

Audit – Planung und Durchführung

An ein Audit werden hohe Anforderungen gestellt. Es geht nicht darum, mal schnell zu schauen und einen Bericht zu erstellen, sondern das Audit stellt eine Qualitätskontrolle dar.

Werden die aus Normen und Standards, aber auch aus eigenen Richtlinien definierten Tätigkeiten auch entsprechend umgesetzt und gelebt? Einen Schuldigen für Fehler zu suchen, ist aber nicht das Ziel, sondern Abweichungen und Verbesserungsmöglichkeiten zu erkennen. Als Ergebnis kann das Managementsystem stetig verbessert und optimiert werden.

Die ISO 19011 hilft, passende Auditoren zu finden, das Audit zu planen und durchzuführen. Die Norm trägt den Titel «Leitfaden zur Auditierung von Managementsystemen/Guidelines for auditing management systems (ISO 19011:2018)». In Kapitel 3 werden zuerst die Begriffe definiert. So zum Beispiel der Unterschied zwischen «kombiniertes Audit» und «gemeinschaftliches Audit». Auch was ein Nachweis und was eine Feststellung ist, wird erläutert.

Kapitel 4

Das Kapitel 4 definiert die notwendigen Prinzipien, um ein Audit objektiv, vollständig und korrekt durchführen zu können. Dabei werden folgende Anforderungen gestellt:

Integrität

Die Auditoren müssen die notwendige Professionalität mitbringen, ehrlich und verantwortungsvoll sein. Nur wenn die entspre-

chende Kompetenz vorhanden ist, darf dieses Gebiet auch überprüft werden. Bei vielen Zertifizierungsfirmen muss die auditierende Person mehrjährige Erfahrung im Bereich des Kunden mitbringen.

Zum Beispiel im Finanzwesen, Medizin, IT oder ähnliches. Die notwendige Kompetenz der Auditoren wird umfassend im Kapitel 7 beschrieben. Darauf wird in diesem Artikel nicht weiter eingegangen.

Sachlichkeit

Werden abweichende Punkte festgestellt, sollten diese offen und wahrheitsgemäss festgehalten werden. Gibt es Meinungsverschiedenheiten gehören diese ebenfalls in den Bericht. Die Kommunikation sollte wahrheitsgetreu, genau, objektiv, zeitgerecht, klar und vollständig sein.

Sorgfalt

Bei den Kontrollen braucht es oft Fingerspitzengefühl. Sei dies bei Interviews, aber auch bei technischen Kontrollen. So dürfen beispielsweise Systeme und Einstellungen auf keinen Fall verändert werden.

Vertraulichkeit

Eigentlich selbstverständlich, aber trotzdem erwähnenswert. Über

Ergebnisse und Erkenntnisse wird nicht mit anderen Personen diskutiert, egal ob beim Kunden, bei der Auditgesellschaft oder im eigenen Umfeld ist. Alle Unterlagen gilt es korrekt und vor fremden Zugriffen geschützt aufzubewahren.

Unabhängigkeit

Die Auditoren müssen ihre Arbeit unabhängig durchführen. Es darf keine Interessenskonflikte geben. Ein Auditor kann beispielsweise nicht das Unternehmen beraten und dann das Zertifizierungsaudit durchführen. Dies sollte, wenn immer möglich, auch nicht durch die gleiche Firma erfolgen. Ein Team berät, das andere auditiert. Hier ist eine Unabhängigkeit nicht gewährleistet.

Faktenbasierend

Werden Abweichungen festgestellt, müssen diese nachvollziehbar sein. Hörensagen, oft in Pausengesprächen etwas aufgeschnappt, gilt nicht als Nachweis. Der Auditor muss Aussagen immer prüfen und genau festhalten.

Risikobasierend

Es ist nicht möglich, alle Prozesse, jeden Schritt darin im Detail zu untersuchen. Im Vorfeld gilt es festzuhalten, wo sind hohe Risiken vorhanden. Diese Gebiete werden genauer und tiefer untersucht als weniger kritische. Weggelassen dürfen aber keine Prüfpunkte.

Kapitel 5

Das Kapitel 5 beinhaltet die Steuerung des Audits. Nachfolgende Punkte gilt es zu definieren:

Audit-Ziele

Das Audit-Programm richtet sich an die Grösse und Komplexität des Unternehmens. Werden diese outgesourced? Sind viele internen und externen Personen involviert? Sind viele, teilweise komplexe Prozesse vorhanden? Gibt es mehrere Standorte? Daher wird vor dem Audit der Kontext des Unternehmens verlangt (siehe Maschinenbau 5/2018: Kontext des Unternehmens). Darin sind die Ziele des Unternehmens, die relevante internen und externen Themen, die Erfordernisse und Erwartungen interessierter Parteien sowie die Anforderungen an die Informationssicherheit und den Datenschutz definiert.

Risiken und Chancen während des Audits

Nachfolgende Fragen gilt es selbstkritisch zu stellen: Wurde das Audit optimal geplant? Sind genügend Ressourcen vorhanden (Zeit, kompetente Auditoren, Hilfsmittel, usw.)? Funktioniert die interne und externe Kommunikation? Wurden Kontrollen korrekt geplant? Ist definiert, wie die (Audit-)Dokumente gelenkt werden (Erstellung, Korrektur, Überprüfung durch vorgesetzte Stelle, Freigabe, Kommunikation mit auditierem Unternehmen)?

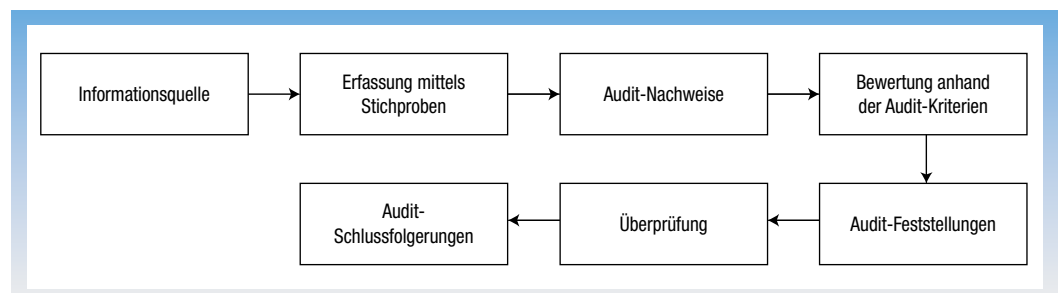
Festlegen des Auditprogramms

Nach der Bewertung der möglichen Risiken wird das Audit-Programm erstellt. Wer führt den Lead des Audits? Werden weitere Auditoren benötigt (zum Beispiel bei fehlendem Fachwissen)? Wurde bereits ein Audit bei diesem Unternehmen durchgeführt? Wie

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



Ein Innosuisse-Projekt zeigt, welche Bedeutung die internationale Beschaffung für Schweizer Unternehmen hat, welche Risiken sie dabei eingehen und wie diese Risiken kontrolliert werden können.

sahen die Resultate aus? Wie sieht der neue Zeitplan aus? Welche Audit-Methoden werden angewendet (Interview, Stichproben, technische Kontrollen, Begehungen, usw.)? Welche Standorte werden angeschaut? Welche Personen werden interviewt? Welche Sprache(n) wird gesprochen? Braucht es einen Dolmetscher? Welche Prozesse, Systeme und/oder Applikationen werden angeschaut? Wie werden die Resultate und Erkenntnisse dokumentiert? Wie werden allfällige Probleme behandelt?

Kapitel 6

Mit dieser seriösen Vorarbeit kann das Audit durchgeführt werden. Das Kapitel 6 beschreibt alle notwendigen Schritte:

- Zuerst wird der Kontakt mit der auditierten Organisation aufgenommen. Dabei wird festgehalten, über welche Kanäle kommuniziert wird (Stichwort Vertraulichkeit der Informationen), es wird nochmals die Befugnis für das Audit abgeholt, Audit-Umfang und -Ziele besprochen, geltende gesetzliche und firmeninterne Anforderungen geklärt, notwendige Vorbereitungen abgemacht und das Audit-Team bekanntgegeben.
- Das auditierte Unternehmen liefert anschliessend die vom Audit-Leiter verlangte Dokumente zur Vorbereitung der Auditoren. Dazu gehören der Anwendungsbereich, die Informationssicherheitsrichtlinie, Rollen und Verantwortlichkeiten, wichtige Prozesse (nicht nur auf Informationssicherheit bezogen), frühere Audit-Resultate (zum Beispiel aus internen Audits) und auf die Ziele des Audits ausgerichtete Dokumentationen.
- Die gelieferten Unterlagen werden vom Audit-Team studiert und erste Erkenntnisse notiert. Allenfalls ist es notwendig, kleine Anpassungen am Audit-Zeitplan vorzunehmen, Themengebiete anzupassen oder zu erweitern.
- Nun kann endlich das Audit stattfinden. Im Eröffnungsgespräch werden die Auditoren sowie die involvierten Personen des Unternehmens vorgestellt und nochmals kurz der Tagesablauf besprochen, notwendige Anpassungen vorgenommen und offene Fragen geklärt.
- Die geplanten Themen werden gemäss Audit-Plan durchgearbeitet, Unklarheiten besprochen und Nachweise schriftlich festgehalten. Der Lead-Auditor sammelt diese und prüft, ob alles verständlich und nachvollziehbar ist (Bild).
- Das Auditoren-Team bereitet im Anschluss das Schlussgespräch vor, überprüft nochmals alle Feststellungen und bewertet diese.
- Die Abweichungen und Empfehlungen werden im Audit-Schlussgespräch den involvierten Personen mitgeteilt. Das Ziel ist es, dass alle wissen, um welche Punkte es sich handelt und dass diese auch verstanden sind. Je nach Schweregrad der Abweichungen wird eine Frist zwischen einem Monat und einem Jahr zur Behebung definiert. Reicht es aus,

einen schriftlichen Nachweis zur Umsetzung zu liefern oder müssen die Auditoren nochmals vorbeikommen? Auch dies wird mit dem Unternehmen besprochen.

- Im letzten Schritt wird der Audit-Bericht erstellt. Hier werden nochmals die Ziele, der Audit-Umfang sowie -Kriterien und die Auditoren erwähnt. Weiter folgen die Auditfeststellungen und die dazugehörigen Nachweise, die Schlussfolgerungen daraus und ob das Audit bestanden wurde oder nicht. Ergänzend können die geforderten Massnahmen erläutert werden.
- Dieser Audit-Bericht wird nach einem Qualitäts-Review dem auditierten Unternehmen zugestellt.

Kapitel 7

Im bereits erwähnten Kapitel 7 werden die notwendigen Kompetenzen von Auditoren ausführlich beschrieben.

Der Anhang rundet das Dokument ab. Darin enthalten sind:

- Wie Audit-Methoden angewendet werden (unterschieden nach Vor-Ort und aus der Ferne)
- Definition von «Fachmännisches Urteil», «Leistungsbezogene Ergebnisse»
- Beschreibung, wie Informationen verifiziert werden
- Anleitung, wie gute Stichproben gezogen (zum Beispiel Grösse) und Informationsquellen ausgewählt werden
- Auditieren von Compliance-Anforderungen, damit keine gesetzlichen oder vertraglichen Anforderungen vergessen gehen
- Wie der Kontext eines Unternehmens idealerweise geprüft wird
- Vorgehen zum Auditieren der Themen Führung und Verpflichtung, also der Verantwortung des Top Managements
- Auditieren von Risiken und Chancen sowie möglicher Lieferketten
- Nachweis des Lebenszyklus des Managementsystems
- Wie Auditarbeitsunterlagen aussehen sollten
- Wie die Begehung vor Ort durchgeführt wird
- Wie virtuelle Tätigkeiten auditiert werden können
- Wie gute Befragungen durchgeführt werden (zum Beispiel offene anstelle von geschlossenen Fragen stellen)
- Und zu guter Letzt, wie Auditfeststellungen bestimmt, aufgezeichnet und festgehalten werden müssen

Die ISO 19011 ist ein sehr umfassendes Dokument, welches alle Anforderungen an Audits definiert. Von der Planung, der Durchführung bis zum Schlussbericht sind alle Schritte ausführlich beschrieben. Ebenfalls sind die notwendigen Kompetenzen von Auditoren enthalten. Dieses Dokument lohnt sich für alle, die selbst Audits durchführen müssen oder sich auf ein Audit vorbereiten möchten.



Jederzeit die maximale Sicherheit



Der Sicherheitssensor 671 mit ATEX-Zulassung nach RL 2014/34/EU bietet mit einer hohen Varianz an Produkten bis Cat. 1 / Zone 0 wirtschaftliche Lösungen für unterschiedlichste Anwendungen. Die Schutzart IP68 (bis 10 bar) macht den Sensor ideal für Anwendungen in der Prozessindustrie. Für die Überwachung von beweglich trennenden Schutzeinrichtungen in Mühlen für die Lebensmittel- und Pharma-Herstellung, aber auch in öl- und gasverarbeitenden Anlagen wie z.B. Lackierstrassen ist der 671 ATEX Sensor hervorragend geeignet.

Für mehr Informationen besuchen Sie uns auch unter www.elobau.ch oder rufen Sie uns an, Telefon 041 530 23 28