



Das Informationssicherheitsmanagementsystem von BS 7799-2:2002

Das Managementsystem zu ISO 17799

Ein Beitrag von Andreas E. Fiedler

Einleitung

Durch die Veröffentlichung des Standards ISO 17799 ist eine internationale Basis für ein gemeinsames Verständnis zum Management der Informationssicherheit geschaffen worden. ISO 17799 wurde als ein Standard entwickelt, dessen Managementsystemmodell sicherstellen soll, daß in einer Organisationen geeignete Maßnahmen getroffen werden, um Speicherung und Transfer von Daten sicher zu gestalten - unbeschadet ob Daten in elektronischer oder Papierform vorliegen.

ISO 17799 "Code of Practice for Information Security Management" nennt als Steuerungsbereiche für diese Maßnahmen:

- Sicherheitspolitik
- Organisation der Sicherheit
- Einstufung und Kontrolle der Werte
- Personelle Sicherheit
- Physische und umgebungsbezogene Sicherheit

- Management der Kommunikation und des Betriebs
- Zugangskontrolle
- Systementwicklung und -wartung
- Management des kontinuierlichen Geschäftsbetriebs
- Einhaltung der Verpflichtungen

Nachdem der inhaltliche Rahmen des Managements von Informationssicherheit gesetzt ist, ergibt sich zwangsläufig die Frage nach dem Managementsystem, welches das Management der Informationssicherheit leisten soll. Wie sieht ein solches Managementsystem aus?

BS 7799-2:2002

Der Standard ISO 17799 ist aus dem britischen Standard BS 7799 hervorgegangen. Im Unterschied zu BS 7799, der aus zwei Teilen besteht, hat die ISO 17799 nur den ersten Teil des BS 7799 übernommen.



BS 7799-2 befaßt sich mit der Fragestellung nach dem Managementsystem. Es werden vier große Bereiche angesprochen:

- das Informationssicherheitsmanagementsystem (ISMS)
- die Verantwortung des Managements
- das Management Review
- die Verbesserung des ISMS

Aus Managementsicht lassen sich diese Bereiche zu zwei Bausteinen zusammenfassen:

- das Managementsteuerungssystem: es umfaßt die Dokumentation, das Audit und das Review, die Verantwortung des Managements, Korrektur- und Vorbeugungsmaßnahmen sowie die kontinuierliche Verbesserung.
- das Management der Informationssicherheit: das meint die Prozesse des PDCA-Zyklus zur Erstellung, Durchführung, Überwachung und Verbesserung des desselben.

Das Management der Informationssicherheit

Übersicht

Nicht nur, um Übereinstimmung mit anderen Managementstandards wie ISO 9000 oder ISO 14000 zu erreichen, wurde das PCDA (Plan-Do-Check-Act)-Modell als Basis für die Revision des BS 7799 gewählt. Vielmehr spiegelt sich in der Übernahme dieses Modells, welches seinen Ursprung im Qualitätsmanagement hat, ein konsequentes Prozeßdenken wieder.

Die Phasen oder Aktivitäten des PDCA-Zyklus sind:

- PLAN: Aufbau des ISMS
- DO: Betrieb des ISMS
- CHECK: Überwachung und Überprüfung des ISMS
- ACT: Verbesserung des ISMS

PLAN

Die Planungsphase befaßt sich mit dem Aufbau des ISMS. Zunächst ist der Umfang des ISMS zu bestimmen, also der Gegenstand, der durch das ISMS betreut wird. Für das ISMS muß eine ISMS-Politik Aufschluß über Zielsetzung, gesetzliche Gebundenheiten, Risikomanagementkontext und Risikobewertungskriterien geben.

Es bedarf eines systematischen Risikomanagementansatzes. Zu diesem Zweck können hier der weit über Australien und Neuseeland bekannt gewordene Standard AS/NZS 4360:1999 oder auch der in UK veröffentlichte Standard AIRMIC, ALARM, IRM:2000 unterstützend sein.

Anmerkung: Dieser Standard ist eine gemeinsame Entwicklung von dem Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) und ALARM The National Forum for Risk Management in the Public Sector.

Das Risikomanagement im Rahmen des ISMS besteht aus sechs Schritten:

1. Risikoidentifikation

In diesem Schritt werden zunächst die Gegenstände der Risikountersuchung bestimmt und welchen Bedrohungen diese unterliegen. Weiter sind die



Schwachstellen, die durch die Bedrohungen betroffen sind, sowie die Bedeutung der möglichen Schäden zu identifizieren.

2. Risikobewertung

Die Risikobewertung untersucht typischerweise zwei Parameter: die Wahrscheinlichkeit des Eintritts des Risikos sowie die Auswirkung im Fall des Eintritts des Risikos.

Die FMEA bietet einen dritten, sehr interessanten Parameter: die Entdeckungswahrscheinlichkeit. Damit ist die Wahrscheinlichkeit gemeint, daß der Eintritt einer Bedrohung durch Entdeckungsmaßnahmen erkannt wird, bevor Auswirkungen größeren Umfangs eintreten. Ein Beispiel für Entdeckungsmaßnahmen sind zum Beispiel Virensensoren oder Schwachstellentests im Netzwerk.

3. Maßnahmenidentifikation und -bewertung

Es gibt verschiedene Möglichkeiten, auf Risiken zu reagieren, darunter:

- Maßnahmen ergreifen
- Risiko akzeptieren
- Risiko umgehen
- Risiko auf Dritte übertragen

4. Steuerung der Risikomaßnahmen

ISO 17799 zeigt eine Reihe von Steuerungsbereichen auf, die allerdings nicht abschließend sind. Die Steuerung ist darzulegen und an Hand der Ergebnisse der Risikobewertung zu begründen.

5. Statement of Applicability

In dem Statement zur Anwendbarkeit werden die in Ziffer 4 benannten Steuerungen dokumentiert.

6. Managementfreigabe

Das Management muß seine Zustimmung zur Implementierung des ISMS geben. Die Verantwortlichkeit des Management ist ein entscheidender Aspekt für den Erfolg des ISMS. (s. dazu unten)

DO

Die DO-Phase befaßt sich mit der Umsetzung der Planung. In dieser Phase kommen Tätigkeiten des Projektmanagements zum Einsatz, um das ISMS aufzubauen. Das sind unter anderem:

- Management der Planumsetzung
- Ressourcenmanagement
- Zeitmanagement
- Schulungsmanagement

CHECK

In der CHECK-Phase geht es um die Überwachung und Überprüfung des ISMS.

1. Überwachung

Die Überwachung des laufenden Betriebs des ISMS beinhaltet das Aufspüren von Verfahrensfehlern, die Überwachung der ISMS-Aktivitäten, Sicherheitsverletzungen, Maßnahmenverfolgung bei Sicherheitsverletzungen.

2. Überprüfung

Die Effektivität des ISMS sollte regelmäßig im Rahmen eines Reviews überprüft werden. Gegenstand eines solchen Reviews sind:

- Sicherheitspolitik und -ziele



- Audits
- Vorkommnisse
- Verbesserungsvorschläge
- Feedback

3. Restrisiko

Das verbleibende und akzeptierte Risiko ist regelmäßig in Hinblick auf die Auswirkungen auf die Organisation, die Technologie, die Geschäftsziele und -prozesse, identifizierte Bedrohungen und externe Effekte wie die Rechtslage oder die gesellschaftliche Wahrnehmung zu überprüfen.

ACT

Die ACT-Phase ist die Phase der Verbesserung. In dieser Phase werden kontinuierlich Verbesserungen implementiert, Korrektur- und Vorbeugungsmaßnahmen ergriffen, die Ergebnisse mit allen betroffenen Parteien kommuniziert und diskutiert sowie die Umsetzung der Verbesserungsmaßnahmen überwacht.

Das Managementsteuerungssystem

Das Managementsteuerungssystem umfaßt:

- die Dokumentlenkung
- das Audit
- das Review
- die Verantwortung des Managements
- Korrektur- und Vorbeugungsmaßnahmen
- die kontinuierliche Verbesserung

Die Dokumentlenkung

Die Dokumentlenkung des ISMS ist identisch zu der des Qualitätsmanagements. Daher haben Organisationen, die eine Dokumentlenkung entsprechend der ISO 9000:2000 implementiert haben, die Anforderung von BS 7799-2, was das Verfahren der Dokumentlenkung anbetrifft, bereits erfüllt. Die einzelnen Verfahrensschritte sind:

- Genehmigung der Dokumente vor Herausgabe
- Überprüfung, Aktualisierung und erneute Genehmigung der Dokumente
- Versions- und Änderungskontrolle
- Verfügbarkeit der Dokumente, wo sie benötigt werden
- lesbare und identifizierbare Dokumente
- Identifikation externer Dokumente
- kontrollierte Verteilung der Dokumente
- Entfernung obsoleter Dokumente
- Identifikation obsoleter Dokumente, falls diese wieder benötigt werden.

BS 7799-2 nennt Dokumenttypen, die Bestandteil des ISMS sein sollen:

- Statements der Sicherheitspolitik und der Sicherheitsziele
- Umfang, Verfahren und Steuerungsmaßnahmen des ISMS
- Risikobewertungsbericht
- Risikomaßnahmenplan
- Verfahren zur effektiven Planung, Durchführung und Kontrolle des Informationssicherheitsprozesses
- Aufzeichnungen (s.u.)
- Statement of Applicability



Lenkung der Aufzeichnungen

Aufzeichnungen müssen erstellt und als Nachweis der Erfüllung der Anforderungen und des effektiven Ablaufs des ISMS vorgehalten werden. Es gelten analog wiederum die Anforderungen des Qualitätsmanagements.

Das Verfahren zur Lenkung der Aufzeichnungen muß dokumentiert sein:

- Identifikation
- Aufbewahrungsort
- Schutz
- Wiedererlangung
- Aufbewahrungsfrist
- Ablage

Das interne Audit

Das interne Audit spielt eine zentrale Rolle bei dem Bestreben nach Aufrechterhaltung der Informationssicherheit und kontinuierlicher Verbesserung. Audits sind planmäßige Überprüfungen der Einhaltung sowie die effektive Umsetzung der festgeschriebenen Verfahren. Dabei werden die zuvor identifizierten Informationssicherheitsanforderungen auf ihre fortwährende Eignung geprüft. Die Ergebnisse von Audits sind:

- aktuelle Mängel (vgl. unten: Korrekturmaßnahmen)
- potentielle Mängel (vgl. unten: Vorbeugungsmaßnahmen)
- Verbesserungsmöglichkeiten (vgl. unten: kontinuierliche Verbesserung)

Die Auditaktivitäten umfassen:

- Definition der Auditziele
- Überprüfung der Dokumente
- Auditplanung

- Auditdurchführung
- Auditergebnisbericht
- Abschluß aller geplanten Auditaktivitäten
- Follow-Up-Audits bei Mängeln

Unternehmen, die ein funktionierendes Qualitätsmanagementsystem unterhalten, können die Auditfunktion des ISMS sehr einfach mit dem des Qualitätsmanagements zusammenführen.

Das Management Review

Analog dem Management Review des Qualitätsmanagements hat das Management ein Review des ISMS durchzuführen, um die fortlaufende Eignung und Effektivität des ISMS zu bestätigen.

Gegenstand des Reviews sind unter anderem Audit- und Reviewergebnisse, Korrektur- und Vorbeugungsmaßnahmen, Verbesserungsvorschläge, neue Techniken und Verfahren.

Ergebnisse des Reviews sind die Korrekturen und Verbesserungen des ISMS sowie die notwendigen Ressourcenbereitstellungen.

Die Verantwortung des Managements

Ein sehr bedeutendes und häufig vernachlässigtes Element des Managementsteuerungssystems ist die Verantwortung des Managements. Sie erstreckt sich auf drei Bereiche:

- das Management Commitment
- das Ressourcenmanagement



- Schulung, Schaffung eines IS-Bewußtsein und Kompetenzen

Management Commitment

Das Management Commitment ist wie in anderen Managementsystemen einer der kritischen Erfolgsfaktoren. Dem Management kommen insbesondere die folgenden Aufgaben zu:

- Entwicklung der Informationssicherheitspolitik
- Überwachung der Entwicklung der Informationssicherheitsziele und der Planung
- Zuordnung von Aufgaben und Verantwortlichkeiten
- Kommunikation der Bedeutung der Informationssicherheit
- Bereitstellung der für das ISMS notwendigen Ressourcen (s.u.)
- Entscheidung über Risikoakzeptanz
- Durchführung von Management Reviews

Ressourcenmanagement

Das Management ist verantwortlich, daß ausreichend Ressourcen bereitgestellt werden, um:

- das ISMS zu planen, durchzuführen und zu erhalten
- sicherzustellen, daß die Verfahren des ISMS in Einklang mit den Geschäftsanforderungen stehen
- sicherzustellen, daß gesetzliche und vertragliche Verpflichtungen eingehalten werden
- sicherzustellen, daß die Informationssicherheit durch geeignete Steuerungsmaßnahmen aufrecht erhalten wird

- Reviews durchzuführen und entsprechend der Review-Ergebnisse Maßnahmen zu ergreifen
- das ISMS kontinuierlich zu verbessern

Schulung, Schaffung eines IS-Bewußtsein und Kompetenzen

Das Management ist verantwortlich, daß das für das ISMS verantwortliche Personal ausreichend geschult ist. Konkret:

- die Feststellung der benötigten Kompetenzen
- Durchführung von Schulungen
- Bewertung der Effektivität von Schulungen
- Aufzeichnungen über Schulungen, Erfahrungen, Qualifikationen und Fähigkeiten.

Korrektur- und Vorbeugungsmaßnahmen

Interne Audits, aber auch andere interne wie externe Quellen geben Aufschluß über die Funktionsfähigkeit des ISMS. Treten Mängel auf, werden Maßnahmen eingeleitet, um die Mängel zu beseitigen und vor allem auch um die Wiederholung eines Mangels zu verhindern. In Hinblick auf das Managementsystem sind zwei Maßnahmentypen von Bedeutung: Korrekturmaßnahmen und Vorbeugungsmaßnahmen.

Korrekturmaßnahmen sind Maßnahmen, die nach Eintritt eines Risikos bzw. eines Mangels getroffen werden, um dem Schaden zukünftig vorzubeugen.

Vorbeugungsmaßnahmen dienen der Antizipation von möglichen Mängeln oder Risiken und sollen einen potentiellen



Schaden verhindern, bevor überhaupt ein konkreter Fall eingetreten ist.

Die kontinuierliche Verbesserung des ISMS

ISO 9000:2000 wie BS 7799-2 benennen neben den erwähnten Korrektur- und Vorbeugungsmaßnahmen noch die kontinuierliche Verbesserung. Während Korrektur- und Vorbeugungsmaßnahmen auf konkret bestehende bzw. potentielle Mängel abzielen, gibt es weiter auch Möglichkeiten, ein mangelfreies, an sich funktionierendes System in dessen Effektivität und Effizienz weiter zu verbessern.

Die kontinuierliche Suche nach Verbesserungen ohne Fehler oder Mängel als Grundlage ist für ein erfolgreiches Managementsystem von großer Bedeutung. Es ist der Schritt vom reaktiven zum proaktiven Management.

Die einzelnen Schritte der kontinuierlichen Verbesserung sind:

- Identifikation möglicher Verbesserungsbereiche
- Analyse und Begründung der notwendigen Maßnahmen
- Feststellung der Verfügbarkeit der Ressourcen
- Entscheidung über die Umsetzung der Verbesserung
- Implementierung der Verbesserung
- Messung des Einflusses auf die Organisation
- Diskussion der Ergebnisse im Management Review
- permanente Ausschau nach neuen Verbesserungsmöglichkeiten

Schlußfolgerungen

BS 7799-2 legt ein Informationssicherheitsmanagementsystem vor, welches es bedarf, um Informationssicherheit, wie ISO 17799 sie bestimmt, zu gewährleisten. Die Nähe zu ISO 9000:2000 ist unübersehbar und ein wichtiger Aspekt zur effizienten Gestaltung des Systems.

BS 7799-2 ist für Organisationen eine sehr wichtige Ergänzung, da dieser Standard für eine Einordnung der Informationssicherheitsmaßnahmen in ein Managementsystem sorgt. Ein solches Managementsystem ist eine Grundvoraussetzung für Erfolg bei der Informationssicherheit.

Im Gegensatz zu ISO 17799 bietet BS 7799-2 Organisationen zudem die Möglichkeit, sich das ISMS zertifizieren zu lassen und somit den eigenen Einsatz für Informationssicherheit zu kommunizieren.