

ISO/IEC 27001 in der Praxis

Bedeutung, Anwendung und Nutzen für Managementsysteme der Informationssicherheit

Carsten Casper ¹

Einordnung: Um Informationssicherheit kontrollierbar herstellen und zielgerichtet verbessern zu können, ist die Anwendung definierter Verfahren und Regeln notwendig, deren Gesamtheit als Managementsystem für Informationssicherheit bezeichnet wird. ISO/IEC 27001 ist ein Standard für Systeme zum Management von Informationssicherheit (ISMS). Die Verwendung von Standards ist nur sinnvoll, wenn sie hinreichend weit verbreitet und etabliert sind. Status, Verbreitung und Erfahrungen bei der Verwendung eines Standards stellen wichtige Informationen dar, wenn diese zur Gestaltung der Informationssicherheit in Unternehmen und Institutionen herangezogen werden.

Schlüsselwörter: ISO27001, ISO27002, ISO27000, ISO27004, ISO27005, ISO2700x, ISO/IEC, Informationssicherheit, Risikomanagement, Kontrollmaßnahmen, Prüfung, Zertifizierung, Beratung

Abstract

Dieser Beitrag beschreibt die Entstehung des ISO/IEC 27001 Standards und die Gründe warum seine Akzeptanz ständig zunimmt. Es wird dargestellt, welchen Status ISO/IEC 27001 heute hat und wie Unternehmen vorgehen, um ein ISMS basierend auf ISO/IEC 27001 aufzubauen. Der Hauptteil besteht aus einer Betrachtung der verschiedenen Phasen von Implementierung, Prüfung und Zertifizierung. Dabei werden auch notwendige Investitionen benannt. Den Abschluss bilden Beobachtungen, wie Unternehmen Prüfung und Zertifizierung in der Praxis effizient vorbereiten und durchführen können.

¹ Kontakt per E-Mail: Carsten.Casper@gartner.com und Carsten@Casper.eu.



Carsten Casper

arbeitet seit über 15 Jahren im Bereich Informationssicherheit, zunächst als technischer und strategischer Berater bei der META Group, dann als Senior Expert bei der Europäischen Agentur für Netzwerk- und Informationssicherheit (ENISA) und schließlich als Research Director beim Marktforschungsunternehmen Gartner.

Dabei hat er für diverse Unternehmen Richtlinien und Organisationsformen für Informationssicherheit entwickelt, meist auf dem Standard ISO/IEC 27001 aufbauend. Zuletzt hat sich die Problematik des europäischen Datenschutzes zu seiner Hauptaufgabe entwickelt.

Einleitung

ISO/IEC 27001 ist Teil einer Serie internationaler Standards zur Informationssicherheit, der langsam aber stetig an Bedeutung gewinnt. Insbesondere für international tätige Firmen gibt es keine Alternative zu ISO/IEC 27001. Laut einer Gartner-Umfrage von 2010 verwenden bereits 33% der Unternehmen diesen Standard, allerdings mit unterschiedlichen Zielsetzungen. Während er für einige lediglich Strukturierungshilfe für die Arbeit des Managementsystems zur Informationssicherheit (ISMS) ist, zielen andere auf die Zertifizierung ab, um sich bescheinigen zu lassen, dass sie in diesem Bereich hinreichend gut aufgestellt sind. In jedem Fall sollten Unternehmen den Standard nur dann nutzen, wenn sich dies mit den Unternehmenszielen in Einklang bringen lässt. Bei der Umsetzung steht umfangreiche Literatur sowie eine große Anzahl erfahrener Berater, Partner und Werkzeuge zur Verfügung.

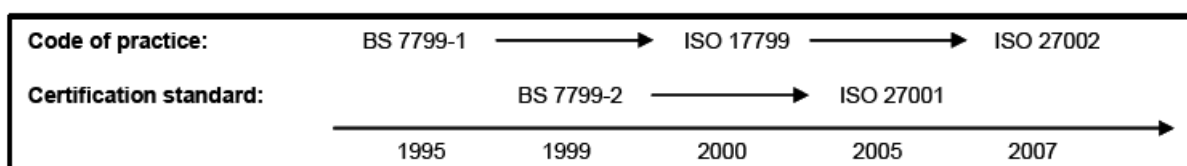
Inhaltsverzeichnis

1.	Entwicklung des Standards	3
2.	Gründe für seine zunehmende Verwendung	3
3.	Umsetzung – Von der Beratung bis zur Zertifizierung	4
3.1.	ISO/IEC 27001 als Struktur	4
3.2.	Interne Prüfung nach ISO/IEC 27001.....	4
3.3.	Zertifizierung nach ISO/IEC 27001	5
4.	Beobachtungen aus der Praxis	5
5.	Zusammenfassung	6
6.	Ausblick.....	6
7.	Verwandte Dokumente	7
8.	Literatur	7

1. Entwicklung des Standards

Der hier diskutierte ISO/IEC Standard basiert auf dem britischen Standard BS7799, der in zwei Teilen vorliegt: Teil 1 wird auch Code of Practice genannt, Teil 2 ist der Standard, nachdem ein ISMS tatsächlich zertifiziert wird.

Bevor der britische Standard als ISO-Standard übernommen wurde, hatten einige Länder bereits ihre eigenen ISMS-Standards entwickelt, die dem britischen Standard sehr ähnlich waren (z.B. UNE 71502 in Spanien, DS 484 in Dänemark und SS 62 77 99 in Schweden). Manche Literatur verweist im gleichen Atemzug auf „BS 7799-1/-2“ und „ISO/IEC 17799“, obwohl genau genommen zwischen dem britischen Standard und dem internationalen Standard, sowie zwischen dem Code of Practice und dem Standard nach dem zertifiziert wird, unterschieden werden muss. Man könnte sagen, dass ISO/IEC 27001 (der Zertifizierungsstandard) das „Was“ beschreibt, während ISO27002 (Code of Practice) die Umsetzung, das „Wie“, detailliert. Die folgende Abbildung veranschaulicht die Geschichte der Entwicklung.



Source: Gartner (September 2008)

Die Standardisierungsgruppe ISO/IEC JTC 1/SC 27, die für ISO/IEC 27001 verantwortlich zeichnet, hat im Laufe der Jahre auch eine Reihe weiterer Standards für Informationssicherheit entwickelt, vor allem zum Risikomanagement (ISO27005), zur Implementierung eines ISMS (ISO27003), zur Messung des Reifegrades (ISO27004) und Prüfungsdurchführung (ISO27007). Der Verbreitungsgrad dieser erst 2008 und 2009 veröffentlichten Standards ist aber noch weit hinter der Verbreitung der weithin bekannten Standards ISO/IEC 27001 und ISO/IEC 27002 zurück.

2. Gründe für seine zunehmende Verwendung

Mehr als 6000 Unternehmen weltweit sind bereits nach ISO/IEC 27001 zertifiziert (davon allein mehr als 3300 in Japan). Diese Zahlen stammen aus einem inoffiziellen Verzeichnis (siehe [2]), die tatsächliche Zahl dürfte deutlich höher ausfallen, da nicht alle Zertifizierungsdienstleister ihre Daten in dieses Register einspeisen. Außerdem orientieren sich viele Firmen am Standard, ohne sich tatsächlich zertifizieren zu lassen. Laut einer Gartner-Umfrage von 2010 verwenden oder unterstützen 33% der Befragten ISO/IEC 27001/27002 als Standard in IT Compliance Projekten – deutlich mehr als bei vergleichbaren Rahmenwerken wie ITIL (18%), SAS 70 (26%), CoBIT (16%) oder PCI DSS (11%). Eine ganze Reihe von Gründen bewegen Unternehmen und Organisationen dazu, sich an ISO/IEC 27001 zu orientieren.

- Ein Unternehmen, das sein ISMS auf den Standard stützt, kann sicher sein, dass es alle derzeit relevanten Aspekte von Informationssicherheit abdeckt. Vielen Firmen behandeln ISO/IEC 27001 – zusammen mit ISO/IEC 27002 – als eine Art Checkliste, die die Elemente Sicherheitsrichtlinien, Sicherheitsorganisation, Personal, physische Sicherheit, Kommunikations- und Betriebsmanagement, Zugriffskontrolle, Beschaffung/Entwicklung/Wartung von Informationssystemen, Vorfallmanagement, Notfallvorsorge und Compliance abdeckt.
- Firmen, die dem Standard folgen, lassen sich leichter überprüfen und die Ergebnisse können besser mit anderen verglichen werden. Der Standard veranlasst Unternehmen dazu, den Geltungsbereich des ISMS genau zu definieren, zwingt sie einem Plan-Do-Check-Act Prozessmodell zu folgen, und zu entscheiden, welche detaillierten Kontrollmaßnahmen das Unternehmen konkret implementieren muss.

- Eine erfolgreiche ISO/IEC 27001 Prüfung oder ein Zertifikat helfen einem Unternehmen darzulegen, inwieweit es seine Sorgfaltspflichten in Bezug auf Informationssicherheit erfüllt hat, zum Beispiel im Rahmen rechtlicher Anforderungen. Obwohl kein Gesetz die Verwendung von ISO/IEC 27001 explizit vorschreibt, verlangen doch einige, wie beispielsweise das Aktiengesetz in §91(2), dass Unternehmen das Thema Risikomanagement ernster nehmen, und zum Beispiel ein internes Kontrollsystem einführen. ISO/IEC 27001 kann hierbei einen wesentlichen Beitrag leisten.
- Eine Ausrichtung auf ISO/IEC 27001 hilft einem Unternehmen außerdem, verschiedene Elemente zusammenzuführen. Wer den Standard einführt, findet breite Unterstützung durch Software-Werkzeuge (insbesondere zur Dokumentation und Automation von Kontrollmaßnahmen), sowie Hilfe bei der Abbildung dieses Informationssicherheitsstandards auf verwandte IT-Standards wie ITIL oder CoBIT. Damit lässt sich die Einhaltung verschiedener Gesetze und Regelwerke nachweisen, ohne Kontrollmaßnahmen mehrfach zu implementieren und Prüfungen wiederholt durchführen zu müssen.

3. Umsetzung – Von der Beratung bis zur Zertifizierung

Unternehmen verwenden ISO/IEC 27001 in vielfältiger Weise. Häufig starten sie zunächst mit einem Beratungsprojekt, um dann später eine formale Prüfung oder Zertifizierung anzuschließen.

3.1. ISO/IEC 27001 als Struktur

Der erste Schritt für alle Unternehmen ist, die notwendige Expertise zusammenzutragen, entweder durch interne Ressourcen oder durch externe Berater. Diese initiieren dann die Einrichtung eines ISMS (d.h. sie definieren Geltungsbereich und Grenzen, Richtlinien, Ziele, Risikoanalyse und Auswahl der Kontrollmaßnahmen), implementieren und betreiben es (inklusive Training und Ressourcenverwaltung), beobachten und beurteilen das ISMS (Effektivität und Risikobeurteilung) und kümmern sich um fortwährende Verbesserung und Wartung.

Man beachte dabei den Unterschied zwischen Einhaltung des Standards und Zertifizierung. Viele Beratungsfirmen helfen bei der Gestaltung von Informationssicherheit „nach ISO/IEC 27001“, was aber nicht heißt, dass die beratenen Firmen auch die Zertifizierung erhalten werden oder würden. Einhaltung von ISO/IEC 27001 ist keine exakte Wissenschaft und Berater vertreten unterschiedliche Meinungen, wann ein Kunde auf die Zertifizierung ausreichend vorbereitet ist. Letztendlich ist das Wort des akkreditierten Prüfers maßgebend.

Für viele Firmen ist die Frage der notwendigen Ressourcen für die Beratung entscheidend. Wichtig ist hier vor allem die Anzahl der Mann-Tage. Einige Monate sind üblicherweise zu veranschlagen. Dabei reicht die hierfür zu vorher zu sehende Spannbreite der Tagessätze von den „Big4“-Beratern über IT-Sicherheitsboutiquen bis hin zur internen IT-Mannschaft. Spezielle ISO/IEC 27001-Ausbildung vom Team zu verlangen ist zwar sinnvoll, aber nicht unbedingt notwendig. Hinreichende Erfahrung im Bereich IT-Sicherheit tut es oft auch.

3.2. Interne Prüfung nach ISO/IEC 27001

Wenn ein ISMS eingerichtet ist – idealer Weise eines, das von Beginn an auf ISO/IEC 27001 ausgerichtet wurde –, dann kann eine interne Prüfung gemäß ISO/IEC 27001 sinnvoll sein, um zum Beispiel der Firmenleitung zu zeigen, dass man standardkonform oder zumindest standardnah arbeitet. Eine Prüfung sollte regelmäßig stattfinden und bestätigen, dass Prozesse und Kontrollmaßnahmen des ISMS effektiv arbeiten und auf dem neuesten Stand gehalten werden. Eine interne Prüfung hat noch nichts mit einer offiziellen Zertifizierung zu tun, aber sie kann helfen, sich ein objektives Bild zu machen.

ISO/IEC 27001 ist keine reine Checkliste (auch wenn er teilweise so verwendet wird) und eine Prüfung erfordert einige Erfahrung. Der Prüfer – entweder ein Externer oder auch jemand aus der Revisionsabteilung – sollte eine formale Ausbildung mitbringen, zum Beispiel die Examinierung als „BSI Lead Auditor“ oder ein vergleichbares Training nach ISO/IEC17024. Am besten ist, wenn er oder sie auch als Prüfer akkreditiert und im International Register of Certificated Auditors eingetragen ist (siehe [3]). Bislang sind solche Prüfer allerdings rar, d.h. entsprechend teuer. Da es auch lediglich darum geht, der eigenen Unternehmensleitung die Standardkonformität vorzuführen, ist der Einsatz eines examinierten und akkreditierten Prüfers in diesen Fällen nicht unbedingt notwendig.

3.3. Zertifizierung nach ISO/IEC 27001

Wenn ein Unternehmen zuversichtlich ist, dass sein ISMS gemäß den vorgegebenen Standards arbeitet, kann es sinnvoll sein, dies mit einem offiziellen Zertifikat den externen Partnern gegenüber darzustellen. Vielleicht möchte das Unternehmen eine ISO/IEC 27001-Zertifizierung auch dafür verwenden, der breiten Öffentlichkeit zu vermitteln, dass im Bereich Informationssicherheit alles Menschenmögliche getan wird. In der Praxis sind es vor allem Dienstleister, die sich mit ISO/IEC 27001-Zertifizierung schmücken. Bei internen IT-Abteilungen ist eine offizielle Zertifizierung eher selten.

Nur bestimmte Prüfungsunternehmen können Zertifikate nach ISO/IEC 27001 ausstellen. Sie folgen dem Standard ISO/IEC17021, der Prinzipien und Anforderungen für die Fähigkeit, Vergleichbarkeit und Unabhängigkeit von Prüfungen und Zertifizierungen von Management-Systemen beschreibt. Solche Prüfungsunternehmen müssen bei einer nationalen Akkreditierungsstelle eingetragen sein. In Deutschland ist dies der Deutsche Akkreditierungsrat (DAR) / Trägergemeinschaft für Akkreditierung (TGA). Jedes Land pflegt ein nationales Register akkreditierter Firmen, ein internationales Register gibt es nicht.

Eine einmalige Prüfung nach ISO/IEC 27001 ist nicht ausreichend für die Zertifizierung. Nach der umfangreichen Erstprüfung muss das Unternehmen alle sechs Monate mit einer Teil-Prüfung rechnen, eine weitere umfassende Prüfung erfolgt nach drei Jahren. Die aufzuwendenden Mann-Tage sind in jedem Fall entscheidend für die anfallenden Kosten, die Zertifizierungsgebühren selber fallen kaum ins Gewicht und sind denen von ISO 9001 oder ISO 14001 Zertifizierungen vergleichbar.

Unternehmen, die eine ISO/IEC 27001-Prüfung wünschen, haben vor allem drei Optionen, einen Prüfer zu finden.

1. Sie können im International Register of Certificated Auditors (siehe [3]) nach einem Prüfer suchen
2. Sie können das nationale Akkreditierungsregister nach einem geeigneten Prüfungsunternehmen abfragen
3. Sie können das eingangs erwähnte inoffizielle ISO/IEC 27001-Register durchsuchen (siehe [2]), das von der ISMS International User Group verwaltet wird. Es zeigt nicht nur Prüfer an, sondern auch welche anderen Unternehmen zertifiziert wurden und für welchen Unternehmensbereich das Zertifikat gilt.

Prüferfirmen, die in den meisten dieser Zusammenhänge erwähnt werden, sind BSI Management Systems, verschiedene TÜV Gesellschaften, KPMG, Bureau Veritas und Det Norske Veritas (DNV), in Deutschland auch DQS.

4. Beobachtungen aus der Praxis

- Prüfungen und Zertifizierungen kosten Zeit und Geld. Unternehmen sind eher geneigt hier zu investieren, wenn der geschäftliche Nutzen auch nachvollziehbar wird. Dies ist in der Regel dann der Fall, wenn die Zertifizierung von einem Geschäftspartner verlangt wird. Noch ist allerdings eine ISO/IEC 27001-Zertifizierung nicht Standard. Der Kunde würde nicht unbedingt einen gleichwertigen Lieferanten finden, der zertifiziert ist. Idealerweise sollte der Anfragende garantieren, dass die Leistung tatsächlich abgerufen werden wird, wenn der Lieferant in die ISMS-Zertifizierung investiert hat.
- Es besteht ein großer Unterschied in der Komplexität zwischen der Einrichtung eines ISMS nach ISO/IEC 27001 und der Erhebung der Nachweise für eine Zertifizierung. Internationale Unternehmen sollten zwar ein ISMS mit globaler Ausrichtung entwerfen, mit einer weltweit gültigen Sicherheitsrichtlinie und weltweit arbeitender Sicherheitsorganisation. Die konkrete Prüfung und Zertifizierung sollte aber Schritt-für-Schritt pro Land erfolgen, mit einem national akkreditierten Prüfer.
- Es gibt einige Überschneidungen mit anderen Management-Systemen, z.B. Qualitätsmanagement nach ISO 9000, Umweltmanagement nach ISO 14000. Erfahrung in diesen Bereichen sollte in eine ISO/IEC 27001-Zertifizierung mit eingebracht werden.
- Einige Firmen haben die ISO/IEC 27001-Prüfungen mit der Innenrevision integriert. Wenn zum Beispiel die Innenrevision jedes Jahr 40% des Unternehmens prüft, und ISO/IEC 27001 im gleichen Zusammenhang mit abgefragt wird, dann hat das Unternehmen nach zweieinhalb Jahren auch die ISMS-Prüfung erledigt. Die Möglichkeit eines solchen Vorgehens hängt aber stark vom konkreten Geltungsbereich des ISMS ab, der auf ein bestimmtes Rechenzentrum, eine Anwendung oder einen Geschäftsprozess beschränkt sein kann.

5. Zusammenfassung

Unternehmen, die ihr Informationssicherheitsmanagement am Standard ISO/IEC 27001 ausrichten wollen, durchlaufen dabei in der Regel verschiedene Phasen. Zunächst schätzen sie die Akzeptanz und damit den Wert des Standards in ihrer Branche ein. Sie holen sich häufig externe Beratung ins Haus, passen die Arbeitsweise ihrer IT-Sicherheitsabteilung an den Standard an, und lassen das neue ISMS zunächst informell überprüfen. Schließlich lässt sich das Unternehmen von einem akkreditierten Berater zertifizieren. Nicht alle Unternehmen durchlaufen allerdings alle Phasen. Andererseits gehen manche Unternehmen auch über diese Phasen und den Standard ISO/IEC 27001 hinaus und verwenden aus der gleichen ISO2700x Serie zusätzlich Standards für Risikomanagement, Messung von Kennzahlen oder Implementierungsrichtlinien.

6. Ausblick

Obwohl die erste Version des Standards bereits 1995, also vor gut 15 Jahren veröffentlicht wurde, ist die Ausrichtung an ISO/IEC 27001 immer noch nicht selbstverständlich. Mit der Zunahme von IT-Sicherheitsproblemen und -Vorfällen war allerdings in den letzten Jahren zu beobachten, dass Unternehmen die Informationssicherheit ihrer Partner verstärkt systematisch durchleuchten wollen. Dieser Trend wird sich fortsetzen, unterstützt durch die Verfügbarkeit verwandter Standards der ISO2700x-Serie für Implementierung, Messung und Risikomanagement, die zusätzliche Hilfestellungen für die Einrichtung und den Betrieb eines Managementsystems für Informationssicherheit geben.

7. Verwandte Dokumente

BSM Anwender Nr. 202: Wolfram Funk: Rollen für Informationssicherheit in einer Best-Practice-Organisation vom 8. Jan. 2010 beschäftigt sich mit Prozessen des Informationssicherheitsmanagements und den Verantwortlichkeiten im Umfeld der Informationssicherheit im Rahmen eines Systems zum Management von Informationssicherheit (ISMS) nach ISO/IEC 27001:2005.

8. Literatur

- [1] ISO/IEC 27001:2005 http://www.iso.org/iso/catalogue_detail.htm?csnumber=42103
- [2] International Register of ISMS Certificates - <http://www.ISO/IEC 27001certificates.com>
- [3] International Register of Certificated Auditors – <http://www.irca.org/about/links.html>

© 2009 Eberhard von Faber und Friedrich-L. Holl, Brandenburg an der Havel, alle Rechte vorbehalten. Verwertung ist nur mit vollständiger Quellenangabe und unter Angabe der Bezugsquelle erlaubt. Reproduktion und anderweitige Wiedergabe des Dokumentes bedarf darüber hinaus der ausdrücklichen Genehmigung der Rechteinhaber.

Titel: The Bulletin Security Management
Herausgeber: Eberhard von Faber und Friedrich-L. Holl

ISSN: 1869-2125
Bezugsquelle: www.security-management.de

Kontakt:



Prof. Dr. Eberhard von Faber und
Prof. Dr. Friedrich Lothar Holl
Fachhochschule Brandenburg
Fachbereich Wirtschaft
Studiengang Security-Management
Magdeburger Str. 50, 14770 Brandenburg

Unterstützt von:



Infos und Kontakt: www.t-systems.de/ict-security