Bild: Pixabay

Die Durchführung des Audits umfasst als ersten Schritt die Überprüfung der Dokumentation.

ISO 27007: Leitfaden für das Auditieren von ISMS

In unserer April-Ausgabe haben wir uns um die Anforderungen an Zertifizierungsstellen gekümmert (beschrieben in der ISO 27006). Begleitend dazu gibt es die ISO 27007, zuletzt im Jahr 2022 aktualisiert, die zeigt, wie ein ISMS-Audit durchgeführt werden soll. Das Dokument gibt eine Anleitung für alle Grössen und Arten von Organisationen, die ISMS-Audits durchführen müssen/wollen, unabhängig davon, ob es sich um einen oder mehrere Auditoren handelt.

Jedes Unternehmen, dass zertifiziert ist, weiss, dass es mindestens jährlich ein internes Audit durchführen muss (ISO 27001, Kapitel 9.2). Daher liegt der Fokus dieser Norm auch auf dieser Art des Audits. Jedoch hilft es auch bei den externen Audits zu verstehen, was der Auditor gerne sehen möchte. Hinweis: diese Norm orientiert sich an der Struktur der ISO 19011 mit dem Titel «Guidelines for auditing management systems». Daher wird jeweils auch auf diese Norm hingewiesen. Die ISO 19011 startet mit den Audit-Prinzipien. Diese haben den Weg in die ISO 27007 nicht gefunden. Es handelt sich um folgende sieben Prinzipien:

- Integrität der Auditoren: die Grundlage der Professionalität
- Sachliche Darstellung: die Pflicht, wahrheitsgemäss und genau zu berichten
- Angemessene berufliche Sorgfalt: Anwendung von Sorgfalt und Urteilsvermögen beim Auditieren
- Vertraulichkeit: Sicherheit von Informationen
- Unabhängigkeit: die Grundlage für die Unparteilichkeit des Audits sowie für die Objektivität der Auditschlussfolgerungen
- Faktengestützter Ansatz: die rationale Methode, um zu zuverlässigen und nachvollziehbaren Auditschlussfolgerungen in einem systematischen Auditprozess zu gelangen
- Risikobasierter Ansatz: ein Auditansatz, der Risiken und Chancen berücksichtigt

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

Ziele dieses Audits kennen

Bevor ein Audit geplant und durchgeführt werden kann, gilt es die Ziele dieses Audits zu kennen. Als Basis können die Erfordernisse und Erwartungen relevanter interessierter Parteien, die Anforderungen an Prozesse(n), Produkte(n), Dienstleistungen und Projekte(n), die Normpunkte aus dem Standard, identifizierte Risiken und Chancen, wie auch Ergebnisse aus vorangegangenen Audits dienen.

Die Norm geht weiter auf Audit-Risiken ein. Das können Fehler bei der Planung (nicht alle Standorte, nicht alle Prüfpunkte), zu wenig Ressourcen, nicht (oder zu wenig) geeignete Auditteam-Mitglieder, schlechte Kommunikation, schlechte Überwachung des Audits oder auf Seiten der auditierten Stellen die Verfügbarkeit oder mangelnde Kooperation sein.

Anhand dieser Risiken erstaunt wenig, dass im nächsten Teil auf die Rollen, inkl. Verantwortlichkeiten der involvierten Personen, die (notwendige) Kompetenz sowie die Festlegung des Umfangs des Auditprogramms eingegangen wird. Die ISO 27007 legt den Fokus auf die Grösse des ISMS: die Gesamtzahl von Personen, die im Auftrag der Organisation tätig sind, die Anzahl von Informationssystemen, die Anzahl der Standorte, die Komplexität des ISMS, die Anzahl und Art der Informationssicherheitsrisiken sowie die Anforderungen an die Vertraulichkeit, die Integrität und die Verfügbarkeit.

Bei der Umsetzung geht es darum, eine Beurteilung zu ermöglichen, dass die Anforderungen zur Informationssicherheit angemessen identifiziert und behandelt wurden. Dazu gehört eine Prüfung der Informationssicherheitspolitik, der Informationssicherheitsziele, Richtlinien und Verfahren; die vertraglichen Anforderungen; die ausgefüllte Erklärung zur Anwendbarkeit (in Englisch Statement of Applicability); die geplanten und umgesetzten Risiko-Behandlungsmassnahmen sowie die Methoden und Kriterien zur Überwachung, Messung, Analyse und Bewertung des ISMS.

Überprüfung der Dokumentation

Die Durchführung des Audits umfasst als ersten Schritt die Überprüfung der Dokumentation. Damit kann ein risikobasierter Planungsansatz abgeleitet werden. Wo sind die aktuellen Risiken des Unternehmens? Wie können die eingeleiteten Massnahmen überprüft werden, damit ein Nachweis der Wirksamkeit

möglich ist? Dies hat Einfluss auf den Auditumfang, die notwendigen Audit-Werkzeuge, die zu prüfenden Standorte und die dazu notwendigen Audit-Team-Mitglieder.

Die ISO 19011 geht weiter darauf ein, wie die Rollen und Verantwortlichkeiten während des Audits aussehen, wie das Eröffnungsgespräch zu erfolgen hat, wie die Kommunikation während des Audits aussieht, wie Informationen gesammelt und verifiziert werden, damit daraus Auditfeststellungen erarbeitet werden können sowie wie das Abschlussgespräch vorbereitet und durchgeführt wird. Danach folgen die Erstellung und Verteilung des Auditberichts und das Audit kann abgeschlossen werden. Allfällige Folgemassnahmen gilt es zusätzlich zu erfassen. Die ISO 27007 hat zu diesen Punkten keine Ergänzungen

Das Kapitel 7 geht auf die Kompetenz und Bewertung der ISMS-Auditoren ein. Auditoren sollten so gewählt werden, dass sie die Komplexität des ISMS sowie die im ISMS durchgeführten Geschäftstätigkeiten im Anwendungsbereich verstehen, den Umfang und Verschiedenartigkeit, der bei der Realisierung der verschiedenen Komponenten des ISMS genutzten Techniken prüfen und die gesetzlichen und sonstigen Anforderungen beurteilen können.

Beim persönlichen Verhalten, Kenntnissen und Fertigkeiten sowie der Kompetenz wird wiederum nur auf die ISO 19011 verwiesen. Es wird lediglich ergänzt, dass ISMS-Auditoren über Kenntnisse und Fertigkeiten in der Informationstechnik und Informationssicherheit verfügen sollten, die beispielsweise durch entsprechende Zertifizierungen belegt sind. Die Berufserfahrung einzelner ISMS-Auditoren sollte darüber hinaus zur Weiterentwicklung ihrer Kenntnisse und Fertigkeiten auf dem Gebiet des ISMS beitragen.

Damit ist die ISO 27007 bereits am Ende. Nein, nicht ganz, wir sind erst auf Seite 17 von 59 Seiten angelangt. Ab jetzt wird es erst richtig spannend. Der Anhang A bietet eine Anleitung zur praktischen Durchführung von ISMS-Audits.

Um ein ISMS zu prüfen, gilt es geeignete Stichproben zu erfassen und zu überprüfen. Dies kann durch Befragung, Beobachtung und der Überprüfung von Dokumenten erfolgen. Zu den Pflichtdokumenten der ISO 27001 gehören folgende:

- Anwendungsbereich des ISMS (4.3)
- Informationssicherheitspolitik (5.2)
- Prozess zur Informationssicherheitsrisikobeurteilung (6.1.2)
- Prozess zur Informationssicherheitsrisikobehandlung (6.1.3)
- Erklärung zur Anwendbarkeit (6.1.3 d)
- Informationssicherheitsziele (6.2)
- Kompetenznachweis (7.2 d)
- Dokumentierte Informationen, die durch die Organisation als für die Wirksamkeit des ISMS notwendig bestimmt wurden (7.5.1 b)
- Betriebliche Planung und Steuerung (8.1)
- Ergebnisse der Informationssicherheitsrisikobeurteilungen (8.2)
- Ergebnisse der Informationssicherheitsrisikobehandlung (8.3)
- Nachweis der Ergebnisse von Überwachung und Messung (9.1)
- Nachweis des Auditprogramms/der Auditprogramme und der Auditergebnisse (9.2 g)
- Nachweis der Ergebnisse von Managementbewertungen (9.3)
- Nachweis der Art von Nichtkonformitäten und der ergriffenen Folgemassnahmen (10.1 f)
- Nachweis der Ergebnisse von Korrekturmassnahmen (10.1 g)

«Versteckte» Anforderungen an eine Dokumentation

Es gibt jedoch diverse weitere «versteckte» Anforderungen an eine Dokumentation. Die ISO 27001 verlangt beispielsweise nicht, dass interne und externe Themen schriftlich festgehalten sind. Es empfiehlt sich aber trotzdem, diese zu erfassen, da es sonst schwierig wird nachweisen zu können, dass diese bestimmt wurden (was die Norm verlangt). Die Tabelle A.2 geht nun durch die gesamte ISO 27001 durch und beschreibt, welcher Auditnachweis vorhanden sein sollte. An dieser Stelle picke ich mal «A.4.2 Kompetenz» heraus (ISO/IEC 27001, 7.2).

Ein Auditnachweis ist möglich anhand dokumentierter Informationen oder anderer Informationen über zutreffende:

a) organisatorische Rollen, Verantwortlichkeiten und Befugnisse;
b) Arbeitsplatzbeschreibungen;
c) erforderliche Kompetenz;
d) Ausbildungsbescheinigungen;
e) Schulungsprogramme, Kurse und Weiterbildungsaktivitäten;
f) Bescheinigungen über unternommene Schritte zum Erwerb und zur Aufrechterhaltung der notwendigen Kompetenz;
g) Bewertung ihrer Wirksamkeit.

Die ISO/IEC 27001:2013, 7.2, erweitert den Anwendungsbereich der Kompetenz auf Personen, die nicht Angehörige der Organisation sind. Diese Anforderung legt fest, dass sie «unter Aufsicht der Organisation Tätigkeiten verrichten». Zu Beispielen können Unterauftragnehmer und Ehrenamtliche gehören.

Auditoren sollten bestätigen, dass die Organisation

a) Folgendes festlegt:
   a. die Personen, die Tätigkeiten in ihrem Auftrag ausführen, die sich auf die Informationssicherheitsleistung auswirken;
   b. die Kenntnisse und Fertigkeiten der Personen, die zum Erreichen der angestrebten Ergebnisse erforderlich sind;
   c. die Fähigkeit der Personen, die Kenntnisse und Fertigkeiten anzuwenden, die zum Erreichen der angestrebten Ergebnisse erforderlich sind;
b) sicherstellt, dass diese Personen auf der Grundlage einer entsprechenden Ausbildung, Schulung oder Erfahrung über diese Fähigkeit verfügen;
c) gegebenenfalls Massnahmen einleitet, um die notwendige Fähigkeit zu erwerben, und die Wirksamkeit der eingeleiteten Massnahmen beurteilt.

Es ist schön ersichtlich, wie genau die Anforderungen an Nachweise beschrieben sind. Selbstverständlich hat der Auditor immer noch Spielraum, seine eigene Audit-Feststellung festzuhalten.

Für uns als Geprüfte auf der anderen Seite des Tisches hilft diese ausführliche Auflistung, sich optimal auf ein Audit vorzubereiten. Es ist damit während des Audits mit wenigen Überraschungen zu rechnen, wenn diese Punkte bekannt sind. Ja, es ermöglicht sogar, sich so vorzubereiten, dass alles bereit ist und das Audit zügig vonstattengeht. Merkt der Auditor, dass alles rund läuft, muss er auch nicht überall bis ins letzte Detail alles prüfen und hinterfragen. Dies schont die Nerven und lässt den einten oder anderen vor dem Audit besser schlafen.