Zertifizierung von Informationssicherheit in Unternehmen – ein Überblick

Leitfaden

BITKOM

Impressum

Herausgeber:	BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Albrechtstraße 10 A 10117 Berlin-Mitte Tel.: 030.27576-0 Fax: 030.27576-400 bitkom@bitkom.org www.bitkom.org
Ansprechpartner:	Lutz Neugebauer Tel.: 030.27576-242 l.neugebauer@bitkom.org
Redaktion:	Lutz Neugebauer
Autorenteam	Prof. Dr. Rainer Rumpel (Persicon cert AG) (Sprecher der PG), Arnd Chrostowski (KPMG AG), Ulf Greifzu (IBM Deutschland GmbH), Frank Hebestreit (IBM Deutschland GmbH), Peter Pakosch (Toll Mobile GmbH & Co. KG), Holger Rieger (Bundesdruckerei GmbH)
Redaktionsassistenz:	Leila Ambrosio
Gestaltung / Layout:	Design Bureau kokliko / Anna Müller-Rosenberger (BITKOM)
Copyright:	BITKOM 2011
Stand:	Januar 2011, Version 1.0

Zertifizierung von Informationssicherheit in Unternehmen – ein Überblick

Leitfaden

BITKOM

Inhaltsverzeichnis

1 Einleitung

Bedeutung der Informationssicherheit für Unternehmen

Der Einsatz moderner Informations- und Kommunikationstechnologie (ITK) ist heute für die meisten Organisationen eine Selbstverständlichkeit. Kaum ein Geschäftsprozess kommt mehr ohne die Unterstützung von ITK-Systemen aus. Das gilt gleichermaßen für die Kernprozesse in Unternehmen wie beispielsweise die Produktion, aber auch Support-Prozesse wie Einkauf, Vertrieb und Verwaltung. Mit einer hohen Durchdringung der Organisationen mit ITK wächst aber auch gleichzeitig deren Abhängigkeit. IT-Systeme, die nicht zur Verfügung stehen, oder Daten, die ausgespäht, manipuliert, kompromittiert oder schlichtweg gelöscht wurden, können für die Nutzer-Organisationen ernsthafte rechtliche oder wirtschaftliche Konsequenzen nach sich ziehen. Daher hat die Informationssicherheit – gerade in Unternehmen mit hohem ITK-Anteil – heute eine hohe Bedeutung bekommen.

Informationssicherheit, also die Verfügbarkeit von Systemen, die Integrität und Vertraulichkeit von Daten und die Authentizität von Transaktionen, betrifft nicht nur die jeweilige Einzelorganisation. Auch Partner einer Organisation wie beispielsweise Kunden und Lieferanten können in einer vielfältig vernetzten Welt von Störungen des normalen Ablaufs in Mitleidenschaft gezogen werden.

Es liegt daher auf der Hand, dass gerade auch die Partner ein berechtigtes Interesse daran haben, dass durch den ITK-Einsatz keine unnötigen Störungen entstehen und sich in die eigene Organisation fortpflanzen. Für die jeweilige Organisation bedeutet das im Umkehrschluss, dass der Nachweis eines sicheren Umgangs mit ITK-Systemen das Vertrauen der externen Partner in die eigene Organisation steigern kann. Unter Umständen werden geschäftliche Beziehungen erst durch diesen Nachweis möglich.

Schwerpunkte und Ziele des Leitfadens

Der vorliegende Leitfaden beschäftigt sich intensiv mit den Möglichkeiten des Nachweises von Informationssicherheit in Organisationen durch Zertifizierung. Dabei steht die Zertifizierung von Managementsystemen im Vordergrund – nicht aber die Zertifizierung von Personen oder ITK-Produkten.

Zielgruppe der Publikation sind Unternehmen und Organisationen, die eine Zertifizierung anstreben oder sich über die wesentlichen Inhalte und Randbedingungen einen ersten Überblick verschaffen wollen. Neben dem theoretischen Unterbau soll über anschauliche Beispiele auch ein möglichst hoher Praxisbezug für den Leser hergestellt werden.

2 Grundlagen

2.1 Managementsysteme für Informationssicherheit im Kontext mit anderen Managementsystemen

Managementsysteme, die die Informationssicherheit in Organisationen unterstützen, haben in den letzten Jahren in erheblichem Maße an Bedeutung gewonnen. Das lässt sich auf zwei Trends zurückführen: Einerseits spielen Managementsysteme in privaten und staatlichen Organisationen eine zunehmend wichtige Rolle. Andererseits erhält die Informationssicherheit in vielen Organisationen wachsende Aufmerksamkeit. Alle Managementsysteme sind geprägt von Ihrem Systemrahmen. Der bekannteste und älteste stammt aus dem Qualitätswesen. Im Jahr 1994 verabschiedete die International Organization for Standardization (ISO) die Normenreihe ISO 9000ff. zu Qualitätsmanagement und Qualitätssicherung. Diese Normen wurden mittlerweile mehrfach revidiert und konsolidiert. Die aktuelle Zertifizierungsnorm ist ISO 9001:2008 Quality management systems -- Requirements. Die Anforderungen an dieses Managementsystem sind hauptsächlich geprägt von folgenden Prinzipien:

- Prozessorientierung
- Dokumentation
- Verantwortung der Leitung
- Messung, Analyse und Verbesserung

An diesen Prinzipien orientiert sich auch die Anforderungsnorm für ISMS, ISO/IEC 27001:2005 Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen.

Grundlage beider Managementsystemrahmen ist der vierphasige, zyklische Managementprozess nach W. E. Deming und W. A. Shewhart (PDCA-Zyklus).

PDCA-Zyklus

Die genannten Prinzipien mitsamt dem PDCA-Zyklus sind das Fundament moderner Managementsysteme. Auch weitere Managementsystemnormen wie Information technology — Service management — Part 1: Specification (ISO/IEC 20000-1:2005) und Umweltmanagementsysteme - Anforderungen mit Anleitung zur Anwendung (DIN EN ISO 14001:2009) basieren hierauf. Somit ergeben sich beachtliche Synergien bei der Einführung von Managementsystemen. Auch bei der Zertifizierung ist es erwägenswert, eine kombinierte Zertifizierung durchführen zu lassen. Allerdings soll darauf hingewiesen werden, dass ein Managementsystem wie das ISMS Spezifika aufweist, die erheblich den Charakter des Managementsystems prägen. Wenn eine Organisation bereits gelernt hat, die Organisationsleitung in das Managementsystem angemessen einzubeziehen, die Dokumente angemessen zu lenken und das System regelmäßig zu prüfen und zu verbessern, dann wird es ihr leichter fallen, das auch bei einem weiteren Managementsystem zu tun. Beim ISMS

1 Herausgeber: Bayerisches Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie – erschienen 2003

ist das aber noch nicht für eine Zertifizierung ausreichend, da die Norm einen umfangreichen Anhang A enthält, in dem verpflichtende Ziele von Sicherheitsmaßnahmen aufgeführt sind. Insofern sollte das Synergiepotenzial bei Kombi-Zertifizierungen eines ISMS und eines weiteren Managementsystems nicht überschätzt werden.

Die Idee der Einführung eines integrierten Managementsystems, also eines übergreifenden Systems, das mehrere Systeme beinhaltet, ist bedenkenswert und wird beispielsweise in der Broschüre „Integriertes Managementsystem – Ein Leitfaden für kleine und mittlere Unternehmen“[1] vorgestellt.

2.2 Motive und Gründe für eine Zertifizierung

Heute ist die überwiegende Zahl der Geschäftsprozesse von unterstützenden IT-Services abhängig. Für viele Unternehmen hängt mittlerweile ihr Image möglicherweise sogar ihre Existenz von der Verfügbarkeit und Zuverlässigkeit dieser Services ab. Es besteht also ein inhärentes Interesse, die Informationstechnologie so zu verwenden, dass die Informationssicherheit im Unternehmen gewährleistet ist. Darüber hinaus ist zu bedenken, dass es bei Einführung und Betrieb eines ISMS nicht nur um IT geht. Nicht zuletzt die aktuellen Entwicklungen rund um die Internetplattform WikiLeaks zeigen: auch jedes bedruckte Blatt Papier, das im Geschäftsbetrieb erzeugt wird, oder jeder gesprochene Satz kann vertrauliche Informationen enthalten. Jede Organisation, für die die Verfügbarkeit, Vertraulichkeit und Integrität wichtiger Informationen – möglicherweise aus ganz unterschiedlichen Motiven – eine besondere Bedeutung hat, sollte die Einführung eines ISMS erwägen. Da aber der Vorbereitungsaufwand für eine Zertifizierung des ISMS beträchtlich ist, wird sich jede wirtschaftlich denkende Organisation zu Recht fragen, ob sich eine solche Zertifizierung lohnt oder ob eine interne Auditierung des ISMS nicht ausreichend ist. Folgende Kriterien eignen sich als Entscheidungshilfe:

a. Differenzierung im Wettbewerb

Mit einem Zertifikat für ein ISMS sind Unternehmen in der Lage, Managementkompetenz im Thema Informationssicherheit nachzuweisen und so das Vertrauen von Kunden, Mitarbeitern und auch der Öffentlichkeit in die eigene Organisation zu stärken. Ein Zertifikat bestätigt, dass die Organisation ein angemessenes Sicherheitsniveau erreicht hat, aufrecht erhält und somit ein zuverlässiger Partner ist. Ein Unternehmen mit ISMS-Zertifikat kann sich am Markt von den Wettbewerbern abheben, da ein ISMS-Zertifikat sicherlich kein Massenprodukt ist.

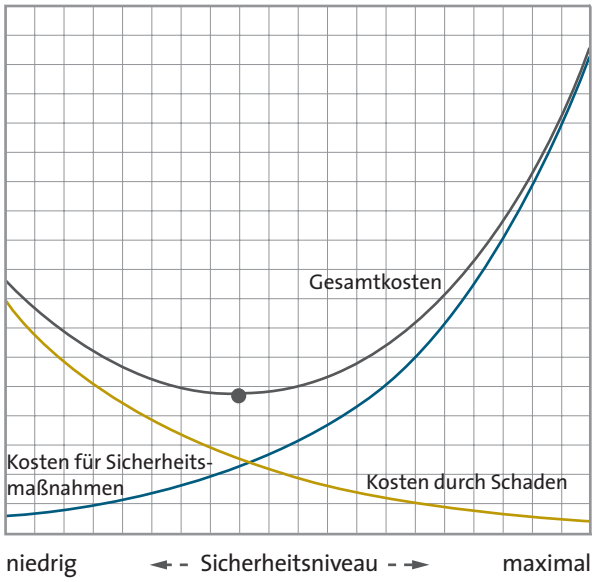
Darüber hinaus wird in aktuellen Ausschreibungen vermehrt verlangt, dass der Anbieter ein ISMS-Zertifikat aufweisen kann. Das gilt insbesondere für Ausschreibungen von öffentlichen Stellen oder Mitwirkung an Projekten der öffentlichen Hand.

b. Interner Nutzen einer Zertifizierung

Mehr Sicherheit kostet Geld, in der Regel ohne erkennbar mehr Umsatz zu generieren. Der Nutzen von Sicherheitsmaßnahmen besteht in erster Linie darin, die möglichen Verluste infolge von Sicherheitsschwachstellen zu reduzieren. Nicht selten entscheidet dann der sogenannte Zusatznutzen über die Angemessenheit einer ISMS-Zertifizierung. Der Zusatznutzen kann für das eine Unternehmen marginal sein, während er für das andere Unternehmen ausschlaggebend ist. Wie groß der Zusatznutzen für Ihr Unternehmen sein könnte, lässt sich an typischen Nutzenaspekten erkennen:

- Konsequente Reduzierung der Verluste infolge von Sicherheitsvorfällen
- Höhere Verfügbarkeit der IT-Systeme
- Bessere Qualität ihrer Geschäftsprozesse
- Kundenbindung
- Wichtiger Beitrag zur Erfüllung von gesetzlichen Anforderungen, zum Beispiel
  - Bilanzrechtsgesetze
  - Datenschutzgesetz

Es ist also offensichtlich auch im Hinblick auf interne Prozesse vorteilhaft, auf eine Zertifizierung hinzuarbeiten. Aber ist ein solches Projekt auch wirtschaftlich? Wie hoch ist der so genannte Return on Invest? Diese Frage sollte vor dem Start eines Projekts zur Zertifizierung des ISMS analysiert werden. Als Illustration soll hierfür Bild ... dienen. Eine Institution, die mit einem Sicherheitsprojekt hundertprozentige Informationssicherheit erreichen will, würde sich mit diesem Projekt ruinieren.



Wirtschaftlich vertretbares Sicherheitsniveau in Abhängigkeit von den Gesamtkosten

c. Vorschriften

Sollten staatliche Vorgaben einer Organisation die Zertifizierung ihres ISMS vorschreiben, so ist eine weitere Diskussion unnötig. Da einschlägige Gesetze für Unternehmen eher implizit davon ausgehen, dass Daten sicher verwaltet und transportiert werden, findet sich derzeit noch keine Gesetzesnorm, die ein ISMS zur Pflicht macht. Dennoch gibt es einige Vorschriften, die eine Zertifizierung – zumindest indirekt – sinnvoll erscheinen lassen.

- Der deutsche Gesetzgeber erwartet von der Leitung einer GmbH die Sorgfalt eines ordentlichen Geschäftsmannes und von dem Vorstand einer AG die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters[2]. Es ist in den genannten Gesetzen allerdings nicht explizit die Rede von der Existenz eines ISMS. Vom Risikomanagementsystem wird zwar dessen Existenz, nicht aber dessen Zertifizierung gefordert.
- Das Bundesdatenschutzgesetz hat umfangreiche Anforderungen an den Datenschutz formuliert. Hiervon ist auch das Themengebiet Datensicherheit in Teilen betroffen. Bei dem im § 9a beschriebenen Datenschutzaudit handelt es sich um eine Kann-Bestimmung.
- Im Rahmen von Globalisierung und Internationalisierung ist es notwendig, über die deutsche, beziehungsweise europäische Sichtweise hinaus weitere Vorschriften zur Kenntnis zu nehmen, die von Relevanz sind. Hierzu gehört insbesondere das amerikanische Gesetz Sarbanes-Oxley Act of 2002 (SOX) , das als Reaktion auf Bilanzskandale von großen amerikanischen Unternehmen erlassen wurde und unter anderem die Ordnungsmäßigkeit der Abschlüsse von Unternehmen verbessern soll, die den öffentlichen Kapitalmarkt der USA in Anspruch nehmen. Das Gesetz betrifft auch ausländische Tochtergesellschaften betroffener Unternehmen. Der Fokus liegt nicht auf der Informationssicherheit, sondern auf Aspekten der betriebswirtschaftlichen Ordnungsmäßigkeit. Ein besonderes Augenmerk sollte aber der Section 404, „Management Assessment of Internal Controls“, gewidmet werden, in der ein internes Kontrollsystem für die Finanzberichtserstattung gefordert wird. Es ist wichtig, dass die Finanzinformationen verfügbar und integer sind. Das sind bekanntermaßen auch Ziele der Informationssicherheit. Die Zertifizierung eines zugehörigen ISMS wird aber nicht explizit gefordert.

2 Im Aktiengesetz ist darüber hinaus sogar Folgendes festgelegt: „Der Aufsichtsrat kann aus seiner Mitte einen oder mehrere Ausschüsse bestellen, namentlich, um seine Verhandlungen und Beschlüsse vorzubereiten oder die Ausführung seiner Beschlüsse zu überwachen. Er kann insbesondere einen Prüfungsausschuss bestellen, der sich mit der Überwachung des Rechnungslegungsprozesses, der Wirksamkeit des internen Kontrollsystems, des Risikomanagementsystems und des internen Revisionssystems sowie der Abschlussprüfung, hier insbesondere der Unabhängigkeit des Abschlussprüfers und der vom Abschlussprüfer zusätzlich erbrachten Leistungen, befasst.“

- Das Bilanzrechtsmodernisierungsgesetz als deutsches Äquivalent zu SOX verpflichtet den Aufsichtsrat zur Überwachung des internen Kontroll- und des Risikomanagementsystems. Es gilt aber nur für Aktiengesellschaften.
- In der Finanzdienstleistungsbranche gilt das Kreditwesengesetz (KWG). § 25a fordert eine angemessene technisch- organisatorische Ausstattung des Kreditinstituts und die Festlegung eines angemessenen Notfallkonzepts, insbesondere für IT-Systeme. Das Institut muss diesbezüglich regelmäßige Überprüfungen durchführen. Die Mindestanforderungen an das Risikomanagement (MaRisk) konkretisieren die gesetzlichen Vorgaben. Der Betrieb eines ISMS ist hier unerlässlich, dessen Zertifizierung allerdings nicht explizit gefordert.
- Bei IT-Dienstleistern ist es naheliegend, dass der Betrieb eines ISMS ausschlaggebend sein kann. Allerdings ist die Relevanz für ein klassisches Systemhaus deutlich weniger hoch als für einen Hosting-Dienstleister, denn im Gegensatz zum Hosting-Dienstleister verarbeitet das Systemhaus nur wenige Daten seiner Kunden, wenn man von den für die Erhaltung der Geschäftsbeziehung notwendigen Daten absieht. Ein Rechenzentrum dagegen, das seine Infrastruktur in erster Linie für seine Kunden betreibt und zur Verfügung stellt, ist in natürlicher Weise damit konfrontiert, dass der Kunde seine Daten beim Dienstleister verarbeiten lässt. Das kann auch für andere Dienstleister gelten, die bestimmte Aufgaben – zum Beispiel Lohn- und Gehaltsabrechnung – für Kunden übernommen haben und infolgedessen auch die zugehörigen Daten verarbeiten. Für diese Dienstleistungsorganisationen gibt es sowohl auf nationaler als auch internationaler Ebene Prüfstandards. Erwähnt werden sollten hier der deutsche Prüfstandard IDW PS 951 IDW PS 951 Prüfung des internen Kontrollsystems beim Dienstleistungsunternehmen für auf das Dienstleistungsunternehmen ausgelagerte Funktionen und der amerikanische Prüfstandard International Standard on Assurance Engagements (ISAE) 3402 „Assurance Reports on Controls at a Third Party Service Organization“[3]. Die hier geprüften internen Kontrollen umfassen in der Regel auch Kontrollen, die die Informationssicherheit und deren Management betreffen. Kein Serviceunternehmen ist verpflichtet, sich nach einem solchen Standard prüfen zu lassen. Die Kunden fordern aber zunehmend entsprechende Prüfberichte. Die Zertifizierung des ISMS der Organisation würde die ISMS-spezifischen Kontrollen gemäß IDW PS 951 und SAS 70 bzw. ISAE 3402 abdecken.

Fazit: Es gibt also bislang keinen aus den Vorschriften deduzierbaren Zwang zur ISMS-Zertifizierung, allerdings besteht für viele Unternehmen eine Pflicht zum Betreiben eines Risikomanagementsystems oder internen Kontrollsystems, bei denen die Analyse und Behandlung von Informationsrisiken Bestandteil sind.

2.3 Wichtige Standards und Normen für die ISMS-Zertifizierung

Im Rahmen der Einführung eines ISMS und der Vorbereitungen auf eine anschließende erfolgreiche Zertifizierung dieses Systems muss zunächst nur die eine internationale Norm ISO/IEC 27001 verbindlich angewendet werden. Weitere, verwandte Normen bieten dem Anwender wertvolle Hilfen hinsichtlich der Interpretation, des Verständnisses und der Anwendung der Norm ISO/IEC 27001.

Im Folgenden werden die für eine ISMS-Einführung und Zertifizierung wichtigsten Normen bzw. Standards kurz vorgestellt.

Die ISO-27000 Familie bestand ursprünglich nur aus den beiden Standards ISO/IEC 27001 und ISO/IEC 27002 (bis 2008: ISO/IEC 17799). Als die Norm ISO/IEC 27001 schnell große Verbreitung fand, wurde deutlich, dass weitere erläuternde bzw. vertiefende Standards notwendig sind, die unter anderem die Themen Risikomanagement, ISMS-Implementierung und Anforderungen an Auditoren

3 bis 2010: SAS 70 Statement on Auditing Standard 70: Service Organizations, herausgegeben vom American Institute of Certified Public Accountants (AICPA)

näher beleuchten sollten. Aus dieser Erkenntnis und Notwendigkeit heraus wurden und werden immer mehr detaillierende ISMS-unterstützende Normen entwickelt und veröffentlicht.

In Deutschland gibt es ein spezielles Verfahren zur Einführung eines ISMS. Auf dieses wird gesondert in Abschnitt 2.3.2 eingegangen.

2.3.1 ISO/IEC-Standards zu Informationssicherheits-Managementsystemen[4]

ISO/IEC 27000:2009, Information technology - Security techniques - Information security management systems - Overview and vocabulary

- Inhalt:
  - Überblick zu den Standards der ISO 27000-Familie;
  - Einführung in Informationssicherheits-Managementsysteme (ISMS)
  - kurze Beschreibung des PLAN-DO-CHECK- ACT (PDCA) Prozesses; und
  - Begriffe und Definitionen, die in den Standards der ISO 27000-Familie verwendet werden.

- Bemerkung:
  Die Anwendung der Norm ist freiwillig und dementsprechend nicht verbindlich für das Erlangen einer ISO/IEC-27001- Zertifizierung. Nichtsdestotrotz ist die Verwendung dieses Standards im Rahmen der Planung und Einführung eines ISMS zu empfehlen.

ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements

- Inhalt
  Dieser internationale Standard spezifiziert die Anforderungen an die Einrichtung, die Implementierung, den Betrieb, die Überwachung, den Review sowie die Pflege und Verbesserung eines Informationssicherheits- Managementsystems (ISMS) im Kontext der allgemeinen Geschäftsrisiken einer Organisation. Er spezifiziert außerdem Anforderungen an die Implementierung von auf eine Organisation oder Teilen einer Organisation zugeschnittenen Informationssicherheitsmaßnahmen. Die Norm ist aufgrund Ihres generischen Charakters für alle Organisation anwendbar.

- Bemerkung
  Die Anwendung dieses Standards im Rahmen einer angestrebten ISO/IEC 27001-Zertifizierung ist zwingend gefordert. Die Zertifizierung eines ISMS gemäß ISO/IEC 27001 wird immer als Bewertung der Konformität mit dieser Norm durchgeführt.

ISO/IEC 27002:2005, Information technology - Security techniques - Code of practice for information security management

- Inhalt
  Dieser Standard bietet eine Liste von allgemein anerkannten Maßnahmenzielen sowie bewährten Maßnahmen samt Implementierungshinweisen an, welche als Unterstützung bei der Auswahl und Implementierung von Informationssicherheitsmaßnahmen herangezogen werden kann. Die behandelten Maßnahmen finden sich in der Norm ISO/IEC 27001 im Anhang A wieder (ohne Implementierungshinweise).

- Bemerkung

Die in der Norm ISO/IEC 27002 beschriebenen Maßnahmen können durch den Anwender in ihrer Granularität nach eigenem Ermessen verfeinert und weiter ausgestaltet werden.

Im Rahmen einer angestrebten ISO/IEC 27001-Zertifizierung sollte ISO/IEC 27002 gemeinsam mit dem ISO/IEC 27001 verwendet werden.

4 Ergänzende Ausführungen und weitere Standards findet man in der BITKOM-Publikation Kompass der IT-Sicherheitsstandard:s, 4. Auflage, BITKOM, 2009

ISO/IEC 27003:2010, Information technology - Security techniques - Information security management system implementation guidance

- Inhalt:
  Diese Norm gibt Anleitungen für die Planung und Einführung eines Informationssicherheits- Managementsystems (ISMS) gemäß ISO/IEC 27001.

ISO/IEC 27004:2009, Information technology - Security techniques - Information security management - Measurement

- Inhalt:
  Diese Norm bietet Unterstützung bei der Entwicklung und Anwendung von geeigneten Kennzahlen und Verfahren zur Messung der Wirksamkeit sowohl von einzelnen eingeführten Sicherheitsmaßnahmen als auch eines ganzen ISMS.

ISO/IEC 27005:2008, Information technology - Security techniques - Information security risk management

- Inhalt:
  Dieser Standard bietet Hilfe bei Entwicklung und Betrieb eines Informationssicherheits-Risikomanagementsystems, welches in seinen Inhalten und seinem Vorgehensmodell den Anforderungen an ein Risiko-Managementsystem gemäß ISO/IEC 27001 entspricht.

- Bemerkung für die Normen 27003 - 27005
  Die Nutzung ist freiwillig und dementsprechend nicht verbindlich für die Erlangung einer ISO/IEC 27001-Zertifizierung. Dennoch ist die Anwendung dieser Standards im Rahmen der Planung und Einführung eines ISMS zu empfehlen.

ISO/IEC 27006:2007, Requirements for bodies providing audit and certification of information security management systems

- Inhalt:
  Diese Norm definiert qualitative Anforderungen an Organisationen, welche eine Akkreditierung als ISO/IEC-27001-Zertifizierungsstelle anstreben. Dabei werden auch die fachlichen und sozialen Anforderungen an die in dieser Zertifizierungsstelle agierenden Personen berücksichtigt. Dieser Standard ergänzt die Norm ISO/IEC 17021 (Anforderungen an Stellen, die Managementsysteme zertifizieren).

- Bemerkung
  Der Standard ist von allen ISO/IEC-27001-Zertifizierungsstellen verbindlich anzuwenden.

2.3.2 IT-Grundschutz-Standards des BSI

Beabsichtigt ein Unternehmen oder eine Behörde sich einer Konformitätsbewertung gemäß ISO/IEC 27001 unterzuziehen, so kann sie sich für das BSI als staatliche Zertifizierungsstelle entscheiden. Das BSI hat ein eigenes Prüfschema, das sie für Antragsteller als verbindlich ansieht. Dort sind Anforderungen festgelegt, wie die antragstellende Organisation ihr ISMS implementieren soll.

BSI Standard 100-1: Managementsysteme für Informationssicherheit (ISMS)

Dieser BSI-Standard definiert allgemeine Anforderungen an ein Informationssicherheits- Managementsystem (ISMS). Gemäß BSI ist dieser Standard vollständig kompatibel zu dem internationalen Standard ISO/IEC 27001. Einige Themenbereiche des ISO/IEC 27001 werden in diesem BSI-Standard etwas ausführlicher als in dem ISO-Standard behandelt, um dadurch dem Leser einen besseren und somit leichteren Einstieg in die ISMS-Thematik zu ermöglichen. Im Rahmen einer Zertifizierung gegen ISO 27001 auf der Basis von IT-Grundschutz muss dieser BSI-Standard zwingend angewendet werden.

BSI Standard 100-2: IT-Grundschutz-Vorgehensweise

Dieser BSI-Standard beschreibt, wie ein Managementsystem für Informationssicherheit in der Praxis aufgebaut und betrieben werden kann. Durch die detailliert beschriebene IT-Grundschutz-Vorgehensweise soll dem Anwender der Aufbau von angemessenen Informationssicherheitsstrukturen erleichtert werden.

Im Rahmen einer Zertifizierung gegen ISO 27001 auf der Basis von IT-Grundschutz muss dieser BSI-Standard zwingend angewendet werden.

BSI Standard 100-3: Risikoanalyse auf der Basis von IT-Grundschutz

Dieser BSI-Standard beschreibt die Vorgehensweise bei einer Risikoanalyse gemäß IT-Grundschutz. Die Durchführung einer Risikoanalyse wird im Rahmen der Einführung und des Betriebs eines ISMS explizit durch den internationalen Standard gefordert. Diese ist aber im Rahmen der IT-Grundschutz-Vorgehensweise für Objekte mit normalem Schutzbedarf bereits vorweggenommen worden. Zu diesem Zweck sind die IT-Grundschutzkataloge eingeführt worden. Bei Objekten mit erhöhtem Schutzbedarf muss in der Regel eine Risikoanalyse gemäß Standard 100-3 durchgeführt werden.

Im Rahmen einer Zertifizierung gegen ISO 27001 auf der Basis von IT-Grundschutz muss eine Risikoanalyse zum Einsatz kommen. BSI-Standard 100-3 ist hierbei sinnvoll, aber nicht zwingend.

BSI Standard 100-4: Notfallmanagement

Dieser BSI-Standard beschreibt den Weg zu einem systematischen Aufbau und Betrieb eines Notfallmanagements im Rahmen eines funktionierenden ISMS.

Im Rahmen einer Zertifizierung gegen ISO 27001 auf der Basis von IT-Grundschutz muss dieser BSI-Standard nicht zwingend angewendet werden. Seine Anwendung ist jedoch zu empfehlen.

IT-Grundschutz-Kataloge

Die IT-Grundschutzkataloge des BSI enthalten Standard-Sicherheitsmaßnahmen für typische Geschäftsprozesse und IT-Systeme.

Die darin aufgeführten sehr zahlreichen Standard-Sicherheitsmaßnahmen helfen einer ISO/IEC 27001-einführenden Organisation, für erkannte Schwachstellen und Bedrohungen Maßnahmen zur angemessenen Behandlung dieser Risiken zu selektieren, zuzuordnen und anschließend zu implementieren.

2.3.3 Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz

Dieses Prüfschema beschreibt die verbindliche Vorgehensweise, wie Auditoren vorgehen müssen, wenn sie im Rahmen einer Zertifizierungsprüfung für die Erlangung eines ISO 27001- Zertifikats auf der Basis von IT- Grundschutz tätig sind.

Dieses Dokument ist zunächst verbindlich für alle durch das BSI lizenzierten ISO-27001-Auditoren anzuwenden. Jedoch ergeben sich aus den Inhalten dieses Prüfschemas durchaus auch Anforderungen an die Organisation, welche ein Zertifikat ISO 27001 auf der Basis von IT-Grundschutz anstrebt. Darum ist es anzuraten, dass sich entsprechende Organisationen kritisch mit den Inhalten dieses Prüfschemas spätestens ab Beginn der relevanten Einführungsaktivitäten auseinandersetzen.

2.3.4 Ablauf der Zertifizierung gemäß ISO/IEC 27001

Der Ablauf einer Konformitätsprüfung bezüglich der Norm ISO/IEC 27001 ist nicht willkürlich bestimmbar, da unter anderem die Norm ISO/IEC 27006 hier Rahmenbedingungen liefert.

Tabelle 1 - Ablauf einer Prüfung gemäß ISO/IEC 27001

Schritt 1: Geltungsbereich des ISMS abstimmen	Der potentielle Kunde und die Zertifizierungsstelle besprechen den Umfang des ISMS. Hiernach wird die Zertifizierungsstelle ein Angebot und einen Vertragsentwurf zur Erbringung der Zertifizierungsdienstleistung erstellen.
Schritt 2: Vertrag schließen	Der Vertrag wird durch den potentiellen Kunden geprüft. Die Parteien unterzeichnen den Vertrag.
Schritt 3: Dokumentenaudit	Dieser Schritt (Audit Stufe 1) beinhaltet ein grobes Review des ISMS und bezieht alle ISMS-Schlüsseldokumente (z.B. Leitlinie für Informationssicherheit, Risikobewertung) mit ein. Es kann ein Standortbesuch stattfinden.
Schritt 4: Vor-Ort-Audit	In dieser Phase (Audit Stufe 2) findet die Umsetzungsprüfung statt, in der das Auditteam vor Ort überprüft, ob das Managementsystem samt den dokumentierten Sicherheitsmaßnahmen implementiert ist.
Schritt 5: Entscheidung über das Zertifikat	Vorausgesetzt dass beide Stufen des Audits ohne Abweichungen, also erfolgreich, abgeschlossen werden, wird die akkreditierte Zertifizierungsstelle ein ISO/IEC-27001-Zertifikat ausstellen.
Schritt 6: Zwischenzeitliche Überprüfungen des ISMS	Das Zertifikat ist drei Jahre gültig. Während dieses Zeitraums wird die Zertifizierungsstelle das ISMS des Mandanten einmal pro Jahr überprüfen, um sicherzustellen, dass das ISMS weiterhin angemessen betrieben wird. Nach drei Jahren kann der Audit-Zyklus mit der Zertifizierungsprüfung zur Erteilung eines Zertifikates von neuem beginnen.

2.3.5 ISO/IEC 27001 nativ und BSI-Grundschutz gegenübergestellt

In der nachfolgenden Tabelle sollen die beiden wesentlichen Ansätze nach dem internationalen Standard ISO/IEC 27000-Familie und dem nationalen Standard nach BSI-Grundschutz hinsichtlich wesentlicher Kriterien gegenüber gestellt werden.

	ISO/IEC 27001:	BSI-Grundschutz (auf Basis ISO/IEC 27001):
Verfügbarkeit und Kosten	Normen 27001/27002 auch in deutsch verfügbar (über Beuth-Verlag, ca. 350,- zusammen)	Normen, Kataloge und vollständiges Zertifizierungsschema in deutscher Sprache und kostenfrei im Internet verfügbar
Umfang der Norm	Etwa 35 Seiten, ca. 10 Seiten netto; 27002: 133 generische Maßnahmen auf ca. 140 Seiten	100-1 bis 100-3: mit ca. 160 Seiten; Grundschutzkataloge ca. 4.000 Seiten mit ca. 79 Bausteinen, 483 Gefährdungen und ca. 1.200 Maßnahmen
Auditoren	Auditoren müssen von einer akkreditierten Zertifizierungsstelle berufen sein.	Ca. 250 lizenzierte Auditoren, Liste veröffentlicht durch BSI
Anzahl der derzeit zertifizierten Institutionen	Rund 150 registrierte Zertifizierungen in Deutschland	Rund 50 Zertifikate veröffentlicht beim BSI
Bedeutung international	International uneingeschränkt anerkannt	Hoher Bekanntheitsgrad im deutschsprachigen Raum, insbesondere Public Sector
Zertifizierungsstellen	Zehn akkreditierte Zertifizierungsstellen, diese sind frei wählbar	BSI als einzige Zertifizierungsstelle
Grad der technischen Detaillierung	Schreibt keine technischen Umsetzungsdetails vor	Technisch sehr detailliert, konkret und umfangreich
Zertifizierungsaufwand	Zertifizierungsaufwand wird nach ISO 27006 kalkuliert und ist vorrangig abhängig von der Mitarbeiteranzahl des Scopes, beginnt bei 5 PT für Erst-Audit (+-30% für konkrete Faktoren wie Komplexität, Standorte, etc.)	Zertifizierungsaufwand mindestens 15 PT unabhängig vom Geltungsbereich (Größe des IT-Verbundes) ohne Mängelbehandlung und Rückfragen durch Zertifizierungsstelle, praktische Erfahrungen und Einschätzungen durch BSI selbst:Zertifizierungsaufwand von 14 bis 30 PT
Verbindung mit Risikomanagement	Freie Wahl einer angemessenen Risikomethodik (vgl. z.B. ISO 27005)	Sollte mit der Risikoanalyse 100-3 des BSI einhergehen, aber andere Risikoanalysen zulässig.
Werkzeuge zur Unterstützung	Tools mit sehr differenzierter Qualität und deutlich unterschiedlichen Kosten auf dem Markt, Auswahl schwieriger. Anwendung und Zertifizierung auch ohne Tools möglich.	Mehrere (auch kostenfreie) Tools am Markt verfügbar. Das BSI hat ein eigenes Tool. Tooleinsatz wird dringend empfohlen.
Voraussetzungen für Zertifizierung	Das ISMS sollte mindestens bereits 6 Monate betrieben werden, um die gelebten Prozesse und Lebenszyklen bis hin zum Verbesserungsprozess nachweisen zu können. Der Anwendungsbereich (Scope) darf sich in dieser Zeit nicht wesentlich ändern.	Das ISMS sollte mindestens bereits 6 Monate betrieben werden, um die gelebten Prozesse und Lebenszyklen bis hin zum Verbesserungsprozess nachweisen zu können. In dieser Zeit sollte der IT-Verbund relativ stabil sein, da sich ansonsten die Dokumentationen von IT-Strukturanalyse, Schutzbedarfsanalyse, Basissicherheits-Check etc. ändern und nachdokumentiert bzw. vollständig auch nachgearbeitet werden müssen.
Kombination mit anderen Zertifikaten	Zertifizierung ist kombinierbar, z.B. mit ISO 9001 (im Kombi-Audit ca. 30% weniger Aufwand);	Die Kombination mit einer anderen Zertifizierung ist beim BSI nicht möglich.

Fazit des Vergleichs:

Um für mehr Sicherheit in der Organisation und beim Einsatz von IT-Systemen innerhalb eines Unternehmens zu sorgen, sind beide Ansätze gleichermaßen geeignet. Vorausgesetzt die Normen werden jeweils ernsthaft berücksichtigt.

ISO-nativ konzentriert sich dabei eher auf die Sicherheitsprozesse, BSI-Grundschutz schafft mehr konkrete technische Sicherheit. ISO besitzt mehr Spielraum (Angemessenheit), BSI ist starrer und insgesamt meist aufwändiger. ISO-nativ lässt sich in vorhandene Managementsysteme leichter einbinden, BSI-Grundschutz kann oft nur als Insellösung betrieben werden auf Grund der speziellen Dokumentationsanforderungen.

Auf Grund des Vollständigkeitsansatzes und der hohen Detaillierung erfordert BSI-Grundschutz in der Regel einen höheren Pflegeaufwand zur Aufrechterhaltung des Zertifikates. Die Gültigkeitsdauer beider Zertifikate wurde inzwischen angeglichen. Ist eine internationale Anerkennung wichtig, führt kein Weg an der Zertifizierung bei einer akkreditierten Zertifizierungsstelle vorbei. Stehen neben dem Sicherheitsgewinn Partner oder Auftraggeber des öffentlichen Dienstes in Deutschland im Ziel der Anstrengungen, kann BSI-Grundschutz von Vorteil sein.

2.4 Zertifizierung: Relevante Institutionen

Eine Institution, die ihr ISMS zertifizieren lassen will, stößt früher oder später auf die Frage, wie eine Zertifizierung konkret abläuft. Deshalb soll an dieser Stelle über die am Zertifizierungsprozess beteiligten Personengruppen und Organisationen informiert werden.

Die Zertifizierungsstelle

Ziel eines ISMS-Zertifizierungsprojekts ist ein Zertifikat, das die Konformität des ISMS mit den Anforderungen in ISO/IEC 27001 bescheinigt. Aber wer erstellt dieses Zertifikat? Grundsätzlich darf jede Institution Bewertungen der Konformität mit der genannten Norm durchführen, da weder der Begriff „Zertifikat“ noch der Begriff „Zertifizierungsstelle“ rechtlich geschützt sind. Ein ISMS-Zertifikat ist aber natürlich nur so viel wert wie die Kompetenz und Anerkennung der zertifizierenden Stelle. Eine Zertifizierungsstelle kann sich deshalb wiederum ihre Konformität mit den Anforderungen an eine kompetente und unparteiliche Zertifizierungsstelle bescheinigen lassen. Diese sogenannte Akkreditierungsprüfung wird von einer Akkreditierungsstelle vorgenommen, die in der Regel vom

DAkkS Deutsche Akkreditierungsstelle

Staat eingesetzt ist. Viele, aber nicht alle Länder haben solche Akkreditierungsstellen. In Deutschland ist die Deutsche Akkreditierungsstelle GmbH für die Akkreditierung von Zertifizierungsstellen zuständig. Es ist also dringend zu empfehlen, sich bei einem Zertifizierungswunsch an eine für ISO/IEC 27001 akkreditierte Zertifizierungsstelle zu wenden, da ansonsten die Aussagekraft und Verwendbarkeit des Zertifikats stark eingeschränkt ist.

Bundesamt für Sicherheit in der Informationstechnik

Das BSI nimmt eine Sonderstellung ein. Die Zertifizierungsstelle des BSI für ISO/IEC 27001 ist nicht akkreditiert. Andererseits handelt ist sie selbst eine staatliche Stelle. Von Unparteilichkeit und Ordnungsmäßigkeit kann ausgegangen werden.

Die Auditoren

Eine Zertifizierungsstelle setzt für die Konformitätsbewertung Auditoren ein. Diese können interne oder externe Mitarbeiter der Stelle sein. Die Auditoren prüfen auf Weisung der Zertifizierungsstelle. Im Auditteam können auch Fachexperten mitwirken. Die Mitglieder des Auditteams müssen ihre Unparteilichkeit nachweisen. Der vom Auditteamleiter erstellte Auditbericht wird von der Zertifizierungsstelle auf Vollständigkeit und Angemessenheit geprüft.

Ausschlaggebend und verantwortlich für die Annahme oder Ablehnung einer Zertifizierung ist also letztlich nicht der Auditteamleiter, sondern die Zertifizierungsstelle.

3 Auf dem Weg zum Zertifikat: Tipps aus der Praxis

Während des Zertifizierungsaudits wird durch eine unabhängige und autorisierte Stelle geprüft, ob das vorhandene ISMS mit der zugrundeliegenden Norm konform ist. Die letztendliche Erteilung des Zertifikats setzt ein gelebtes, ISO/IEC 27001 konformes ISMS im Geltungsbereich voraus.

Tipp 1: Gemeinsames Norm-Verständnis erarbeiten

Die ISO/IEC 27001 als Grundlage ist mit ca. 10 Seiten „netto“ eine sehr kompakte Norm. Jeder einzelne Satz und oft sogar einzelne Worte sind von Bedeutung, manchmal entscheidend. Als Zertifizierungsbasis wird stets ohne Diskussion die offizielle internationale ISO/IEC 27001 (in englischer Sprache) gewählt und referenziert, in der praktischen Umsetzung in Deutschland aber häufig die DIN ISO/IEC 27001 genutzt. In deren „Nationalen Vorwort“ heißt es, dass die „Internationale Norm ISO/IEC 27001:2005-10 ... unverändert in das Deutsche Normenwerk übernommen“ wurde unter fachlicher Zuständigkeit des Arbeitsausschusses NA 043-01-27 AA „IT-Sicherheitsverfahren“ des Normenausschusses Informationstechnik und Anwendungen (NIA) im DIN. Aber über Übersetzungen wurde mitunter schon diskutiert und über die Bedeutung der einzelnen Worte im Original der ISO/IEC 27001 durch die Fachwelt übrigens auch. Eine detaillierte inhaltliche Auseinandersetzung, ein interner und externer fachlicher Austausch über das Normverständnis und ggf. auch eine Diskussion mit den Auditoren stärken eine ISMS und gehören zum Zertifizierungsprozess.

Tipp 2: Unterschiedliche Interessenlagen berücksichtigen

Die akkreditierten Zertifizierungsstellen sind angehalten, normkonforme Verfahren zur Durchführung von Zertifizierungen bereitzustellen und einzuhalten. Dafür sind die ISO/IEC 17021 „Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren“ und die ISO 19011 „Leitfaden für Audits von Qualitätsmanagement und/ oder Umweltmanagementsystemen“ maßgebend. Letztere definiert u.a. Auditprinzipien mit Anforderungen und Verhaltensgrundsätzen für Auditoren. Beide Normen werden in der ISO/IEC 27006 aufgegriffen. Die ISO/IEC 27006 enthält darüber hinaus Vorgaben für die Berechnung von Audit-Aufwänden und Empfehlungen für praktische Prüfhandlungen.

Die akkreditierten Zertifizierungsstellen selbst einschließlich ihrer Auditoren unterliegen mit ihrem Geschäft dem Wettbewerb sowie wirtschaftlichen Zwängen und werden in ihrer Tätigkeit ebenfalls überwacht, von der Deutschen Akkreditierungsstelle GmbH (DAkkS). Damit treffen in einem Audit verschiedene Parteien mit unterschiedlichen Interessen und Auflagen aber auch mit unterschiedlichen Erfahrungen, Ansichten und fachlichen Hintergründen aufeinander. Dies alles sollte im Umfeld einer Zertifizierung der Informationssicherheit beachtet werden. Es kann sehr hilfreich sein, sich gedanklich in die Lage der jeweils anderen Partei zu versetzen.

Vorbereitung eines Zertifizierungsaudits

Tipp 3: Verfügbarkeit notwendige Elemente sicherstellen

Ein gut vorbereitetes Audit schafft Vorteile für alle Beteiligten. Ein internes Audit ist eine geeignete Methode den Reifegrad des ISMS vor dessen offizieller Zertifizierung festzustellen und ist zugleich ein obligatorischer Normbestandteil. Die Zuverlässigkeit und Wirksamkeit des internen Auditsystems besitzen eine herausragende Bedeutung. Dazu gehören auch die hierfür belegbare Qualifizierung und Unabhängigkeit des „internen Auditors“, der auch ein „Externer“ sein darf. Sind die Planung und Durchführung von internen Audits sowie die Behandlung von dabei festgestellten Mängeln nicht nachweisbar, stellt

das eine wesentliche Abweichung dar. Wenn ein normatives Element, welches nicht ausgeschlossen werden darf (vgl. ISO/IEC 27001 Kapitel 1.2), nicht implementiert ist, kann kein positives Votum durch einen Auditor ausgesprochen werden. Eine Nachbesserung oder gar ein Abbruch des Zertifizierungsaudits wären notwendige Folge.

Ähnlich schwer wiegen z.B.

- das Fehlen einer Leitlinie zur Informationssicherheit,
- ein unzureichend definierter Geltungsbereich,
- eine fehlende oder nicht aktuelle Risikoanalyse bzw. deren nicht nachvollziehbare Methode,
- die Nichtexistenz einer Anwendbarkeitserklärung (als Ergebnis der Risikoanalyse und Zusammenfassung von bereits ergriffenen und anzuwendenden Maßnahmen und deren Ziele),
- eine unzureichende Unterstützung durch das Management, erkennbar an fehlenden Initiativen, Zustimmungen, Bestätigungen oder gar einer nicht vorhandenen Managementbewertung zum ISMS.

Tipp 4: Geeignete Zertifizierungsstelle auswählen

Die Auswahl einer geeigneten Zertifizierungsstelle steht an, wenn der Reifegrad des ISMS intern als normkonform eingeschätzt wird und dies nun offiziell bestätigt werden soll. Geeignet ist eine Zertifizierungsstelle sicher dann, wenn bereits eine vertrauensvolle Zusammenarbeit existiert, z.B. durch die Zertifizierung anderer Managementsysteme. Kann die bereits bekannte Zertifizierungsstelle zudem auf Erfahrungen zur Zertifizierung nach ISO/IEC 27001 verweisen, fällt die Entscheidung wahrscheinlich leicht. In diesem Falle kann man prüfen, ob ein kombiniertes Audit möglich ist.

Möglichkeit zu kombiniertem Audit nutzen

Hierdurch lassen sich Synergien nutzen und Aufwände reduzieren. Dann sind aber die Zertifizierungstermine zu beachten und deren Synchronität von Beginn einzuplanen.

Angebote vergleichen

Für alle anderen Fälle gelten die Grundsätze jeder Beschaffung, Angebote einholen, prüfen und vergleichen. Die akkreditierten Zertifizierungsstellen können mittels einer Abfrage auf den Webseiten der oben aufgeführten DAkkS abgerufen werden. Die Kosten, bzw. die Anzahl der Audit-Tage sollten sich auf Grund der einzuhaltenden Vorgaben nicht zu sehr unterscheiden. Entsprechende „Ausreißer“ bedürfen einer gründlichen Betrachtung.

Fachlichen Hintergrund der Auditoren prüfen

Es ist von Vorteil, sich mit einem Angebot die Auditoren namentlich nennen zu lassen. Leider gibt es aktuell kein aussagekräftiges zentrales Register der zugelassenen und aktiven Auditoren. Sind die Auditoren bekannt, kann heutzutage über deren beruflichen Werdegang oder fachlichen Hintergrund im Internet einiges in Erfahrung gebracht werden. Die Stärken der Auditoren ermöglichen Schlüsse auf zu erwartende „Tiefenprüfungen“. Der Auditor sollte das Geschäft des zu prüfenden Unternehmens verstehen. In einem unverbindlichen Vorgespräch einer Beauftragung besteht die Möglichkeit, sich gegenseitig kennenzulernen. Sicherheitsprojekte sind Vertrauenssache. Die „Chemie“ muss stimmen.

Optional: Voraudit durchführen

Mit der Durchführung eines Voraudits lassen sich letzte Zweifel an der grundsätzlichen Zertifizierungsbereitschaft ausräumen. Dies ist allerdings optional und in den meisten Fällen bei guter Vorbereitung überflüssig.

Chancen von so genannten Witness-Audits nutzen

Gelegentlich fragen Zertifizierungsstellen nach potentiellen Kunden für Witness-Audits. Bei diesen Audits wird die Zertifizierungsstelle gleichzeitig durch die DAKkS überwacht und bewertet. Es ist ein Irrtum, wenn Unternehmen glauben, dabei besonders streng geprüft zu werden und dann lieber davon Abstand nehmen. Das Gegenteil ist der Fall. Die Zertifizierungsstelle wird nur erfahrene Auditoren einsetzen und peinlichst darauf achten, dass

nichts verlangt wird, was die Norm nicht wirklich fordert und die Auditoren der DAKkS greifen in der Regel selbst nicht ein.

Tipp 5: Auditoren bei der Vorbereitung des Audits unterstützen

Geeignete Unterlagen für die Auditoren bereitstellen

Die erste zu übergebende Information ist eine aktuelle Unternehmenspräsentation. Sie erzeugt Verständnis und liefert zudem für den Auditor erforderliche Pflichtangaben für seine Berichte. Dazu gehört auch ein Organigramm. Wenn einzelne Dokumente des ISMS besonders sensibel sind, sollte überlegt und vorbereitet werden, inwieweit man diese Dokumente vor eventuellem Missbrauch schützt (z.B. geschützte PDF-Dokumente), eine Weitergabe von Auszügen oder Referenzen genügt oder ob in Absprache mit dem Auditor auf eine Weitergabe gänzlich verzichtet werden kann. Wenn bestimmte Informationen nicht gezeigt werden dürfen, muss dies vor einem Audit geklärt werden. Ebenso sollte vor einem Audit immer eine Geheimhaltungsvereinbarung abgeschlossen werden.

Die Bereitstellung bzw. Übergabe von Dokumenten zur Prüfung sollte so vorbereitet sein, dass deren Vertraulichkeit gewährleistet wird. Eine ZIP-Verschlüsselung garantiert dies nicht und zeugt nicht von einer Beherrschung aktueller Sicherheitstechnologien. Wenn keine E-Mail-Verschlüsselung bereitgestellt werden kann, könnte ein HTTPS-geschütztes Portal eine Alternative sein.

Verfügbarkeit von internen Fachleuten sicherstellen

Liegen die Auditplanungen vor, ist zu beachten, dass zu den Terminen alle Audittätigkeiten (auch parallele durch mehrere Auditoren) seitens des auditierten Unternehmens stets durch eigene Sachverständige begleitet werden. Gibt es terminliche Probleme mit der Verfügbarkeit einzelner Prozessverantwortlicher, sollte dies frühzeitig den Auditoren mitgeteilt werden. Deren Entgegenkommen ist dann wahrscheinlich.

Wenn die Vorbereitung noch eine Information und Motivation der Mitarbeiter im Geltungsbereich beinhaltet, ist auch deren korrekte Reaktion gesichert.

Durchführung/ Begleitung eines Zertifizierungsaudits

Tipp 6: Arbeitsbedingungen für die Auditoren optimieren

Alle Beteiligten wünschen eine erfolgreiche effiziente Durchführung des Zertifizierungsaudits. Dafür sind geeignete Arbeitsbedingungen bereitzustellen. Dies beinhaltet einen ungestörten Arbeitsraum mit besten Möglichkeiten zur Präsentation der relevanten Informationen und administrativen Zugriff auf die relevanten Anwendungen und Systeme zur Vorführung und Inspektion. Das leisten in der Regel ein PC mit Drucker und Projektor sowie LAN-Anschluss. Für die Auditoren sind nur Anschlüsse und Kommunikationsmittel erlaubt, wie sie sonst für Externe üblich bzw. im Regelwerk verbindlich vorgeschrieben sind. Wenn die Nutzung von fremden USB-Sticks im Unternehmen nicht erlaubt ist, gilt dies erst recht im Zertifizierungsaudit. Wenn fremde Notebooks keinen Zugang in das Unternehmensnetz erhalten, dann auch die Notebooks der Auditoren nicht. Im Notfall können geforderte Informationen auch geeignet nachgereicht werden.

Gerade im Beisein der Auditoren haben die Festlegungen des Unternehmens absolute Verbindlichkeit. Eine vertrauensvolle und angenehme Atmosphäre, beinhaltet keine Aufforderung zur Nachlässigkeit z.B. hinsichtlich eines aufgeräumten und gesicherten Arbeitsplatzes. Auch sonst sollten keine Schwachstellen oder Mängel freiwillig offenbart oder gar um Rat nach deren Behandlung angefragt werden, es sein denn, mit einer solchen Aktion soll von anderen Schwachstellen abgelenkt werden. Auditoren sind jedoch diesbezüglich sehr sensibel und in der Regel sehr erfahren und es ist ihnen untersagt zu

beraten oder konkrete Produkte zu empfehlen. Ebenso werden Auditoren es stets vermeiden, selbst in produktive Systeme einzugreifen.

Tipp 7: „Klassische“ Prüfpunkte beachten und Fehlerquellen beseitigen

Fast alle Auditoren prüfen den Zutrittsschutz und die Einhaltung von Passwortrichtlinien. Alle reagieren auf typische „Reizsignale“ wie Brandlasten, Schmutz oder Wasser führende Leitungen in Rechenzentren bzw. Bastelmaterialien in Serverschränken oder herumliegende ggf. unbeschriftete Datenträger. In der ISO/IEC 27006 werden in deren Anhang (Tabelle D) einige Auditmethoden empfohlen. Besonders die expliziten Empfehlungen und ggf. Kommentare zu den Systemtests sind wichtig. Eine kritische Sichtung und Berücksichtigung dieser Tabelle lohnt sich.

Tipp 8: Unmittelbares Feedback der Auditoren einfordern

Auditoren sind angehalten ihre Prüfabschnitte mit den Betroffenen unmittelbar auszuwerten. Sollte dies im Eifer untergehen, kann eine Nachfrage helfen. So sind frühzeitig Ergebnisse und Trends aber auch Missverständnisse oder nicht repräsentative Einzelabweichungen bzw. irrtümliche Falschaussagen erkennbar. Eine Reaktion bzw. Korrektur ist so noch direkt im Audit möglich. Sollten über geprüfte Sachverhalte unterschiedliche Bewertungen oder Meinungen entstehen, lohnt sich durchaus eine fachlich fundierte und sachliche Diskussion mit dem Auditor bis hin zur Wahrnehmung des Rechts zur diesbezüglichen Dokumentation im Auditbericht. Dem auditierten Unternehmen darf daraus kein Nachteil entstehen.

Tipp 9: Abschlussbesprechung mit Auditor ernstnehmen

Das Zertifizierungsaudit sollte mit der Abschlussbesprechung enden. An dieser sollte wie auch zum Auftaktgespräch ein verantwortlicher Vertreter des Managements teilnehmen. Dies bekräftigt die Wahrnehmung der geforderten Verantwortung. Zur Abschlussbesprechung ist dem Unternehmen das vorläufige Gesamtvotum mitzuteilen und die Liste der festgestellten Abweichungen zu übergeben, deren Nachbesserungsfrist von 90 Tagen damit beginnt. Es gibt viele Möglichkeiten erfolgte Nachbesserungen zu belegen. Gelingt eine diesbezügliche Vereinbarung, was letztendlich im Ermessen des Auditors liegt, ist eine Nachkontrolle vor Ort nicht erforderlich.

Nachbereitung eines Zertifizierungsaudits

Tipp 10: Nachbesserungsfrist sinnvoll nutzen und Termine einhalten

Wenn ein Nachreichen von Dokumenten oder Nachweisen vereinbart wurde, sollte dies nicht zum letztmöglichen Termin stattfinden. Auch in dieser Phase sind ggf. noch Rückfragen zu klären. Alle eingebundenen Parteien haben ihre Termine. Zertifizierungsaudits sind für die Auditoren relativ kurze Projekte mit einer extrem hohen Informationsmenge. Eine Rückbesinnung nach fast 90 Tagen ist u.U. für die Auditoren sehr anstrengend. Die nachgereichten Dokumentationen zu den Mängelbeseitigungen sollten deshalb möglichst so zusammengestellt sein, dass der Auditor nicht genötigt wird, umfangreiche Dokumente nochmals zu recherchieren. Ebenso sollten wie auch im Audit stets nur die absolut nötigen bzw. geforderten Informationen präsentiert werden. Erstens spart das einem Auditor Zeit und zweitens kann es nicht dazu führen, bisher übersehene Schwachstellen im Nachhinein noch zu offenbaren.

Tipp 11: Nach dem Audit ist vor dem Audit.

Falls eine Beseitigung von Mängeln im Einzelfall noch etwas hakt, spätestens zum folgenden Überwachungsaudit sollte dies abgestellt sein. Die Nachkontrolle von Mängelbeseitigungen ist obligatorischer Bestandteil eines

Überwachungsaudits. Eine unzweckmäßige, fehlerhafte oder fehlende Behandlung von festgestellten Abweichungen eines Zertifizierungsaudits stellt den Sicherheitsprozess ernsthaft in Frage.

Eine frühzeitige Abstimmung und Reservierung von Terminen für Folgeaudits schafft langfristige Verbindlichkeit für alle intern und extern Beteiligte, ermöglicht die Planung ausreichender Zeitreserven zu den einzuhaltenden Fristen und vermeidet so Stress.

Um den Erfolg einer bestandenen Zertifizierung für alle Interessierten sichtbar zu machen, besteht die Möglichkeit einer Veröffentlichung in einschlägigen Registern wie z.B. unter www.iso27001certificates.com/.

4 Aufwand einer Zertifizierung

Unter dem Aufwand für eine Zertifizierung wird hier nicht der gesamte Aufwand für den Aufbau eines ISMS mit der Umsetzung der daraus abgeleiteten Maßnahmen verstanden. Diese Vorbereitungsphase ist immer zeitaufwändig. Es sollen lediglich die für das Zertifizierungsaudit entstehenden Aufwände durch externe Auditoren dargestellt werden. Anbei trotzdem zur Information: Der während eines Audits intern anfallende Aufwand ist in der Regel mindestens so groß wie der externe Aufwand, da die Auditoren fast über die gesamte Auditzeit Interviewpartner benötigen und damit binden.

Für die Kalkulation des externen Auditaufwandes gelten die Planungsrichtlinien der ISO/IEC 27006, welche in die Kalkulations- und Angebotsverfahren jeder akkreditierten Zertifizierungsstelle übernommen sein sollten. Üblicherweise wird ein dreijähriger Zertifizierungszyklus betrachtet, welcher ein Zertifizierungsaudit und zwei Überwachungsaudits umfasst. Danach kann eine Rezertifizierung mit dem nächsten Zyklus anschließen.

Der Aufwand für ein Zertifizierungsaudit zur Informationssicherheit wird in der Norm höher eingeschätzt als der vergleichbare Aufwand für die Zertifizierung eines Qualitäts- oder Umweltmanagementsystems. Dies wird im Anhang C.3 der ISO/IEC 27006 dargestellt. Hauptkriterium zur Aufwandsberechnung ist die Anzahl der Beschäftigten im Geltungsbereich. Die Tabelle beginnt mit einem Richtwert für eine Erstzertifizierung von 5 PT bei bis zu 10 Beschäftigten, empfiehlt 15 PT bis 425 und endet mit 28 PT für Geltungsbereiche mit ca. 10.700 Beschäftigten und dem Hinweis bei Bedarf der Progression zu folgen.

Dieser Richtwert ist allerdings nur Ausgangsbasis für eine detaillierte Kalkulation, bei der die Größe des Geltungsbereiches, dessen räumliche Verteilung und Komplexität sowie die Relevanz der Informationssicherheit wegen der speziellen Geschäftstätigkeit oder der genutzten Technologien zu Aufschlägen oder Reduktionen im Umfang von ca. 30% führen können. In diesem Rahmen sollte sich also der Aufwand bewegen.

Bei kombinierten Audits (z.B. Qualitäts- und Informationssicherheitsmanagement) können ggf. weitere Reduktionen (ca. 15%) gewährt werden.

Dreißig Prozent des so ermittelten Aufwandes dürfen für Planung und Berichterstattung aufgewendet werden. Reisezeiten sind nicht enthalten. 70% sind demnach durch Auditoren vor Ort im Geltungsbereich zu erbringen.

Für die jährlichen Überwachungsaudits sind etwa ein Drittel Aufwand der Erstzertifizierung vorzusehen, für eine Rezertifizierung nach 3 Jahren ca. zwei Drittel.

Konkrete Zahlen soll nachfolgendes Beispiel liefern: Zertifiziert werden soll der Geltungsbereich eines ISMS an einem Standort mit 120 Beschäftigten. Der Basisrichtwert für die Erstzertifizierung liegt damit bei 12 Personentagen. Es handelt sich um ein Unternehmen, welches einfache Dienstleistungen erbringt. Nur wenige der Beschäftigten haben direkt mit der IT zu tun. Wenige Server werden in einem Serverraum für typische Büroarbeiten genutzt. Andere Kernanwendungen für die Lohnbuchhaltung, Kundenverwaltung sowie Abrechnung werden durch externe Dienstleister sicher gestellt. Eine Reduktion um 30% ist zulässig. Demnach sollten für die Erstzertifizierung etwa 8,5 PT geleistet werden, davon ca. 6 PT vor Ort. Diese 6 PT verteilen sich sinnvoll auf 2 PT für das Stufe-1-Audit (Bereitschaftsbewertung bzw. Dokumentenprüfung) und 4 PT für das abschließende Stufe-2-Audit. Für die jährlichen Überwachungsaudits sollten jeweils etwa 3 PT (2 vor Ort) vorgesehen werden. Somit wäre ein Gesamtaudit-Aufwand über den typischen Angebotszeitraum von 3 Jahren von 14,5 PT zu erwarten. Zu diesen aufwandsbezogenen Auditkosten kommen noch Bearbeitungsgebühren der Zertifizierungsstelle und üblicherweise die Reisekosten hinzu.

5 Zwei Fallstudien

5.1 Zertifizierung eines Unternehmens nach ISO/IEC 27001 nativ

Ausgangslage

In dieser Fallstudie wird ein mittelständisches Unternehmen betrachtet. Geschäftszweck ist die Bereitstellungen von IT-Diensten für Dritte (Webhosting, u.ä.).

Das Unternehmen wurde von seinem größten Kunden aufgefordert, eine Zertifizierung nach ISO27001 nachzuweisen.

Das Rechenzentrum des Unternehmens arbeitet seit Jahren sehr effektiv. Der physische und der Zutrittsschutz der Gebäude sowie eine hohe Qualität der Netzwerksicherheit und Hochverfügbarkeit sind gegeben. Das Unternehmen hat ein Qualitätsmanagement eingeführt, ist aber nicht nach ISO 9001 zertifiziert. Es gibt nur wenig Dokumentation zu den Prozessen. Des Weiteren gibt es kein durchgängiges Assetmanagement und keine geregelten Verfahren zur Erstellung und Freigabe von Dokumenten. Ein Risikomanagementsystem ist im Unternehmen etabliert, allerdings auf Geschäftsrisiken ausgerichtet. IT- und Sicherheitsrisiken waren nicht erfasst.

Projektorganisation

Für die Leitung des Projektes wurde ein Mitarbeiter berufen, der bereits Erfahrung mit dem Qualitätsmanagementsystem hat. Das Projektteam setzte sich aus einem Kernteam und Mitarbeitern aus den einzelnen Fachbereichen zusammen. Weiterhin wurde der IT-Betrieb, die interne Revision, der Datenschutz- und Unternehmenssicherheitsbeauftragte eingebunden. Zur Steuerung des Projektes wurde ein Steering Board mit Beteiligung des Geschäftsführers und dem CIO wurde aufgesetzt. Da im Unternehmen die fachliche Kompetenz für die Einführung des Sicherheitsmanagementsystems nicht ausreichte, wurde eine Ausschreibung zur Beauftragung von externen Beratern durchgeführt. Das Unternehmen legte Wert darauf, eine Bietergemeinschaft von Sicherheitsberatern und ISO27001-zertifizierten Auditoren zu beauftragen. Mit den externen Beratern wurde eine Vertraulichkeitsvereinbarung abgeschlossen.

Projektdurchführung

- Projektplan mit internen Audits

Im Projektplan wurden mehrere interne Audits im regelmäßigen Abstand vorgesehen, um den Projektfortschritt und das Erreichen der Zertifizierungsfähigkeit zu dokumentieren.

Begonnen wurde mit einer Analyse der Anforderungen aus den Normen ISO/IEC 27001 (ISMS), ISO/IEC 27002 (Security Controls) und ISO/IEC 27005 (Risk Management). In einem ersten Schritt wurde eine Gap-Analyse durchgeführt. Die Analyse überprüfte die vorhandenen Sicherheitsmaßnahmen auf Übereinstimmung mit Sicherheitspolitik und Sicherheitsrichtlinien des Unternehmens sowie den relevanten ISO-Standards. Auf Basis der in der Gap-Analyse evaluierten Punkte wurde ein Maßnahmenkatalog erstellt, die offenen Punkte dokumentiert und deren Umsetzung in der Projektplanung aufgenommen.

- Top-Down und Buttom-Up-Ansatz

Das Unternehmen hatte sich entschlossen, das Projekt sowohl „von oben – Top down“, also aus einer Managementperspektive heraus, als auch „von unten – Bottom up“, also aus Sicht des Betriebes, voranzutreiben. Im Rahmen des Top-Down-Ansatzes wurden im Wesentlichen die Sicherheitsrichtlinien erstellt, die Sicherheitsorganisation definiert, Rollen beschrieben, Sicherheitsprozesse eingeführt, notwendige Sicherheitsmaßnahmen sowie entsprechende Sicherheitschecks identifiziert und beschrieben. Im Rahmen des Buttom-Up-Ansatzes wurden bereits

existierende Sicherheitsmaßnahmen und Checks sowie bestehende Schnittstellen zu anderen Betriebsprozessen überprüft und dokumentiert. Im besten Fall erfolgt ein regelmäßiger Abgleich der Ergebnisse beider Ansätze, z.B. in der Bewertung der Umsetzbarkeit der neuen Richtlinien und Maßnahmen. Insbesondere sollte man keine Sicherheitsrichtlinie in Kraft setzen oder Sicherheitsmaßnahmen umsetzen, deren Einhaltung nicht kontrolliert werden kann.

Durch den Buttom-Up-Ansatz wurde die Betriebsorganisation stark in das Projekt eingebunden und spezifische Anforderungen und Randbedingungen der Betriebsprozesse konnten so eingebracht werden.

- Aufbau der Sicherheitsorganisation und Benennung von Sicherheitsbeauftragten

Eine Etablierung der Sicherheitsorganisation erfolgte in diesem Unternehmen ohne Probleme. Der Beauftragte für Informationssicherheit hatte sich schon im Vorfeld mit dem Thema auseinander gesetzt und wurde regelmäßig geschult. Rollen und Tätigkeiten wurden definiert und geeignete Mitarbeiter nach Absprache mit den Fachabteilungen ernannt. Aufgrund des Schulungsaufwandes und des Umstands, dass die Mitarbeiter noch weitere Aufgaben im Unternehmen wahrnehmen, musste mehrfach ein Ressourcenengpass überwunden werden.

- Einführung von Freigabeverfahren für Dokumente

Der Zertifizierungsprozess machte es aufgrund der großen Anzahl von Dokumenten erforderlich, ein unternehmensweites Dokumentenmanagement einzuführen. Hiermit wurde unter anderem ein verlässliches Versionsmanagement sichergestellt. Da die Freigabe von Richtlinien über mehrere Hierarchiestufen viel Zeit in Anspruch nahm, musste das Freigabeverfahren gestrafft werden.

- Einführung Assetmanagement

Im Unternehmen war ein Überblick über die wichtigen und schutzbedürftigen Werte (assets) nicht vorhanden. Daher wurde der Beschluss gefasst, ein so genanntes Assetmanagementsystem mit einem Asset-Lifecycle einzuführen.

- Einbindung der Sicherheitsrisken in das Risikomanagementsystem

Ein wesentliches Element eines ISMS nach ISO 27001 ist das Risikomanagement, das auf der systematischen Erkennung und Einschätzung von Risiken anhand von Risikoanalysen und Risikobewertungen basiert. Das im Unternehmen vorhandene Risikomanagementsystem ist in erster Linie prozess- und nicht assetorientiert. Das im Einsatz befindliche Tool konnte nicht angepasst werden. Das Unternehmen entschied sich daher dafür, eine Methode der Risikoanalyse anzuwenden, die dem Standard ISO/IEC 27005 entspricht.

- Einbeziehen der Mitarbeiter und des Managements

Im Rahmen der Einführung der Informationssicherheit im Unternehmen wurde eine umfangreiche Awareness-Kampagne durchgeführt. Die Maßnahmen wurden adressatengerecht vorbereitet. Für das Management und die Administratoren wurden beispielsweise spezifische Schulungen vorgenommen. Die Mitarbeiter wurden mittels E-Learning-Kursen, Flyern und Infoständen für Informationssicherheit sensibilisiert.

- Interne Audits

Neben der ersten Gap-Analyse wurden mehrere interne Audits von den beauftragten externen Auditoren durchgeführt, um den aktuellen Projektstatus zu verifizieren und Empfehlungen für eine Priorisierung bei der weiteren Projektplanung zu erhalten. Die Audits überprüften die vorhandenen Sicherheitsmaßnahmen auf Konformität mit der Sicherheitspolitik und den Sicherheitsrichtlinien des Unternehmens sowie dem Standard ISO/IEC 27001.

Um eine Nachverfolgung und fristgerechte Erledigung von offenen Maßnahmen sicherzustellen, wurden sämtliche Korrektur- und Verbesserungsmaßnahmen in einer

übergreifenden Maßnahmenliste zusammengefasst und von dem Projektteam nachgehalten. Die internen Audits wurden nicht vollumfänglich, d.h., bis auf die untersten Sicherheitsmaßnahmen, durchgeführt. Es wurde mit Stichproben gearbeitet, um den Zeit- und Budgetplan einhalten zu können.

Im Projekt wurden parallel zu den Audits der externen Auditoren eigene, interne Stichprobenaudits durchgeführt. Das Projektteam hatte dazu die interne Revision beauftragt, Prüfungen vorzubereiten und umzusetzen.

Erkenntnisse

- Eine Einführung eines ISMS wird ohne eine klare und sichtbare Unterstützung durch die Geschäftsführung und des Managements nicht erfolgreich sein.
- Eine Kombination von Top-Down- und Buttom-Up-Ansatz war erfolgreich durch die Einbindung aller Beteiligten bei einer offenen Kommunikation der erreichten Ergebnisse.
- Eine Projektdurchführung mit mehreren internen Audits schärft den Blick für die Erfordernisse an die Zertifizierung.
- Der Einsatz externer Berater ergänzt das methodische und fachliche Wissen des Unternehmens und verringert somit den Aufwand in der Umsetzung.
- Eine Gefahr beim Top-Down-Ansatz ist eine zu formale Herangehensweise. Das generische Vorgehensmodell zur Umsetzung eines ISMS liefert eine einheitliche Systematik und Vokabular und ermöglicht ein strukturiertes Vorgehen. Es ist aber kein Selbstzweck, sondern Mittel zum Zweck. Angebracht ist Pragmatismus und gesunder Menschenverstand. Letztendlich ist die Nachhaltigkeit der Maßnahmen im Unternehmen anzustreben.
- Beim Asset- und Risikomanagement ist eine frühzeitige und zügige Umsetzung anzustreben. Ein Risikomanagement benötigt, um effektiv funktionieren zu können, ein auf das Unternehmen angepasstes Kennzahlensystem. Dafür sind eine Inventarisierung von Assets, die Analyse der Abhängigkeiten und quantitative Risikobetrachtungen notwendig. Allerdings sollte hierbei auf einen angemessenen Detailierungsgrad geachtet werden, um den Aufwand in einem organisatorisch und kostenmäßig handhabbaren Rahmen zu halten.
- Die Einführung des Managementsystems für Informationssicherheit hat im betrachteten Unternehmen für eine Neuausrichtung in folgenden Unternehmensbereichen gesorgt: Qualitätsmanagement, Risiko- und Assetmanagement, Dokumentenverwaltung und IT-Betriebsprozesse. Die Umsetzung des Zertifizierungsprojektes wäre leichter gewesen, wenn die Beteiligten in den angesprochenen Bereichen bereits auf Bestehendes hätten aufbauen können. Die Entscheidung einer konsequenten Einführung eines ISMS hat das Unternehmen auch in Nachbarbereichen wesentlich vorangebracht.

5.2 Zertifizierung eines Unternehmens nach ISO/IEC 27001 und BSI-Grundschutz

Ausgangslage

In dieser Fallstudie wird ein mittelständisches Industrieunternehmen betrachtet, das sich aufgrund seines Produktportfolios sowohl im nationalen als auch im internationalen Markt positioniert. Das Unternehmen besitzt verschiedene nationale und internationale Standorte. Im nationalen Markt ist das Unternehmen unter anderem für öffentliche Auftraggeber tätig. Sicherheit ist in dem Unternehmen aufgrund seiner Kerntätigkeit als strategischer Erfolgsfaktor definiert.

Heutzutage ist der Besitz von Sicherheitszertifikaten die Voraussetzung dafür, sich an nationalen und internationalen Ausschreibungen beteiligen zu können. Es hat sich herauskristallisiert, dass internationale Auftraggeber in der Regel im Bereich Informationssicherheitsmanagement (ISM) das Zertifikat „ISO 27001 (nativ)“ verlangen, während nationale und öffentliche Auftraggeber sich Sicherheitskonzepte gemäß dem Standard „ISO 27001 auf der Basis IT-Grundschutz“ wünschen.

Das Unternehmen hatte sich aufgrund der Anforderungen internationaler Kunden in der Vergangenheit nach „ISO 27001 (nativ)“ zertifizieren lassen. Seine Risikoanalysen entsprechen diesem Standard. Dafür hat das Unternehmen u. a. eine einheitliche Methodik definiert, mit der die Eintrittswahrscheinlichkeit und die Auswirkungen von Risiken nach vorgegebenen Kategorien bewertet werden können. Auf Basis von definierten Sicherheitsrichtlinien und unternehmensspezifischen Bedrohungen wurden die kritischen informationstechnischen Unternehmenswerte analysiert. Dabei wurden auch Herstellerinformationen von Komponenten der eingesetzten IT-Infrastruktur berücksichtigt. Das Unternehmen hat sich hierbei von Beratungshäusern mit Schwerpunkt in der Informations- und IT-Sicherheit unterstützen lassen. Es war bereits nach „ISO 9001“ zertifiziert und hatte damit bereits wesentliche Prozesse zur Qualitätssicherung definiert. Dazu zählen beispielsweise geregelte Verfahren zur Erstellung und Freigabe von verbindlichen Regelungsdokumentationen oder die Etablierung eines kontinuierlichen Verbesserungsprozesses.

Eine weitere Maßnahme war, die wesentlichen Prozesse des Unternehmens – also seine Kernprozesse und Unterstützerprozesse – zu definieren und entsprechende Verantwortlichkeiten festzulegen. Das hat dazu beigetragen, dass inzwischen das Denken der Mitarbeiter in Prozessen etabliert und die Verantwortung für permanente Prozessoptimierung in der Belegschaft verankert ist und angenommen wird. Auch bei der Implementierung des Informationssicherheitsmanagement-Systems (ISMS) nach „ISO 27001 (nativ)“ konnte auf vorhandene Strukturen zurückgegriffen werden. So gab es bereits durch die Einführung des Qualitätsmanagements diverse Systematiken, wie z. B. die Erstellung und Freigabe von qualitätsgesicherten Dokumenten.

Im Unternehmen sichert eine eigene Organisationsabteilung die Qualität der Prozesse und deren Ergebnisse. Sie ist auch dafür zuständig, Maßnahmen aus internen und externen Audits zu verfolgen. Mitarbeiter der Abteilung unterstützen die jeweiligen so genannten Prozesseigner dabei, die Prozesse inhaltlich zu optimieren. Außerdem stellen sie die unternehmensweite Konsistenz der Prozesse sicher.

Problemstellung

Da seit einiger Zeit der nationale ISMS-Standard „ISO 27001 auf der Basis IT-Grundschutz“ immer bedeutender wird, musste das Unternehmen sich für beide Standards zertifizieren lassen.

Die beiden ISMS-Standards haben unterschiedliche Dokumentationsanforderungen. So benötigt die „ISO 27001 (nativ)“ z. B. eine so genannte Anwendbarkeitsdeklaration, während bei der „ISO 27001 auf der Basis IT-Grundschutz“ zur Bearbeitung der IT-Grundschutzkataloge eine datenbankbasierte Lösung eingesetzt werden muss. Auch wenn beide Standards eine große Schnittmenge aufweisen, besteht die Herausforderung darin, die Dokumentationsvorgaben beider Standards voll zu erfüllen. Dabei muss das Augenmerk auch darauf liegen, die Kosten für das Unternehmen, das in einem sehr wettbewerbsgetriebenen Markt tätig ist, möglichst gering zu halten.

Lösung

ISMS-Strategie festlegen

Um mittelfristig beide Standards erfüllen zu können, wurde eine entsprechende ISMS-Strategie festgelegt. Zunächst wurde der Standard „ISO 27001 auf der Basis IT-Grundschutz“ nur projektbezogen angewendet, um die vom jeweiligen Auftraggeber geforderten Audits bzw. Zertifizierungen vorlegen zu können. Um langfristig nicht zwei verschiedene Welten bearbeiten zu müssen, hat das Unternehmen sich dazu entschlossen, auch für die Zertifizierung nach „ISO 27001 (nativ)“ die Methoden des IT-Grundschutzes (z. B. Risikoanalysen) sukzessive unternehmensweit anzuwenden. Dies wurde dadurch erleichtert, dass die gemäß „ISO 27001 auf der Basis IT-Grundschutz“ eingesetzten Methoden (nämlich die BSI-Standards 100-1 bis 100-4) nicht im Widerspruch zum nativen ISO-27001-Standard stehen. Bei der schrittweise

unternehmensweiten Umsetzung wurden dann die Risikoanalysen für die unternehmenskritischen Werte („Assets“) aktualisiert.

Standardanforderungen umsetzen

Zunächst wurde das ISMS dahingehend optimiert, dass es die Anforderungen beider Standards erfüllt und die übergreifenden Aspekte der IT-Grundschutzmethodik und des BSI-Standards 100-1 vollständig abdeckt. Aufgrund der Annäherung des IT-Grundschutzes an die Norm „ISO 27001 (nativ)“ können zwischen den beiden Normen erhebliche Synergieeffekte erzielt werden. Das Unternehmen nutzte zur Dokumentation das so genannte GSTOOL des BSI (wobei durchaus vergleichbare Tools anderer Anbieter am Markt vertreten sind). GSTOOL ist ein datenbankgestütztes IT-Werkzeug, mit dem Standardanforderungen auf Basis des IT-Grundschutzes dokumentiert werden können. Das bestehende ISMS nach der nativen Norm wurde darauf geprüft, ob es auch die konkreten Vorgaben zum Standard „ISO 27001 auf der Basis IT-Grundschutz“ erfüllt. Dies gelang durch die konsequente Abarbeitung der übergreifenden Aspekte des IT-Grundschutzes.

Geltungsbereiche definieren

Bei seinen Aufträgen definiert das Unternehmen immer genau den jeweiligen Geltungsbereich („Scope“). Scopes, die Bestandteil von öffentlichen Aufträgen sind bzw. bei Aufträgen, die mit der Forderung nach IT-Grundschutz verbunden sind, setzt das Unternehmen die Methodik „ISO 27001 auf der Basis IT-Grundschutz“ immer vollständig um. Durch die exakte Definition der Scopes können die Aufwände dafür minimiert und Mittel projektspezifisch eingeplant werden. Es wird jeweils geprüft, ob vom Auftraggeber ein Audit oder eine Zertifizierung verlangt wird. Notwendige Zertifizierungen der Scopes führen dann zu entsprechenden jährlichen Aufwänden, die jeweils einzuplanen sind. Die pro Scope geforderten übergreifenden Aspekte können dabei mit einer zentralen Dokumentation gemäß BSI-Standards verknüpft werden.

Gleiche Kriterien festlegen

Um eine Vergleichbarkeit innerhalb des Unternehmens sicherzustellen, werden für beide Methoden gleiche Kriterien für den Schutzbedarf – also eine Einschätzung des kritischen Potenzials der betrachteten Prozesse, Informationen und IT-Komponenten – und die (Rest-) Risikoeinschätzung festgelegt. Dies ist notwendig, da der Unternehmensleitung mittlere bis hohe Risiken gemeldet werden müssen.

Assets transparent gestalten und Maßnahmen dokumentieren

Voraussetzung für die Konformität mit verschiedenen Standards ist, die für die Informationssicherheit relevanten Assets transparent zu gestalten. Außerdem müssen die Sicherheitsmaßnahmen in einem zentralen Verzeichnis („Repository“) dokumentiert und bearbeitet werden. Hier bietet sich der Einsatz von datenbankgestützten Werkzeugen an. Das Unternehmen hat das Strukturkonzept des bereits erwähnten GSTOOL ausgewählt, das unternehmensspezifische Bausteine erlaubt. Die bei den Risikoanalysen ermittelten Gefährdungen wurden aufgenommen und Verweise auf weiterführende Dokumente an zentraler Stelle gepflegt. Aus diesem Datenbestand können wesentliche Dokumentationen (halb-)automatisch generiert werden. Hilfreich ist, unternehmensspezifische Reports einzuführen, die an vorgegebene Layouts angepasst sind und unter anderem spezifische Nomenklaturen des Unternehmens berücksichtigen. Aufgrund der ISMS-Strategie des Unternehmens wurde damit die bestehende Dokumentation sukzessive vollständig datenbankbasiert abgebildet.

Audits durchführen

Eine wesentliche Forderung beim ISMS ist, Audits durchzuführen, um kontinuierliche Verbesserungsprozesse zu gewährleisten. Das Unternehmen hat sich dafür entschieden, jährlich interne Audits durchzuführen. Um auch hier aufwandsarm agieren zu können, hat das Unternehmen

systematisch Audits verschiedener Standards – also z. B. „ISO 9001“ und „ISO 27001“ – zusammengelegt. So mussten die betroffenen Fachabteilungen nicht mehrmals mit ähnlichen Fragestellungen in Anspruch genommen werden. Gemeinsam behandelt werden konnten unter anderem die Auditierung der internen Maßnahmenverfolgung, die Überprüfung der Wirksamkeit des Change-Management-Systems bei der Einführung informationssicherheitsrelevanter Assets oder das Dokumentenmanagement für relevante Dokumente des ISMS. Wichtig ist, dass auch das ISMS bzw. relevante Teilprozesse daraus den im ISO-9001-Standard geforderten internen Qualitätsmanagement-Audits unterzogen werden müssen.

Alle Maßnahmen listen und nachhalten

Um eine Nachverfolgung und fristgerechte Erledigung von offenen Maßnahmen sicherzustellen, wurden sämtliche Korrektur- und Verbesserungsmaßnahmen in einer übergreifenden Maßnahmenliste zusammengefasst und von der internen Organisationsabteilung nachgehalten.

Die geschilderten Maßnahmen haben für das Unternehmen zahlreiche Erkenntnisse gebracht, die größtenteils allgemeingültig sein dürften und die wir als Empfehlungen hier zusammenfassen können:

a. Wesentliche Voraussetzung für den erfolgreichen Aufbau eines ISMS ist, dass das Prozessdenken im Unternehmen etabliert ist. Optimalerweise sollte auch ein funktionierendes Qualitätsmanagementsystem nach „ISO 9001“ vorhanden sein. Ansonsten läuft man Gefahr, dass die Managementsysteme nicht gelebt werden.

b. Es sollten exakt die ISMS-Standards identifiziert werden, die die geschäftlichen Ziele des Unternehmens unterstützen. Nur dann kann eine optimale Kosten-Nutzen-Relation erreicht werden, die letztendlich die Voraussetzung zur Freigabe der benötigten Mittel ist. Damit wird dann auch die Umsetzung der Informationssicherheit im Unternehmen zu einem wichtigen Beitrag zum Geschäftserfolg.

c. Unternehmen sollten eine langfristige Strategie festlegen, wie sie unterschiedliche ISMS-Standards behandeln und die Vereinheitlichung wesentlicher Basisprozesse erreichen wollen. So lässt sich die Informationssicherheit wirtschaftlich betreiben.

d. Es ist zielführend, ein einheitliches ISMS zu definieren, das für alle ausgewählten Standards anwendbar ist. Nur so ist eine sinnvolle und tatsächlich gelebte Implementierung möglich. Die dafür definierten Prozesse müssen unternehmensweite Gültigkeit besitzen, damit keine verschiedenen Prozesswelten aufgebaut werden müssen. Hierbei ist die Unterstützung externer Sicherheitsdienstleister zu empfehlen. Fehler auf dieser Ebene können die angestrebten Zertifizierungen ernsthaft gefährden.

e. Um zunächst mehrere Standards parallel betreiben zu können, müssen die spezifischen Anwendungsbereiche (Scopes) für die jeweiligen Standards eindeutig identifiziert werden. So lassen sich Unsicherheiten bzw. Fehler bei der Gültigkeit von Methoden und Vorgaben vermeiden.

f. Standardübergreifende Kriterien und Normen, um das kritische Potenzial von Unternehmenswerten bewerten und Risikoanalysen durchführen zu können, sind nötig, um eine unternehmensweite Vergleichbarkeit nicht zu verlieren. Das gilt auch für die Umsetzung verschiedener Standards.

g. Eine zentrale Verzeichnisdatenbank für die relevanten Sicherheitsmaßnahmen und Sicherheitsdokumente hilft dabei, die umgesetzten Sicherheitsmaßnahmen unternehmensweit transparent zu machen. Die Datenbank dient als Quelle der für die verschiedenen Sicherheitsstandards zu referenzierenden Sicherheitsmaßnahmen.

h. Letztendlich darf nicht vergessen werden, einen standardübergreifenden Evaluierungsprozess und eine zentrale Maßnahmenverfolgung zu etablieren. So können mit einem überschaubaren wirtschaftlichen

Aufwand die verschiedenen Anwendungsbereiche kontinuierlich verbessert werden.

Fazit

Die Umsetzung unterschiedlicher Standards im Unternehmen ist auch mit begrenzten personellen Ressourcen möglich, wenn bestimmte Rahmenbedingungen geschaffen werden. Dafür müssen die Geltungsbereiche definiert und bei der Zertifizierungs- bzw. ISMS-Strategie die prozessualen Synergien ausgenutzt werden. Außerdem ist eine einheitliche Dokumentationsplattform nötig.

6 Wichtige Institutionen (International / National)

DIN Deutsches Institut für Normung e. V., Burggrafenstraße 6, 10787 Berlin, URL: www.din.de

International Organization for Standardization, ISO Central Secretariat, 1, ch. de la Voie-Creuse, CP 56
CH-1211 Geneva 20, Switzerland, URL: www.iso.org

Bundesamt für Sicherheit in der Informationstechnik (BSI), Postfach 20 03 63, 53133 Bonn, URL: www.bsi.bund.de

DAkkS Deutsche Akkreditierungsstelle GmbH, Spittelmarkt 10, 10117 Berlin, URL: www.dakks.de

INTERNATIONAL ACCREDITATION FORUM INC. (IAF), Norbert Borzek, Chair of Technical Committee, c/o DAkkS Deutsche Akkreditierungsstelle GmbH, URL: www.iaf.nu

7 Danksagung

Der vorliegende Leitfaden entstand in der BITKOM-Projektgruppe „Zertifizierung von Informationssicherheit in Unternehmen“ des Kompetenzbereiches Sicherheit.

Wir danken allen Mitgliedern der Projektgruppe und des Arbeitskreises Sicherheitsmanagement für das kontinuierliche Interesse am Thema und die zahlreichen Anregungen. Besonderer Dank gilt Herrn Professor Rainer Rumpel, dem Sprecher der Projektgruppe, für sein außerordentliches Engagement bei der Fertigstellung des Leitfadens sowie bei der Leitung des Projektes. Unser Dank gilt weiterhin den federführenden Autoren für die zahlreichen Textbeiträge, die diesen Leitfaden erst ermöglichten:

- Arnd Chrostowsk, KPMG AG Wirtschaftsprüfungsgesellschaft
- Ulf Greifzu, IBM Deutschland GmbH
- Frank Hebestreit, IBM Deutschland GmbH
- Lutz Neugebauer, BITKOM e.V.
- Peter Pakosch, Toll Mobile GmbH & Co. KG
- Holger Rieger, Bundesdruckerei GmbH
- Prof. Dr. Rainer Rumpel, Persicon cert AG:

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.350 Unternehmen, davon über 1.000 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org