goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

IT-Sicherheitsstandards

Die IT-Sicherheit nimmt einen immer wichtigeren Wert in einem Unternehmen ein. Dabei ist es wichtig, das Rad nicht neu zu erfinden, sondern auf bestehende Standards aufzubauen. Dieser INFONEWS bietet eine Übersicht über die IT-Sicherheitsstandards und beantwortet dabei folgende Fragen:

- Welche IT-Sicherheitsstandards gibt es?
- Welche Merkmale bieten diese?
- Wie können diese Standards angewendet werden?

Inhaltsverzeichnis

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1 Einleitung

Viele Firmen können heutzutage nicht mehr auf moderne Informations- und Kommunikationstechniken verzichten. Die Informationstechnologie dient als Basis für zahlreiche Geschäftsprozesse: Vom Einkauf über die Produktion bis zum Verkauf sowie die komplette Verwaltung. Der Zugriff von überall her ist dank Handys, PDAs und Notebooks möglich und auf eine funktionierende IT angewiesen.

Die Risiken gilt es auf ein möglichst geringes Niveau zu bringen, das wirtschaftlich vertretbar ist und dauerhaft aufrechterhalten werden kann. Daher ist für ein Unternehmen das IT-Risikomanagement notwendig. Standards spielen im Rahmen eines IT-Risikomanagements eine wichtige Rolle. Der Einsatz von solchen Sicherheitsstandards verbessert die sicherheitsrelevanten IT-Prozesse zum Vorteil des Unternehmers, seiner Kunden sowie seiner Mitarbeiter und reduziert damit das Gesamtrisiko.

1.1.1 Nutzen von Standards

Die Etablierung eines umfassenden IT-Sicherheitsmanagements ist eine anspruchsvolle Aufgabe, da Planungsfehler und impraktikable Umsetzung vermieden werden müssen. Selbst entwickelte Vorgehensweisen sind in der Regel teuer und entsprechen nicht ohne weiteres dem Stand der Technik. Daher ist es sinnvoll, auf bewährte Vorgehensweisen, die in Standards festgehalten sind, zurück zugreifen.

Wesentliche Ziele beim Einsatz von Standards sind:

Kostensenkung	Nutzung vorhandener und praxiserprobter Vorgehensmodelle Methodische Vereinheitlichung und Nachvollziehbarkeit Ressourceneinsparung durch Kontinuität und einheitliche Qualifikation Interoperabilität
Einführung eines angemessenen Sicherheitsniveau	Orientierung am Stand der Technik und Wissenschaft Gewährleistung der Aktualität Verbesserung des Sicherheitsniveaus durch die Notwendigkeit der zyklischen Bewertung
Wettbewerbsvorteile	Zertifizierung des Unternehmens sowie von Produkten Nachweisfähigkeit Verbesserung des Unternehmensimage Rechtssicherheit

1.2 Inhalt

Dieser INFONEWS stellt die wichtigsten Normen im Bereich der IT-Sicherheit vor. Es sind dies:

- CobiT
- ITIL
- ISO 27000
- BSI Grundschutzkataloge

Hinweis: detaillierte Informationen zu den Themen IKS und Basel II finden Sie in den folgenden INFONEWS:

- INFONEWS 2/05, Einfluss von Basel II auf die Informatik
- INFONEWS 3/08, Internes Kontroll-System IKS

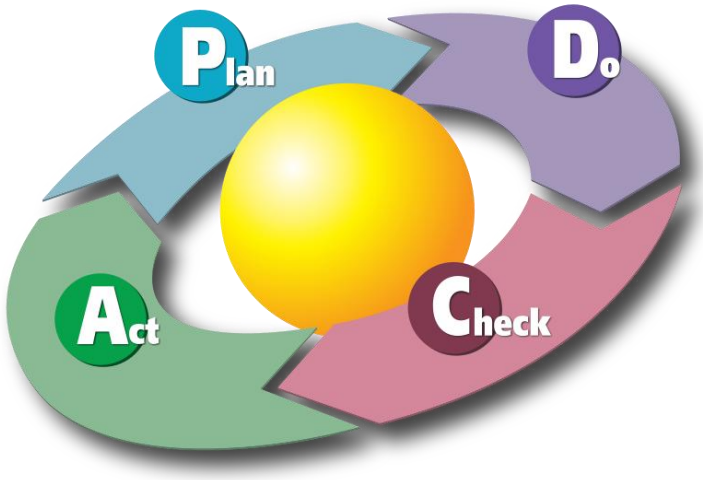
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

1.3 PDCA-Zyklus

Als Hilfsmittel zur stetigen Kontrolle und Erweiterung wird häufig der PDCA-Zyklus verwendet und gilt praktisch bei allen Standards als Referenz. Aus diesem Grund wird er hier kurz beschrieben (Ausschnitt aus Wikipedia).

Der PDCA-Zyklus beschreibt die Phasen im kontinuierlichen Verbesserungsprozess. Er ist die Grundlage aller Qualitätsmanagement-Systeme. Damit wird im Unternehmen eine stetige Verbesserung der Prozesse und Abläufe verfolgt mit dem Ziel, die Effizienz, Kunden- und Mitarbeiterzufriedenheit des Unternehmens zu verbessern.



© Karn G. Bulsuk

Der PDCA-Zyklus besteht aus vier Elementen:

- Plan
  Der jeweilige Prozess muss vor seiner eigentlichen Umsetzung geplant werden: Plan umfasst das Erkennen von Verbesserungspotentialen, die Analyse des aktuellen Zustands sowie das Entwickeln eines neuen Konzeptes.

- Do
  Do bedeutet das Ausprobieren beziehungsweise Testen und praktische Optimieren des Konzeptes mit schnell realisierbaren, einfachen Mitteln (z.B. provisorische Vorrichtungen) an einem einzelnen Arbeitsplatz.

- Check
  Der im Kleinen realisierte Prozessablauf und seine Resultate werden sorgfältig überprüft und bei Erfolg für die Umsetzung auf breiter Front als Standard freigegeben.

- Act
  In der Phase Act wird dieser neue Standard auf breiter Front eingeführt, festgeschrieben und regelmässig auf Einhaltung überprüft (Audits).

Die Verbesserung dieses Standards beginnt wiederum mit der Phase Plan.

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

2 CobiT

CobiT, IT Governance Institute, Control Objectives for Information and related Technology, wurde zur internen Kontrolle von verschiedenen Aspekten entwickelt. Mehrheitlich richtet es sich an Geschäftsführer, jedoch werden auch IT Elemente stark fokussiert. Wie bereits erwähnt, ist eine Firma ohne IT heute kaum mehr zu führen. Diesem Umstand wird Rechnung getragen.

Entwickelt wurde CobiT vom IT Governance Institute. Aktuell liegt die Version 4.1 vor. CobiT geht davon aus, dass die IT die Informationen liefern soll, die der Empfänger benötigt, um seine Ziele zu erreichen. Daher liegt ein Schwerpunkt in der Kontrolle von Prozessen und deren Eigner.

In der Regel wird die Geschäftsleitung nur über die Struktur, den Umfang und die Umsetzbarkeit der IT informiert. Wesentliche Themen wie Risikomanagement und IT-Governance kommen oft zu kurz. Daher liegt bei CobiT ein grosser Fokus bei der IT-Governance:

- Steigende IT-Kosten und deren Nutzung müssen so verwaltet werden, dass die Investitionen einen angemessenen Gewinn erzielen.
- Risiken, die in der digitalen Welt entstehen, müssen erkannt und gemanagt werden. Dies muss auch die Auswirkung berücksichtigen.
- Die IT ist so zu betreiben, dass die Kontinuität auch in einem Notfall sichergestellt ist (Business Continuity).
- Die IT-Mittel sind so zu benützen, dass die Informationen zu jedem Zeitpunkt vollständig und korrekt zur Verfügung stehen.
- Es muss sichergestellt sein, dass das IT-Wissen aufgebaut und verfügbar ist.
- Fehler und Problemstellen müssen erkannt und vermieden werden.

Das Hauptziel der IT-Governance ist es, die Anforderungen an die IT sowie die strategische Bedeutung der IT zu verstehen, um den optimalen Betrieb der Unternehmensziele sicherzustellen und Strategien für die zukünftige Erweiterung des Geschäftsbetriebes zu schaffen. IT-Governance ermöglicht, dass Erwartungen an die IT erfüllt und mögliche Risiken entschärft werden.

CobiT definiert dazu im Bereich der IT-Governance fünf Ziele:

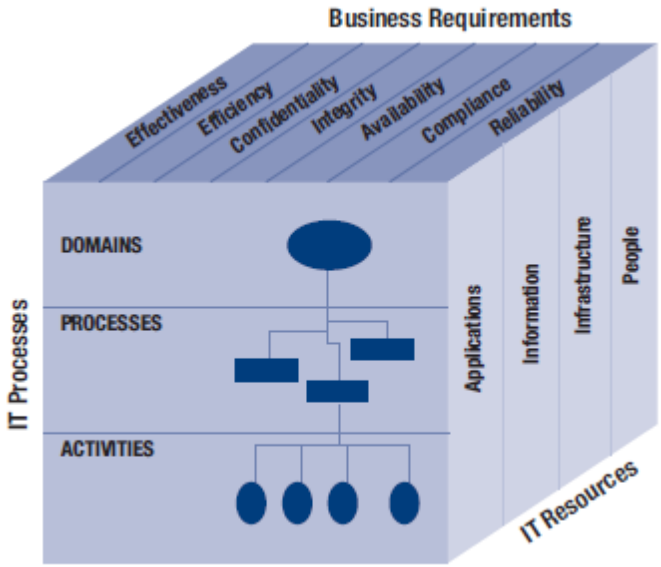
- Strategische Ausrichtung mit Fokus für Unternehmenslösungen (Strategic Alignment)
- Nutzengenerierung mit Fokus auf die Optimierung der Ausgaben und Bewertung des Nutzens der IT (Value Delivery)
- Risikomanagement, das sich auf den Schutz des IT Assets bezieht, unter Berücksichtigung von Disaster Recovery (Wiederaufbau nach Katastro-

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

phen) und Fortführung der Unternehmensprozesse im Krisenfall (Risk Management)
- Management von Ressourcen: Personen, aber auch Mittel (Resource Management)
- Optimierung von Wissen und Infrastruktur (Performance Measurement)

Weiter werden aber auch Aspekte der Compliance, der Sicherheit und der Qualität betrachtet. Dazu beinhaltet die Norm sieben Informationskriterien. Dabei beschreiben diese Kriterien die Kerngeschäfte jeder Firma: Effektivität, Effizienz, Verfügbarkeit, Integrität, Vertraulichkeit, Verlässlichkeit und die Compliance.



Die IT-Prozesse werden dazu in 4 Domänen mit 34 Prozessen aufgeteilt. Diesen Prozessen wurden so genannte High-Level Kontrollziele vorgegeben, die sich in Kontrollbereiche und Informationskriterien aufteilen.

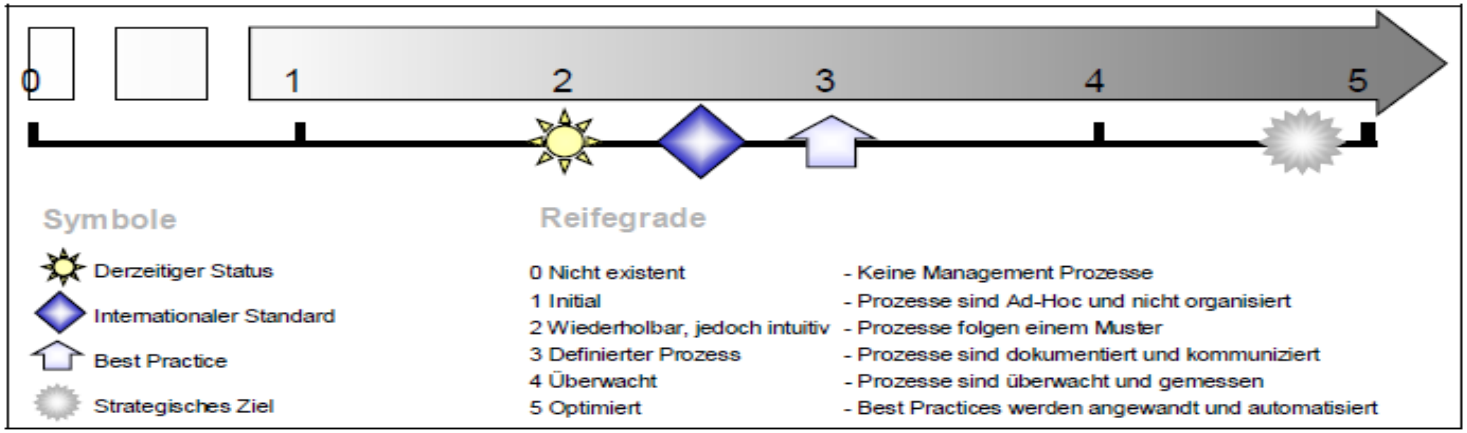
Die wesentlich umfangreicheren Elemente von CobiT stellen dem Management und IT Verantwortlichen die Best Practice in der Umsetzung eines Kontrollumfeldes in Form von mehr als 300 detaillierten Kontrollzielen zur Verfügung. Im Anhang von CobiT sind zudem umfangreiche Audit Richtlinien abgedruckt, die helfen, die eigene Infrastruktur schnell und umfassend zu beschreiben und zu überprüfen.

Da alles auf Prozesse ausgerichtet ist, wird auch ein entsprechendes Instrument zur Verfügung gestellt. Jeder Prozess wird in mehrere Schritte unterteilt: Prozessname, welche IT-Mittel werden benötigt, welche Ziele werden damit verfolgt und welche Aktivitäten beinhaltet dieser Prozess. Weiter gehören immer auch die Kontrollpunkte mit dazu. Jeder Prozess wird dabei in den vorgestellten Würfel abgebildet: die Verknüpfung zwischen Business Anforderungen, IT-Prozessen und den Ressourcen wird damit sicher gestellt.

Damit die Resultate aus den Kontrollen verglichen werden können, wird eine Skala von 0 bis 5 verwendet. So ist für das Management schnell ersichtlich, wo sich ein Prozess befindet, ob Massnahmen getroffen werden müssen oder ob Änderungen zu planen sind:

CobiT ist ein mächtiges „Tool“ zur Unterstützung interner Ressourcen. Da es sich immer um vorhandene Prozesse dreht, ist es auch sehr praxisnah. Die Kontrollziele helfen, den Prozess jederzeit zu überprüfen und genügend schnell auf Veränderungen reagieren zu können.

Weiterführende Informationen:
http://www.isaca.org/cobit/



3 ITIL - IT Infrastructure Library

Beim Infrastructure Library, kurz ITIL handelt es sich um eine Sammlung von Good Practices, die in einer Reihe von Publikationen eine mögliche Umsetzung eines IT-Service Managements (ITSM) beschreibt und inzwischen als Defacto-Standard für Gestaltung, Implementierung sowie Management wesentlicher Steuerungsprozesse in der IT gilt.

ITIL wurde von der Central Computing and Telecommunications Agency (CCTA), heute Office of Gouvernement Commerce (OGC), einer Regierungsbehörde in Grossbritannien, seit 1989 entwickelt. Als Version 1 wurden zwischen 1992 und 1998 insgesamt 34 verschiedene Dokumente veröffentlicht. 2001 wurde die Publikationen der Version 2 herausgegeben und am 1. Juni 2007 folgte die aktualisierte Version 3. Die Inhalte der ITIL V3 beschreiben in mehreren Büchern die verschiedenen Themenbereiche des Lebenszyklus von Serviceleistungen.

Das Ziel von ITIL besteht im Wesentlichen darin, die bislang technologiezentrierte IT-Organisation prozess-, service- und kundenorientiert auszurichten. Damit sind die ITIL-Empfehlungen eine entscheidende Grundlage für zuverlässige, sichere und wirtschaftliche IT-Services aus Sicht eines IT-Dienstleisters.

Das gesammelte ITIL-Wissen ist öffentlich uneingeschränkt zugänglich. Es ist in einer Bibliothek von circa 40 englischsprachigen Publikationen verfügbar:

- IT Service Provision and IT Infrastructure Management Sets
- Manager's Set (inkl. ITIL Security Management)
- Software Support Set
- Computer Operations Set
- Environmental Set
- Business Perspective Set

Die Sicherheitsanforderungen für die IT-Services werden auf Grundlage der Geschäftsprozesse bzw. –anforde-

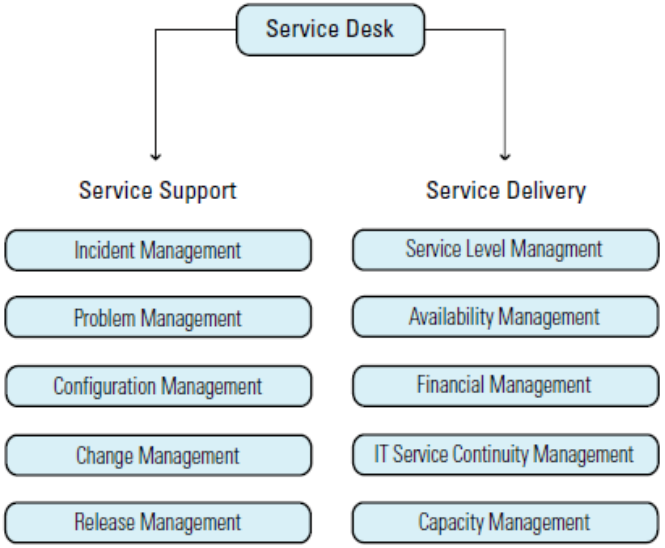
GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

rungen definiert. Folgende Prozesse stehen dabei im Vordergrund:



Mit dem IT-Dienstleister werden die Anforderungen in Service Level Agreement (SLA) aufgenommen, abgestimmt, umgesetzt, evaluiert und dokumentiert. ITIL hat selber aber keine eigenen IT-Sicherheitsmassnahmen definiert. Dafür müssen andere Standards, wie zum Beispiel ISO 27001 herangezogen werden.

3.1 Incident / Problem Management

In vielen Betrieben, vor allem auch in kleineren Firmen, wird nicht das gesamte Framework umgesetzt, sondern nur Teile davon. Die zwei wichtigsten sind dabei sicherlich das Incident und das Problem Management. Aus diesem Grund wird hier kurz auf diese beiden Prozesse eingegangen.

Das **Incident Management** umfasst die gesamtheitliche Verwaltung aller Störungen. Als erstes wird beim Auftreten einer Störung eine Klassifizierung vorgenommen. Aus der Klassifizierung sollte ersichtlich sein, welche Sicherheitsziele verfolgt werden. Als Faktoren werden die Schadensauswirkung und die Dringlichkeit, also die zugeordnete Priorität, berücksichtigt. Die Analyse der Störung beginnt mit der Prüfung, ob es sich um eine bereits bekannte Störung handelt. Hier helfen zum Beispiel Trouble Ticket Systeme weiter. Falls es sich um ein bekanntes Problem handelt, wird ein zuvor definierter Lösungsweg eingeschlagen. Ist kein Weg bekannt und auch keine schnelle Lösung ersichtlich, wird die Störung zum Support-Team eskaliert (in der Regel First Level Support genannt). Das Incident Management gibt zwar die Störung weiter, muss jedoch den Fall bis zur Erledigung weiterverfolgen. Nicht immer kann das Problem auch durch den First Level Support gelöst werden, sondern muss an weitere Stellen weitergeleitet werden. So können auch Programmänderungen notwendig sein, was Zeit benötigt. Wichtig ist, dass die Nachvollziehbarkeit der Störung sowie der aktuelle Status gewährleistet sind. Daher muss die Störung mit folgenden Punkten dokumentiert werden:

- Eindeutige Störungsnummer
- Wann ist die Störung aufgetreten?
- Wo ist die Störung aufgetreten?
- Wer hat die Störung gemeldet?
- Eine Störungsbezeichnung (Schlagwort)
- Genaue Beschreibung der Störung
- Entstandener Schaden (dies darf auch geschätzt werden)
- Priorität
- Lösung

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

Das **Problem Management** beginnt dort, wo das Incident Management aufhört. Durch das Incident Management werden die Gründe für eine Störung nicht analysiert. Die Aufgabe des Problem Managements ist es nun, die Ursache(n) für die bereits aufgetretene Störung zu untersuchen und proaktiv Massnahmen zu treffen, damit diese Art von Störung nicht mehr auftreten kann. Häufig löst dies einen Änderungsantrag an das Change Management aus (ein sogenannter Request for Change) aus.

Somit kann gesagt werden, dass beim Incident Management die Schnelligkeit der Lösung wichtig ist, während das Problem Management eine nachhaltige Identifizierung und Ausschaltung der Ursache darstellt.

3.2 Informationssicherheit als zyklischer Prozess

Eingangs wurde bereits auf den PDCA-Zyklus hingewiesen. Dieses Ziel wird natürlich auch mit ITIL verfolgt. ITIL gliedert dabei die Informationssicherheit in die vier Bereiche: Richtlinien (Gesamtziele einer Organisation), Prozesse (Wie erreicht sie diese Ziele), Vorgehensweise (Wer macht was und wann, um die Ziele zu erreichen) sowie Arbeitsanweisungen für konkrete Aktionen. Dieser Prozess läuft idealtypisch in sieben Schritten ab:

1. Über eine Analyse der Risiken (beispielsweise Softwarefehler, Betriebsfehler, Kommunikation unterbrochen, Wahrscheinlichkeit des Auftretens, potenzieller Einfluss auf das Business, vergangene Erfahrungen) identifizieren die IT-Kunden ihre Sicherheitsanforderungen.

2. Die IT-Abteilung prüft die Machbarkeit dieser Anforderungen und vergleicht sie mit den in der Organisation festgesetzten Minimalrichtlinien für Informationssicherheit.

3. Der Kunde und die IT-Abteilung verhandeln und erarbeiten ein Service Level Agreement (SLA), das die Anforderungen an Informationssicherheit in messbaren Grössen definiert und genau festlegt, wie diese überprüfbar erreicht werden sollen.

4. Die IT-Organisation definiert Operational Level Agreements (OLA), die detailliert beschreiben, wie sie die Services für Informationssicherheit bereitstellt.

5. Die SLA und OLAs werden implementiert und überwacht.

6. Die Kunden erhalten regelmässig Berichte über die Effektivität und den aktuellen Status der Services, welche die Informationssicherheit garantieren sollen.

7. Die SLAs und OLAs werden überarbeitet, falls es notwendig sein sollte.

3.3 Fazit

ITIL ermöglicht es Firmen die vorhandenen IT-Prozesse auf Grundlage von Best Practices strukturiert zu entwickeln und zu implementieren. Da ITIL Rollen und Verantwortlichkeiten für die verschiedenen involvierten Stellen klar definiert, steht auch während eines Zwischenfalls sofort fest, wer zuständig ist. Die Unterteilung zwischen Incident und Problem Management garantiert zudem, dass eine Störung schnell behoben und anschliessend

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

auch analysiert wird. Eine „Pflästerli"-Politik wird damit klar verhindert.

ITIL etabliert dokumentierte Standards und Prozesse, die sich überwachen lassen, und fordert regelmässig Berichte über den aktuellen Stand. Daher ist die Firmenleitung jederzeit über die Effizienz der Prozesse informiert und kann auf Grund fundierter Tatsachen ihre Entscheidungen treffen. Da ITIL, wie auch die anderen ISMS Richtlinien, eine ständige Überprüfung erfordert, sorgt es dafür, dass getroffene Massnahmen hinterfragt, verändert bzw. verbessert oder neue Massnahmen dazu kommen, und sich somit veränderte Anforderungen oder Bedrohungen schnell integrieren lassen.

Weiterführende Informationen:
http://www.itil-officialsite.com

4 ISO 27000

Aufgrund der Komplexität von Informationstechnik und der Nachfrage nach einer Zertifizierung sind in den letzten Jahren zahlreiche Anleitungen, Standards und nationale Normen zur IT-Sicherheit entstanden. Die internationale Norm ISO/IEC 27001:2005, "Information technology - Security techniques - Information security management systems - Requirements" ist der erste internationale Standard zum IT-Sicherheitsmanagement, der auch eine Zertifizierung ermöglicht. Diese spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung, und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der Risiken innerhalb der gesamten Organisation. Hierbei werden sämtliche Arten von Organisationen berücksichtigt.

Die gesamte ISO 2700x Reihe besteht aus verschiedenen Standards, die sich ergänzen:

Standard	**Inhalt**
ISO 27000	Begriffsdefinitionen zum ISMS
ISO 27001	Definition der Zertifizierungsanforderungen an ein ISMS *(Löst BS 7799-2 ab)*
ISO 27002	Leitfaden zur Implementierung, Kontrollfragen *(Löst ISO 17799 bzw. BS 7799-1 ab)*
ISO 27003	Einführungshilfe für ein ISMS *(in Arbeit)*
ISO 27004	Definition von Kennzahlensystemen für ein ISMS
ISO 27005	Risikomanagement *(Löst BS 7799-3 ab)*
ISO 27006	Kriterien für Institutionen die das Audit und die Zertifizierung durchführen
ISO 27007	Richtlinien für das Audit *(in Arbeit)*

Nach ISO 27001 soll ein Informationssicherheits-Managementsystem (ISMS) aufgebaut werden, welches die Grundlage zur Identifikation und Beherrschung der Informationssicherheitsrisiken sowie zur Sicherstellung der Zuverlässigkeit von Systemen bietet.

Mögliche Ereignisse, die auf eine Organisation einwirken können sind z.B. gezielte Angriffe von Personen auf technische oder organisatorische Schwachstellen; Elementarereignisse wie Erdbeben, Feuer, Wassereinbruch, Blitzschlag; Fahrlässige Handlungen oder Fehlbedienung von Systemen; Verstösse gegen Gesetze oder Verträge; sowie potentielle Schädigung von Personen (Ansehen, Gesundheit, Leben).

Die Konsequenzen können je nach Ereignis unmittelbaren monetären Schaden verursachen, aber auch Imageverlust, Verlust der Kreditwürdigkeit oder Entzug von Genehmigungen mit sich bringen.

Der ISO Standard verlangt für jeden erkannten Informationswert die Risiken bezüglich der Verfügbarkeit, Vertraulichkeit und Integrität und ggf. weiterer Ziele zu identifizieren und abzuschätzen. Dabei gehen die Bedrohungen, Schwachstellen sowie die Einschätzung von Ausmass und Häufigkeit der Schäden ein.

Eine grosse Herausforderung stellt die Dokumentation dar. Ständig kommen neue Informationen dazu, die Prozesse ändern und Risiken verlagern sich. Es ist wichtig, dass das Management ständig einen Überblick über den Stand der Arbeiten hat und entsprechende (Korrektur-) Massnahmen einleiten kann.

4.1 Zertifizierung

Bei der Zertifizierung nach ISO 27001 versuchen sich die Auditoren in die Lage des Unternehmens zu versetzen und selber die Risikostellen zu identifizieren. Anschliessend werden diese mit denjenigen des Unternehmens verglichen. Sind alle vorhanden? Sind weitere erkannt worden? Werden entsprechende Massnahmen abgeleitet? Erst danach werden die entsprechenden Massnahmen genauer angeschaut. Dabei geht es weniger um die technischen Details, sondern um die korrekte Erkennung und das Einleiten von Massnahmen. Diese Schritte müssen zwingend dokumentiert werden. Protokolle der Managementsitzungen und internen Audits bilden einen weiteren Kontrollpunkt der Auditoren. Sind auch hier Risiken und passende Massnahmen enthalten sowie Umsetzungen durchgeführt? Falls dies regelmässig und vollständig stattfindet, steht einer erfolgreichen Zertifizierung nach ISO 27001 nichts mehr im Wege.

Die obenstehenden Erklärungen stammen aus dem INFONEWS 1/09, Security Management nach ISO 27001.

Weiterführende Informationen:
http://www.27000.org/

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

5 BSI IT-Grundschutz

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet seit 1994 das IT-Grundschutzhandbuch (GSHB) an, welches detailliert IT-Sicherheitsmassnahmen aus verschiedenen Bereichen (Technik, Organisation, Infrastruktur und Personal) sowie Anforderungen an das IT-Sicherheitsmanagement beschreibt. Damit auch der internationale Standard für Informationssicherheits-Managementsysteme abdeckt werden kann, wurde das Vorgehen nach IT-Grundschutz im Jahr 2006 an die ISO/IEC 27001 angepasst. Die empfohlene Vorgehensweise bei der Umsetzung von IT-Grundschutz wird nun in so genannten BSI-Standards beschrieben, wobei Bausteine, Gefährdungen und Sicherheitsmassnahmen aus dem IT-Grundschutzhandbuch weiterhin in den IT-Grundschutz-Katalogen verfügbar sind:

- BSI-Standard 100-1: Managementsysteme für Informationssicherheit
- BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise
- BSI-Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz
- BSI-Standard 100-4: Notfallmanagement
- IT-Grundschutz-Kataloge

5.1 Inhalt und Anwendungsbereich

In den Dokumenten wird beschrieben, mit welchen Methoden Informationssicherheit in einem Unternehmen generell initiiert und gesteuert werden kann. Dieses Rahmenwerk kann auf die individuellen Belange eines Unternehmens angepasst werden, so dass ein effektives Informationssicherheits-Managementsystem aufgebaut werden kann. Dies schliesst Kataloge mit bewährten Vorgehensweisen (best practices) und präzisen Umsetzungshilfen mit ein.

5.2 Methodik

Die Erstellung der IT-Sicherheitskonzeption ist eine der zentralen Aufgaben des IT-Sicherheitsmanagements. Es müssen die erforderlichen IT-Sicherheitsmassnahmen identifiziert und in einem Konzept dokumentiert werden. Um den unterschiedlichen Anwendungsszenarien in den Unternehmen gerecht zu werden, erfolgt eine strukturierte Vorgehensweise nach dem Baukastenprinzip.

Zu übergeordneten Themen, wie u. a. dem Sicherheitsmanagement, der Notfallvorsorge sowie typischen Bereichen des technischen IT-Einsatzes sind Bausteine verfügbar, die Gefährdungen und Massnahmenempfehlungen zusammenfassen. Im Rahmen der Erstellung eines IT-Sicherheitskonzeptes wird die Umsetzung der folgenden Schritte empfohlen:

- IT-Strukturanalyse
- Schutzbedarfsfeststellung
- Modellierung des IT-Verbunds (Auswahl der Massnahmen, Soll-Ist-Vergleich)
- Ergänzende Sicherheitsanalyse
- Konsolidierung und Umsetzung der Massnahmen
- Audit / Aufrechterhaltung u. Verbesserung

Weiterführende Informationen:
http://www.bsi.de/gshb

goSecurity.ch/infonews

GO OUT Production GmbH
Schulstrasse 11
CH-8542 Wiesendangen

Telefon 052 320 91 20
Fax 052 320 91 21

6 Weitere Standards

Dies sind nur wenige Standards, die im Bereich IT-Sicherheit existieren. Ein umfassendes Nachschlagewerk für viele weitere Standards bildet der „Kompass der IT-Sicherheitsstandard“, des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien e.V. BITKOM. An diesem hat auch die Firma GO OUT Production GmbH mitgearbeitet. Sie können die aktuelle Version kostenlos unter http://www.nia.din.de/sixcms_upload/media/2397/Kompass%20der%20IT-Sicherheitsstandards_2009.pdf herunterladen.

7 Fazit

Standards geben eine gute Übersicht, welche Vorgehensweisen und welche Mittel zum Ziel führen. Die Umsetzung benötigt jedoch weiterhin eine gute Planung, viel Zeit, Durchhaltewillen und die Unterstützung der Geschäftsleitung. Wenn alle am gleichen Strick und vor allem auf der gleichen Seite ziehen, führt ein strukturiertes Vorgehen zur Erhöhung der IT-Sicherheit.