management - Integrated Framework (USA 2004)
- ONR 49000 ff. Risikomanagement für Organisationen und Systeme: Begriffe und Grundlagen (Österreich 2004)
- AS/NZS 4360:2004 Risk Management (Australien, Neuseeland 2004)

Risikomanagement umfasst dabei:

- Definition der Zielsetzung der Organisation
- Definition kritischer Erfolgsfaktoren hinsichtlich der Zielsetzung
- Definition der Risikomanagement-Strategie
- Identifikation von Risiken
- Bewertung/Messung von Risiken
- Definition und Priorisierung von Risiko mindernden Maßnahmen
- Steuerung der Umsetzung der definierten Maßnahmen
- Monitoring bzw. Früherkennung von Risiken.

Sarbanes Oxley

Der Sarbanes-Oxley Act of 2002 (SOX, SarbOx auch SOA – nicht zu verwechseln mit „Service Oriented Architecture“) ist ein US-Gesetz zur verbindlichen Regelung der Unternehmensberichterstattung infolge der Bilanzskandale von Unternehmen wie Enron oder Worldcom. Benannt wurde es nach seinen Verfassern, Paul S. Sarbanes (Demokrat) und Michael Oxley (Republikaner).

Die Zielsetzung war, das Vertrauen der Anleger in die Richtigkeit und Verlässlichkeit der veröffentlichten Finanzdaten von Unternehmen wiederherzustellen. Das Gesetz gilt für alle Unternehmen, deren Wertpapiere an US-Börsen (national securities exchanges) gelistet sind. Auch in den USA börsennotierte ausländische Unternehmen müssen das Gesetz beachten. Im Zusammenhang mit den erheblichen Hürden, die für einen Rückzug von US-amerikanischen Börsen (Delisting) zu überwinden sind, werden rückzugswilligen nicht-amerikanischen Unternehmen die Kosten der Erfüllung dieser Gesetzesvorschriften quasi aufgezwungen.

Das Gesetz gliedert sich in die Sektionen 302 und 404. Die für die IT relevante Sektion 404 beschäftigt sich mit der Beurteilung der Wirksamkeit des internen Kontrollsystems für die Rechnungslegung durch die Geschäftsleitung und den Wirtschaftsprüfer. Der Sarbanes-Oxley Act selber legt dieses Kontrollsystem nicht fest, sondern stützt sich auf einige der vorher genannten Rahmenwerke und Normen.

Auf internationaler Ebene wurden mögliche Konflikte des Sarbanes-Oxley Acts mit nationalen Vorschriften identifiziert. Beispielsweise die Individualhaftung von Vorstandsmitgliedern, die im deutschen Recht nicht verankert ist. Darüber hinaus verlangt der Sarbanes-Oxley Act z. T. von Rechtsanwälten Handlungen und Verhaltensweisen, die in Deutschland als Parteiverrat oder Bruch der Verschwiegenheitspflicht zu standes- oder gar strafrechtlichen Sanktionen führen können. Wie diese Konflikte gelöst werden können, ist größtenteils noch ungeklärt.

COBIT 4

CobiT (Control Objectives for Information and Related Technology) ist das international anerkannte Framework zur IT-Governance und gliedert die Aufgaben der IT in Prozesse und Control Objectives (Anmerkung: diese werden oft mit Kontrollziel übersetzt, eigentlich sind aber Steuerungsvorgaben passender). CobiT definiert hierbei nicht, wie die Anforderungen umzusetzen sind, sondern nur was umzusetzen ist.

CobiT wurde ursprünglich (1993) vom internationalen Verband der EDV-Prüfer (Information Systems Audit and Control Association, ISACA) entwickelt, seit 2000 obliegt dem IT Governance Institute, einer Schwesterorganisation der ISACA, CobiT zu entwickeln und fortzuschreiben.

Die in CobiT festgelegten Control Objectives sind in 34 Prozesse gegliedert. Ausgehend von Unternehmenszielen werden IT-Ziele festgelegt, die wiederum die Architektur der IT beeinflussen. Hierbei gewährleisten angemessen definierte und betriebene IT-Prozesse die Verarbeitung von Informationen, die Verwaltung von IT-Ressourcen (Personal, Technologie, Daten, Anwendungen) und die Erbringung von Services.

Zusätzlich zu den einzelnen Prozessen sind generische (für alle Prozesse gültige) Control Objectives und Control Objectives für Anwendungskontrollen (Eingabe-, Verarbeitungs-, Ausgabe- und Übertragungskontrollen) angegeben.

CobiT versteht sich als Rahmenwerk, welches zur Steuerung eingesetzt wird. Es sind weitere operative Rahmenwerke und Normen notwendig, die eine Leistungserbringung sicherstellen in dem von CobiT identifizierten Umfang.