Bild: Pixabay

Die Norm ISO 27006 gibt die Anforderungen an die Zertifizierungsstellen vor.

ISO 27006 – Anforderungen an die Zertifizierer

Während die ISO 27001 die Anforderungen an das Informationssicherheitsmanagementsystems eines Unternehmens definiert, gibt die ISO 27006 die Anforderungen an die Zertifizierungsstellen vor. Doch nicht nur für diese ist ein Blick in die Norm spannend.

Als Grundlage für die gesamte Norm wird die ISO 17021-1 (Konformitätsbewertung – Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren) verwendet. Die ISO 27006 erweitert diese an vielen Stellen um die Informationssicherheitsaspekte.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Vermeidung von potenziellen Interessenkonflikten

Das Kapitel 5 geht auf die Rechts- und Vertragsfragen ein. Ein wichtiger Aspekt ist die Vermeidung von potenziellen Interessenkonflikten. Dies beginnt bereits bei Schulungen. Diese dürfen sich nicht auf das Unternehmen und das dazugehörende Managementsystem beziehen. Auch konkrete Empfehlungen oder unternehmensspezifische Ratschläge verstossen gegen die Unabhängigkeit. Das Aufzeigen von Verbesserungsmöglichkeiten ist hingegen erlaubt und bietet einen Mehrwert während des Zertifizierungsaudits.

Ein wichtiger Aspekt sind die Kompetenzanforderungen für ISMS-Audits. Das Kapitel 7.1.2 geht näher darauf ein. Dazu gehören:

- Kenntnis der Informationssicherheit;
- Kenntnis der Managementsysteme;
- technisches Wissen in Bezug auf die Tätigkeit, die auditiert werden soll;
- Kenntnis der Auditgrundsätze; (die ISO 19011 geht ausführlich darauf ein)
- Kenntnis der ISMS-Überwachung, -Messung, -Analyse und -Beurteilung.

Viele Zertifizierungsstellen arbeiten aus diesen Gründen mit externen Spezialisten zusammen. Sie verfügen über eine angemessene Arbeitserfahrung. Einige Stellen erwarten sogar, dass der Auditor bereits im Sektor des zu auditierenden Unternehmens gearbeitet hat. Damit können die Anforderungen der Norm, das Wissen über gesetzliche und behördliche Anforderungen im jeweiligen Informationssicherheitsgebiet, das jeweilige geographische Gebiet und das jeweilige Rechtssystem, die mit dem Geschäftsfeld zusammenhängenden Informationssicherheitsrisiken sowie die Prozesse und die Technologien erfüllt werden.

Weiter wird gefordert, dass die Struktur und der Inhalt der Norm sowie die ISMS-Prozesse bekannt und Methoden zur Risikobewertung und -management verstanden sind. Auch aktuelle Technologien, die zu Problemen führen können, müssen erkannt werden.

Über das notwendige Wissen verfügen

Bevor die Audit-Resultate nach dem Audit an den Kunden gehen, werden sie nochmals von einer unabhängigen Person der Zertifizierungsstelle geprüft. Auch diese Person muss über das notwendige Wissen verfügen, um geeignete Zertifizierungsentscheidungen treffen zu können.

Die Zertifizierungsstelle muss über einen Nachweis über jede eingesetzte Person verfügen, in der hervorgeht, dass die Auditoren über Wissen und Erfahrung verfügen. Dies können ISMS-spezifische Qualifikationen, Registrierung als Auditor, Teilnahme an ISMS-Schulungen und Aufzeichnungen der beruflichen Entwicklung sein. Die ISO 27006 verlangt dabei, dass Auditoren über eine Ausbildung oder Schulung auf einem mit einer universitären Ausbildung vergleichbaren Niveau, mindestens vierjährige praktische Vollzeitberufserfahrung, inkl. mindestens zwei Jahre in der Informationssicherheit, eine mindestens fünftägige Schulung erfolgreich absolviert und über Erfahrung zum Auditieren eines ISMS verfügen.

Geprüft werden diese Vorgaben in der Schweiz durch die SAS, die Schweizerische Akkreditierungsstelle (www.sas.admin.ch). Sie prüft die vorhandenen schriftlichen Nachweise und begleitet unregelmässig die Auditoren bei ihrer Arbeit. Als Kunde kann dies nicht verhindert werden und wird bereits in der Vereinbarung so erwähnt.

Ein wichtiger Punkt bei der Planung eines Audits ist der benötigte Zeitaufwand. Zertifizie-

rungsstellen müssen Auditoren genügend Zeit geben, um alle Tätigkeiten in Bezug auf ein Erstaudit, ein Überwachungsaudit oder ein Re-Zertifizierungsaudit auszuführen. In die Berechnung des Gesamtauditzeitaufwands muss auch genügend Zeit für die Auditberichterstattung enthalten sein. Der Anhang B listet in einer Tabelle auf, wie viele Audittage eingeplant werden müssen. Ein wichtiger Faktor ist dabei die Anzahl Vollzeitstellen im Anwendungsbereich. Als Beispiel muss für ein Unternehmen zwischen 16 und 25 Mitarbeitenden mit einem Aufwand von 7 Tagen für das Erst-Audit gerechnet werden. Die Auditzeitaufwandtabelle darf jedoch nicht isoliert verwendet werden. Berücksichtigt werden müssen die Komplexität des ISMS, die getätigten Geschäfte, die Grösse und Komplexität der IT-Umgebung, die Art und Nutzung von externen Dienstleistungen wie der Cloud sowie die Anzahl der Standorte und Anzahl der Notfallwiederherstellungsstandorte. Die Norm erwähnt auch komplizierte Logistik, fremdsprachiges Personal (wodurch Dolmetscher erforderlich werden oder einzelne Auditoren nicht unabhängig arbeiten können) sowie eine grosse Anzahl an Normen und Vorschriften, die für das ISMS gelten. Der Anhang C listet die erwähnten Punkte auf und gibt Beispiele, wann ein verringerter, normaler oder erhöhter Aufwand gilt. Damit dies berechnet und eine Offerte erstellt werden kann, verschicken die Zertifizierungsstellen im vornherein einen kurzen Fragebogen. Anhand der Antworten kann anschliessend die gewünschte Offerte erstellt und dem Kunden zugestellt werden.

Auch Remote-Audits lässt die Norm zu

Bei grösseren Unternehmen kann es der Fall sein, dass mehrere Standorte geprüft werden müssen. Die Norm erlaubt in diesem Fall, dass Zertifizierungsstellen einen stichprobenbasierten Ansatz erwägen. Die Norm listet 13 Punkte auf, die bei der Planung und Durchführung berücksichtigt werden müssen. Möglich ist auch, dass beim Erst-Audit der Hauptstandort geprüft und in jedem Aufrecht- oder Rezertifizierungsaudit ein anderer Standort an der Reihe ist.

Auch Remote-Audits lässt die Norm zu. Gerade während der Corona-Pandemie mussten die Zertifizierungsstellen auf diese Möglichkeit ausweichen. Die Norm erlaubt aber nur eine maximale Dauer von 30 Prozent des gesamten geplanten Zeitaufwands. Wird mehr benötigt, muss die Zertifizierungsstelle den Auditplan begründen und vor dessen Umsetzung eine spezielle Genehmigung seitens der Akkreditierungsstelle einholen.

Bei Unternehmen, die nicht nur eine Norm überprüfen lassen möchten (zum Beispiel ISO 9001, ISO 14001, ISO 27701 zusätzlich zu ISO 27001), ist eine Kombination möglich, vorausgesetzt, dass nachgewiesen werden kann, dass das Audit alle Anforderungen an die Zertifizierung des ISMS erfüllt. Wichtig ist auch, dass die eingesetzten Auditoren über die entsprechende Qualifizierung und Erfahrung verfügen. Auch ein Audit mit mehreren Auditoren ist denkbar. Jedoch kann nur ein Auditor den Lead haben.

Das Erst-Audit wird in zwei Stufen durchgeführt. In der ersten wird die Dokumentation des ISMS geprüft. Die Zertifizierungsstelle muss ein ausreichendes Verständnis der Gestaltung des ISMS im Kontext der Organisation, Risikobeurteilung und -handhabung, Informationssicherheitspolitik und -ziele des Kunden und insbesondere der Bereitschaft des Kunden für das Audit erlangen. Die Ergebnisse müssen in einem schriftlichen Bericht festgehalten werden. Auf dieser Basis kann die zweite Stufe geplant werden.

Umsetzung der Massnahmen

Die zweite Stufe prüft, ob die Anforderungen der ISO 27001 sowie die vom Unternehmen dokumentierten Punkte auch so umgesetzt wurden. Insbesondere verlangt die Norm unter anderem, dass ein Schwerpunkt auf die Führung durch die oberste Leitung und Verpflichtung zur Informationssicherheitspolitik, der Bewertung der damit zusammenhängenden Risiken, die Informationssicherheitsleistung und die Wirksamkeit des ISMS sowie die Umsetzung der Massnahmen gelegt wird.

Für die Überwachungsaudits gelten weitere Anforderungen. So muss pro Kalenderjahr eines erfolgen. Zweck der Überwachung ist die Überprüfung, dass das freigegebene ISMS weiterhin umgesetzt wird, die Betrachtung der Auswirkungen von Änderungen und die Bestätigung der weiteren Einhaltung der Zertifizierungsanforderungen.

Ein weiteres Kapitel definiert die Anforderungen an den Audit-Bericht. Enthalten sein müssen die Darstellung des Audits, einschliesslich einer Zusammenfassung der Dokumentenprüfung, Darstellung des Zertifizierungsaudits, Abweichungen vom Auditplan sowie der geprüfte ISMS-Anwendungsbereich. Dabei muss er eine ausreichende Detailtiefe aufweisen. Dazu gehören verfolgte Auditpfade und angewandte Auditmethoden, positive und negative Beobachtungen, Aussagen zu gefundenen Nichtkonformitäten sowie eine Empfehlung des Auditteams, ob das ISMS des Kunden zertifiziert werden kann.

Zusammenfassend bietet die ISO 27006 einen guten Einblick in die Anforderungen und Tätigkeiten einer Zertifizierungsstelle. Dies ermöglicht es einem Unternehmen, sich optimal auf die eigene Zertifizierung vorzubereiten und auch zu verstehen, wie die Auditoren denken und vorgehen.