Vorwort

Zum Inhalt

Die Sicherheit der Information und der informationsverarbeitenden Prozesse wird heute immer mehr zu einem Eckpfeiler der Unternehmensvorsorge.

Image, Geschäftserfolg und Unternehmensstabilität hängen in entscheidendem Maße von qualifizierten Management-Prozessen und Management-Systemen ab – sei es, dass solche

- von Aufsichtsbehörden gefordert,
- von Geschäftspartnern erwartet,
- von Kunden wohlwollend bei Kaufentscheidungen berücksichtigt,
- bei Ausschreibungen sogar verbindlich vorgeschrieben werden oder
- zur Bewertung von Kreditwürdigkeit und Versicherungsrisiken (Stichwörter Basel II/III, Solvency II) erforderlich sind.

Management-Standard

Die sich hieraus ergebenden Anforderungen wurden bereits in der Vergangenheit in Management-Standards zusammengefasst, z. B. die ISO 9000-Reihe für das Qualitätsmanagement, die ISO 14000-Reihe für das Umweltschutzmanagement und die ISO 20000 für das IT-Service-Management.

Im vorliegenden Buch wird das Management der *Informationssicherheit* auf der Basis der Normenreihe ISO 27000 erläutert. Informationssicherheit umfasst neben IT-Sicherheit und Datenschutz *alle* mit der Sicherheit von Informationen zusammenhängenden Aspekte einer Organisation.

Es richtet sich an Leser, die

- sich für die genannten Standards interessieren,
- mit der Einrichtung eines entsprechenden Management-Systems in einer Organisation beauftragt sind,
- IT-Sicherheitsbeauftragter (IT Security Manager) sind,
- zum IT-Sicherheitsmanagement in anderen Funktionen beitragen,
- in der Leitungsebene einer Organisation solche Management-Systeme überwachen,

- das Informationssicherheitsmanagement-System (ISMS) ihrer Organisation zertifizieren lassen wollen,
- Beratungen zu Management-Systemen durchführen,
- Management-Systeme prüfen und auditieren.

In diesem Buch werden vor allem die Inhalte des Standards ISO 27001 exemplarisch erläutert, weil nach dieser Norm zertifiziert werden kann. Der Leser wird Schritt für Schritt bei der Herstellung von Konformität zu diesem Standard angeleitet und begleitet. Bei der Darstellung werden auch wesentliche Inhalte der begleitenden Normen aus der ISO 27000-Reihe berücksichtigt, die wichtige Elemente eines ISMS vertiefen und beispielhafte Interpretationen der Normtexte liefern – etwa die ISO 27002 und die ISO 27003.

Mindest-anforderungen

Anforderungskataloge an Management-Systeme gewinnen in der Standardisierung immer mehr an Bedeutung. Sie werden darüber hinaus in Gesetzen und Ausschreibungstexten herangezogen, um Management-Strukturen und Prozess-Modelle in abstrakter Weise (unabhängig vom jeweiligen Kontext) festlegen zu können.

Ebenso wie im Umwelt-, Qualitäts- und IT-Service-Management wurden auch beim Management der Informationssicherheit keine standardisierten Management-Systeme festgelegt, sondern lediglich *Mindestanforderungen* aufgestellt.

Tailoring

Die Anwendung solcher Anforderungskataloge auf eine Organisation erfordert ein exaktes Maßnehmen, Zuschneiden und Verknüpfen (Tailoring) der Einzelaspekte zu einem auf die Organisation zugeschnittenen Management-System. Bei diesem Tailoring muss eine Organisation das Ziel verfolgen, die Anforderungen aus den verschiedenen Standards zweckentsprechend zu interpretieren und zu harmonisieren, um so effiziente und effektive Strukturen, Prozess-Modelle und Management-Aktivitäten festzulegen.

Ein derartiges Tailoring ist wegen seiner tief greifenden Implikationen nicht ohne ein hohes Maß an Engagement des Top Managements der Organisation durchführbar.

Kopiert man dagegen Management-Systeme anderer Organisationen oder beschränkt sich auf das formale Erfüllen von Zertifizierungsnormen, so wird einem die leidvolle Erfahrung (z. B. aus der Anwendung der ISO 9000-Reihe) nicht erspart bleiben, eine überbordende Bürokratisierung, aber eben keinen für die Organisation nutzbringenden Ansatz gewählt zu haben.

Risikoanalyse Die Risikobetrachtung ist ein wesentlicher Grundpfeiler der Informationssicherheit. Sie ist Gegenstand der ISO 27005 und wird in Kapitel 6 dieses Buches an Beispielen erläutert.

Darunter findet sich auch ein Abschnitt zur *monetären Einschätzung von Risiken*, um dieses in der Praxis oft auftauchende Thema zu unterfüttern.

Maßnahmen Einen erheblichen Umfang nimmt das Kapitel 7 *Maßnahmenziele und Maßnahmen bearbeiten* ein, in dem die einzelnen Controls aus dem Anhang der ISO 27001 kommentiert und mit Beispielen versehen sind.

Bei allen Aspekten wird auch die Verbindung zum Maßnahmenkatalog des IT-Grundschutzes (siehe unten) behandelt.

Validieren Das Kapitel 8 *Maßnahmen: Validieren und Freigeben* beschreibt, wie mögliche Maßnahmen-Alternativen nach verschiedenen Faktoren bewertet werden können, bevor eine Alternative ausgewählt und für die Umsetzung freigegeben wird.

Kennzahlen Für das Normerfordernis, die Leistungsfähigkeit bzw. Wirksamkeit der ergriffenen Sicherheitsmaßnahmen zu beurteilen, sind seit geraumer Zeit Ansätze für Metriken und Kennzahlen in der Diskussion. Dieses Thema wird Kapitel 9 dieses Buches behandelt und orientiert sich an ISO 27004.

Audits Die Normen ISO 27006, 27007 und 27008 befassen sich mit Audits und Zertifizierungen. Im vorliegenden Buch werden dazu in Kap. 10 umfangreiche praktische Hinweise gegeben, darunter ein Abschnitt mit Erfahrungen aus realen Audits.

Leitlinien Im *Anhang* dieses Buches wird ein kommentiertes Beispiel für eine Informationssicherheitsleitlinie wiedergegeben. Dieses Beispiel dient der Erläuterung der Sachverhalte an einem sehr einfach gestrickten Fall, kann aber durchaus als Ausgangspunkt für reale Leitlinien angesehen werden.

IT-Grundschutz In Deutschland bzw. im deutschsprachigen Raum ist die Anwendung des IT-Grundschutzes des BSI verbreitet. Inzwischen wurde dessen Vorgehensmodell ebenfalls nach der ISO 27000-Reihe ausgerichtet. Der IT-Grundschutz mit seinen Baustein- und Maßnahmenkatalogen kann sehr hilfreich sein, um die Anforderungen des Standards vor allem auf der Maßnahmenseite zu konkretisieren. Insofern wird in diesem Buch auch beschrieben, wie der IT-Grundschutz bei dem Bemühen um Konformität zu ISO 27001 helfen kann.

Änderungen in der 4. Auflage

In dieser 4. Auflage sind folgende Ergänzungen vorgenommen worden:

- Aktualisierung aller Angaben zu Gesetzen, Richtlinien und Normen.
- Informationen über den aktuellen Stand des Ausbaus der ISO 27000-Reihe.
- Das Thema *Datenschutz* (personenbezogener Daten) wird durch viele Hinweise vertieft.
- Die Erläuterungen zu den Controls aus Anhang A der ISO 27001 wurden aktualisiert und ergänzt.
- Die vom BSI herausgegebene *Auslagerungsrichtlinie* wird im Zusammenhang mit der Grundschutz-Zertifizierung näher behandelt; sie enthält u. a. Anforderungen an Auftragnehmer bei der Vergabe von Aufträgen (Outsourcing) durch öffentliche Stellen.

Wichtige Hinweise

Nicht zuletzt wegen der zunehmenden Berücksichtigung der ISO 27001 in der Unternehmenspraxis, die die Autoren in ihrer beruflichen Tätigkeit als Auditoren und Zertifizierer feststellen konnten, haben sich einige Checklisten als nützlich erwiesen, in denen wichtige Schritte im Sicherheitsprozess tabellarisch abgebildet worden sind. Die Checklisten sind über den Verlag erhältlich[1].

Das vorliegende Buch versteht sich *nicht* als Einführung in die Informationssicherheit. Grundbegriffe und Grundstrukturen in dem hier verstandenen Sinne findet man z. B. in dem Buch *Der IT Security Manager*[2]. Da die genannten Standards jedoch eigene Begrifflichkeiten verwenden, werden wir diese in einem einführenden Abschnitt behandeln und den klassischen Begriffen gegenüberstellen.

---

1 http://www.springer.com/springer+vieweg; nach dem vorliegenden Buch suchen und auf den Auswahlpunkt „ZUSÄTZLICHE INFORMATIONEN“ klicken!

2 3. Auflage erschienen 2012 im gleichen Verlag.

Danksagung

Allen Lesern herzlichen Dank für die vielen Anregungen zu den früheren Auflagen. Die vorliegende vierte Auflage des Buches entstand mit tatkräftiger Unterstützung des Verlags Springer Vieweg. Vielen Dank an Herrn Hansemann und das gesamte Lektorat IT/Informatik.

Im Februar 2013
Heinrich Kersten, Jürgen Reuter, Klaus-Werner Schröder

http://www.springer.com/978-3-658-01723-1

IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz

Der Weg zur Zertifizierung

Kersten, H.; Reuter, J.; Schröder, K.-W. - Kersten, H.; Wolfenstetter, K.-D. (Hrsg.)

2013, XIII, 377 S. 4 Abb., Softcover
ISBN: 978-3-658-01723-1