Zertifizierungs- und Auditprozess

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

Impressum

Herausgeber
ConformityZert GmbH
Leiter der Zertifizierungsstelle
Faberstr. 10, 55278 Mommenheim, Deutschland

Geltungsbereich
ConformityZert GmbH

Dateiname	Dokumententyp/Klassifizierung
CZ_Zertifizierungs- und Auditprozess_20200709.doc	Prozess/intern

Version, Stand	Gültig bis	Status
1.4 vom 09.07.2020	08.07.2021	Freigegeben

Autor / fachlicher Ansprechpartner	Geprüft von	Freigegeben von
Adrian Berger	Daniela Schmidt	Hannes Stelzer

Kurzinfo/Abstract:
Die Darstellung und Beschreibung des Zertifizierungs- und Auditprozesses stellen eine einheitliche Vorgehensweise im Rahmen der Zertifizierung und der Zertifizierungsaudits sicher. Dieses Dokument fasst die Dokumente CZ_Zertifizierungsprozess_jjjjmmtt und CZ_Audit-Prozess für Zert-Audits_jjjjmmtt zusammen und ersetzt diese.

Änderungshistorie

Version	Stand	Bearbeiter	Änderungen/Kommentar
1.0	30.09.2019	Stefanie Bock	Ersterstellung
1.1	29.10.2019	Stefanie Bock	Anpassung Geschäftsführung und redaktionelle Änderungen, Aufnahme Abs. 4.11 Stichproben bei Multi-Standort-Organisationen
1.2	13.02.2020	Daniela Schmidt	Anpassung Normbezeichnung
1.3	14.02.2020	Daniela Schmidt	Korrektur Normbezeichnung
1.4	09.07.2020	Adrian Berger	Erweiterung Kap. 4.4 - Zeichennutzung

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

Inhalt

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

1. Einleitung

Die Aussage eines Zertifikates über Fähigkeit und Wirksamkeit eines ISMS ist nur dann sowohl für ein Unternehmen als auch für interessierte Parteien von Nutzen, wenn das entsprechende Zertifizierungsverfahren fachkundig, objektiv und unabhängig durchgeführt werden konnte.

Ein wesentlicher Aspekt ist dabei ein eindeutig definierter Zertifizierungsprozess, der sowohl Kunden als auch interessierten Parteien und allen mit Zertifizierungstätigkeiten betrauten Personen der ConformityZert GmbH jederzeit zugänglich ist.

2. Übertragung akkreditierter Zertifizierungen von Informationssicherheits-Managementsystemen

Die Übertragung der Zertifizierung wird definiert als die Anerkennung einer durch eine akkreditierte Zertifizierungsstelle (im Weiteren bezeichnet als "die ausstellende Zertifizierungsstelle") erteilten und gültigen Zertifizierung eines Managementsystems durch die Zertifizierungsstelle der ConformityZert GmbH zum Zwecke der Erteilung ihrer eigenen Zertifizierung.

2.1. Anforderungen

2.1.1. Akkreditierung

Nur Zertifizierungen, die durch eine Akkreditierung eines IAF MLA-Unterzeichners -wie z. B. die DAkkS - erfasst werden, sind übertragungsberechtigt. Organisationen, die Inhaber von Zertifizierungen sind, die nicht durch solche Akkreditierungen abgedeckt werden, werden wie neue Kunden behandelt.

2.1.2. Bewertung vor der Übertragung

Das Zertifizierungspersonal der ConformityZert GmbH führt eine Bewertung der Zertifizierung des voraussichtlichen Kunden durch. Diese Bewertung erfolgt mittels einer Unterlagenprüfung und beinhaltet in der Regel eine Begehung beim zukünftigen Kunden. Gründe, diese Begehung nicht durchzuführen, werden vollständig gerechtfertigt und dokumentiert. Eine Begehung muss durchgeführt werden, wenn kein Kontakt mit der ausstellenden Zertifizierungsstelle hergestellt werden kann. Die Bewertung umfasst folgende Aspekte und deren Feststellungen werden vollständig dokumentiert:

- Bestätigung, dass die zertifizierten Tätigkeiten des Kunden in den akkreditierten Bereich der ConformityZert GmbH fallen;
- Gründe für das Beantragen einer Übertragung;

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

- dass der Standort bzw. die Standorte, die die Übertragung wünschen, eine akkreditierte Zertifizierung besitzen, die gültig ist im Hinblick auf Echtheit, Dauer der Gültigkeit sowie Gültigkeitsbereich der Tätigkeiten, die von der Zertifizierung des Managementsystems abgedeckt werden. Falls zweckmäßig, werden die Gültigkeit der Zertifizierung und der Status der offenen Nichtkonformitäten mit der ausstellenden Zertifizierungsstelle überprüft, außer diese hat ihre Geschäftstätigkeiten bereits eingestellt. Wenn es nicht möglich ist, mit der ausstellenden Zertifizierungsstelle zu kommunizieren, muss die anerkennende Zertifizierungsstelle die Gründe aufzeichnen;
- eine Prüfung der letzten Auditberichte zur Zertifizierung bzw. Re-Zertifizierung, darauf folgende Überwachungsberichte sowie jedwede offene Nichtkonformitäten, die daraus resultieren. Diese Prüfung muss ebenfalls jede weitere verfügbare relevante Dokumentation bezüglich des Zertifizierungsprozesses beinhalten, d. h. handgeschriebene Notizen, Checklisten. Wenn die letzten Auditberichte zur Zertifizierung, Re-Zertifizierung oder zur darauf folgenden Überwachung nicht zur Verfügung gestellt werden oder wenn das Überwachungsaudit überfällig ist, dann ist die Organisation wie ein neuer Kunde zu behandeln;
- vorliegende Beschwerden und getroffene Maßnahmen;
- der Stand im aktuellen Zertifizierungszyklus
- jegliche aktuelle Vereinbarung der Organisation mit Behörden bezüglich der Rechtskonformität.

2.2. Zertifizierung

Die Übertragung sollte in der Regel nur von gültigen akkreditierten Zertifizierungen erfolgen. In dem Falle, dass eine Zertifizierung von einer Zertifizierungsstelle ausgestellt wurde, die ihre Geschäfte beendet hat oder deren Akkreditierung abgelaufen ist, ausgesetzt oder zurückgezogen wurde, kann die ConformityZert GmbH allerdings nach ihrem Ermessen eine solche Zertifizierung zur Übertragung in Erwägung ziehen. In solchen Fällen holt die ConformityZert GmbH, bevor sie die Übertragung einleitet, die Zustimmung von derjenigen Akkreditierungsstelle ein, deren Zeichen sie auf dem Zertifikat zu platzieren beabsichtigt.
Im Falle einer Akquisition einer Zertifizierungsstelle wird die ConformityZert GmbH die bisherigen vertraglichen Verpflichtungen der übernommenen Zertifizierungsstelle - da wo praktikabel - erfüllen.

Eine Zertifizierung, von der bekannt ist, dass ihre Gültigkeit ausgesetzt ist oder deren Aussetzung angedroht wurde, wird für eine Übertragung nicht akzeptiert. Wenn die ConformityZert GmbH nicht in der Lage ist, den Stand der Zertifizierung mit der ausstellenden Zertifizierungsstelle zu überprüfen, wird die Organisation aufgefordert zu bestätigen, dass das Zertifikat nicht ausgesetzt bzw. eine Aussetzung nicht angedroht wurde.

Offene Nichtkonformitäten sollten nach Möglichkeit mit der ausstellenden Zertifizierungsstelle vor der Übertragung geschlossen werden. Falls dies nicht möglich ist, müssen die offenen Nichtkonformitäten mit der ConformityZert GmbH geschlossen werden.

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

Wenn keine weiteren offenen oder potentiellen Probleme bei der Prüfung vor der Übertragung festgestellt werden, kann eine Zertifizierung im Anschluss an den üblichen Entscheidungsprozess erteilt werden. Das Programm zur laufenden Überwachung sollte sich auf den vorherigen Zertifizierungszyklus stützen, außer wenn die ConformityZert GmbH ein Erstaudit oder ein Re-Zertifizierungsaudit basierend auf dem Ergebnis ihrer Prüfung durchgeführt hat.

Wenn nach der Prüfung vor der Übertragung weiterhin Zweifel bezüglich der Angemessenheit einer aktuellen oder früheren Zertifizierung bestehen, so wird die ConformityZert GmbH - in Abhängigkeit vom Ausmaß ihrer Zweifel - entweder:

- den Antragsteller wie einen neuen Kunden behandeln
  oder
- ein Audit durchführen, das sich auf die identifizierten Problembereiche konzentriert.

Die Entscheidung bezüglich der erforderlichen Aktivität hängt ab von der Art und dem Umfang der identifizierten Probleme und wird gegenüber der Organisation erläutert. Die Begründung der Entscheidung wird dokumentiert, und die Unterlagen werden durch die ConformityZert GmbH aufbewahrt.

3. Darstellung des Zertifizierungs- und Auditprozesses

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

4. Detaillierte Beschreibung der Prozess-Schritte

4.1. Beantragung der Zertifizierung

Der Antrag auf Zertifizierung eines Informationssicherheitsmanagementsystems gem. ISO/IEC 27001:2015 ist auf der Homepage der ConformityZert GmbH unter www.ConformityZert.de veröffentlicht und steht dort zum Download bereit. Auf Anfrage wird er auch per Mail an den Antragsteller übermittelt.

Sollen im Rahmen der Zertifizierung durch die ConformityZert GmbH eine dem Kunden bereits gewährte Zertifizierung und Audits, die von einer anderen Zertifizierungsstelle durchgeführt wurden, berücksichtigt werden, so sind durch den Kunden ausreichende Nachweise über diese Tätigkeiten vorzulegen.

4.2. Prüfung und Annahme/Ablehnung des Zertifizierungsantrages

Die Prüfung des Zertifizierungsantrags stellt sicher, dass

- die Informationen über die antragstellende Organisation und deren Managementsystem ausreichend für die Durchführung des Audits sind,
- die Anforderungen an die Zertifizierung klar definiert und dokumentiert sind und der antragstellenden Organisation bereitgestellt wurden,
- alle bekannten Differenzen im Verständnis zwischen der ConformityZert GmbH und der antragstellenden Organisation geklärt werden,
- die ConformityZert GmbH über die Kompetenz und die Fähigkeit verfügt, die Zertifizierungstätigkeiten durchzuführen,
- der Geltungsbereich der angestrebten Zertifizierung, der/die Standort(e) der Tätigkeiten der antragstellenden Organisation, die zur Ausführung der Audits erforderliche Zeit sowie alle andere Aspekte, die die Zertifizierungstätigkeit beeinflussen, berücksichtigt werden (Sprache, Sicherheitsbedingungen, Gefährdungen der Unparteilichkeit usw.),
- Aufzeichnungen zur Begründung der Entscheidung, ein Audit durchzuführen, aufrechtzuerhalten sind.

Die ConformityZert GmbH gibt dem Kunden unverzüglich nach Prüfung des Zertifizierungsantrags schriftlich dessen Annahme bzw. Ablehnung bekannt.

Falls die ConformityZert GmbH einen Zertifizierungsantrag nach Prüfung des Antrags ablehnt, werden die Gründe für die Ablehnung dokumentiert und dem Kunden verdeutlicht.

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

4.3. Angebotserstellung

Im Fall der Annahme des Antrags erstellt die ConformityZert GmbH ein Angebot auf der Grundlage der Angaben in Zertifizierungsantrag und entsprechend vom Kunden ausgefüllten Fragebogen (s. CZ_Berechnungstool.xls).

4.4. Abschluss Zertifizierungsvertrag mit dem Kunden

Bei Annahme des Angebots schließt die ConformityZert GmbH eine Zertifizierungsvereinbarung mit dem Kunden (CZ_Zertifizierungsvertrag_TEMPLATE.doc). Diese beinhaltet insbesondere eine rechtlich durchsetzbare Vereinbarung mit dem auftraggebenden Kunden über die Bereitstellung von Zertifizierungstätigkeiten. Sowie umfassende und verbindliche Vorgaben zur Zeichennutzung.

Im Rahmen der Überwachungstätigkeiten erfolgt auch eine Überprüfung der Einhaltung der Zeichennutzungsregelungen.

4.5. Beauftragung der Auditoren zur Durchführung des Zertifizierungsaudits

4.5.1. Kompetenzermittlung für Auditteam und Zertifizierungsentscheidung

Basierend auf den Informationen aus der Antragstellung sowie dem Ergebnis der Prüfung des Zertifizierungsantrags werden die für die Durchführung der Zertifizierungsaudits und das Treffen der Zertifizierungsentscheidung erforderlichen Kompetenzen ermittelt.

- Auditteam:
  Grundlage für die Kompetenzfeststellung des Auditteams ist die Auditoren-Kompetenz-Matrix, die durch die ConformityZert GmbH geführt wird. Im Rahmen der Ermittlung der erforderlichen Kompetenzen ist es dadurch möglich, auch den eventuellen Bedarf an zusätzlichen Fachexperten zur Auditierung zu erheben. Hierdurch kann sichergestellt werden, dass das unter diesen Bedingungen bestellte Auditteam den Anforderungen an das Audit/die Audits für jeden spezifischen Kunden genügt.
  Auditoren, die sich noch in der Ausbildung befinden, dürfen am Audit teilnehmen, sofern ein Auditor mit der Beurteilung beauftragt wird. Der mit der Beurteilung beauftragte Auditor muss über die notwendige Kompetenz verfügen und trägt die endgültige Verantwortung für die Tätigkeiten und Ergebnisse des Auditors in Ausbildung.

- Zertifizierungsentscheidung:
  Im Zug der Bestellung des Auditteams werden auch die Personen/wird auch die Person benannt, die die Zertifizierungsentscheidung treffen werden/wird. Damit kann sichergestellt werden, dass in diesem Bereich ebenfalls die erforderliche Kompetenz verfügbar ist.

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

4.5.2. Auswahl des Audit-Teams

Die Auswahl des Audit-Teams erfolgt auf der Grundlage der Auditoren-Kompetenz-Matrix und der aktuellen Einsatzplanung.

Dabei werden folgende Rahmenbedingungen berücksichtigt:

- Auditziele, Auditumfang, Auditkriterien und die geschätzte Dauer des Audits
- ob das Audit ein kombiniertes, integriertes oder gemeinschaftliches Audit ist;
- die Gesamtkompetenz des Auditteams, die erforderlich ist, um die Auditziele zu erreichen;
- Zertifizierungsanforderungen (einschließlich aller anzuwendenden gesetzlichen, behördlichen oder vertraglichen Anforderungen);
- Sprache und Kultur;
- ob die Mitglieder des Auditteams das Managementsystem des Kunden zuvor bereits auditiert haben.

Wenn erforderlich wird das Audit-Team durch Fachexperten, Übersetzer oder Dolmetscher ergänzt, die unter der Anleitung eines Auditors arbeiten. Übersetzer oder Dolmetscher werden dabei so eingesetzt, dass sie keinen unangemessenen Einfluss auf das Audit ausüben.

Der Auditteamleiter ordnet in Absprache mit dem Auditteam jedem Teammitglied die Verantwortung für die Auditierung bestimmter Prozesse, Funktionen, Standorte, Bereiche oder Tätigkeiten zu. Solche Zuordnungen berücksichtigen die erforderlichen Kompetenzen und den wirksamen und effizienten Einsatz des Auditteams sowie die unterschiedlichen Rollen und Verantwortlichkeiten der Auditoren, der Auditoren in Ausbildung und der Fachexperten. An der Aufgabenverteilung können im Verlauf des Audits Änderungen vorgenommen werden, um das Erreichen der Auditziele sicherzustellen.

4.6. Erstellung Auditplan (inkl. Auditziele, -umfang und –kriterien)

- Vorbereiten und Erstellen des **Auditplans** (s. Template Auditplan)
  Wenn beim Kunden in Schichten gearbeitet wird, werden die Tätigkeiten, die während einer Schicht ausgeführt werden, bei der Erstellung des Auditprogramms und Auditplans berücksichtigt.

- Die **Auditziele**, die durch den Audit-Bereich der ConformityZert GmbH festgelegt werden, beinhalten folgende Aspekte:

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

- Feststellung der Konformität des Managementsystems des Kunden oder von Teilen dieses Managementsystems mit den Auditkriterien;
- Beurteilung der Fähigkeit des Managementsystems, die Erfüllung der geltenden gesetzlichen, behördlichen und vertraglichen Anforderungen durch die Kundenorganisation sicherzustellen;
- Beurteilung der Wirksamkeit des Managementsystems in Bezug auf die Sicherstellung, dass die Kundenorganisation dauerhaft ihre festgelegten Ziele erfüllt;
- falls anwendbar, die Nennung von Bereichen für mögliche Verbesserungen des Managementsystems.

- Der **Auditumfang** beschreibt das Ausmaß und die Grenzen des Audits, wie z. B. physische Standorte, Organisationseinheiten, Tätigkeiten und Prozesse. Falls ein Erst- oder Re-Zertifizierungsprozess mehr als ein Audit umfasst (z. B. wenn mehrere Standorte abgedeckt werden müssen), ist es möglich, dass der Auditumfang eines einzelnen dieser Audits nicht den gesamten Geltungsbereich der Zertifizierung abdeckt, die Gesamtheit der Audits muss jedoch zum im Zertifizierungsdokument angegebenen Geltungsbereich passen.

4.7. Durchführung des Audits (inkl. Auditfeststellungen und –schlussfolgerungen)

4.7.1. Erstzertifizierung

Das Erstzertifizierungs-Audit eines ISMS wird in zwei Stufen durchgeführt– Stufe 1 und Stufe 2. Der Kunde muss Vorbereitungen treffen, die den Zugriff auf interne Audit-Berichte und eigenständige Überprüfungen der Informationssicherheit gewährleisten.

Das Auditteam prüft das ISMS des Kunden gem. dem definierten Geltungsbereich gegen alle geltenden Zertifizierungsanforderungen. Die Zertifizierungsstelle muss bestätigen, dass der Kunde die Anforderungen zur Festlegung des Anwendungsbereichs des ISMS gem.DIN ISO/IEC 27001:2015, Abs. 4.3 erfüllt. Das Risikomanagement des Kunden muss ordnungsgemäß dessen Aktivitäten widerspiegeln und durch den Geltungsbereich des ISMS begrenzt sein. Dies muss sich im Geltungsbereich des ISMS des Kunden und der Erklärung zur Anwendbarkeit widerspiegeln. Es muss mindestens eine Erklärung zur Anwendbarkeit pro Geltungsbereich der Zertifizierung geben. Schnittstellen mit Dienstleistungen oder Tätigkeiten, die nicht vollständig im Geltungsbereich des ISMS sind, werden im Geltungsbereich zur Zertifizierung berücksichtigt und werden im Informationssicherheits-Risikomanagement des Kunden betrachtet. Ein Beispiel für eine solche Situation ist die gemeinsame Nutzung von Einrichtungen (z. B. IT-Systeme, Datenbanken und Telekommunikationssysteme oder die Auslagerung von einer Business-Funktion) mit anderen Organisationen.

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

Das **Audit der Stufe 1** wird durchgeführt, um

- die Managementsystem-Dokumentation des Kunden zu auditieren,
- den Standort und die standortspezifischen Bedingungen des Kunden zu beurteilen, sowie Diskussionen mit dem Personal der Organisation des Kunden zu führen, um die Bereitschaft für das Audit Stufe 2 zu ermitteln,
- den Status des Kunden zu bewerten sowie das Verständnis bezüglich der Anforderungen der DIN ISO/IEC 27001:2015, insbesondere im Hinblick auf die Identifizierung von Schlüsselleistungen bzw. bedeutsamen Aspekten, Prozessen, Zielen und das Betreiben des ISMS,
- notwendige Informationen zu sammeln bezüglich des Geltungsbereichs des ISMS, der Prozesse und des/der Standorts(e) des Kunden sowie zugehörige gesetzliche und behördliche Aspekte und deren Einhaltung (z. B. Qualitäts-, Umwelt-, rechtliche Aspekte der Tätigkeiten des Kunden, damit verbundene Risiken usw.),
- ein ausreichendes Verständnis für die Gestaltung des ISMS im Zusammenhang mit der Organisation des Kunden, der Risikobewertung und -behandlung (einschließlich der festgelegten Maßnahmen), der Informationssicherheitspolitik und der -ziele zu erhalten
- die Zuteilung der Ressourcen für Audits der Stufe 2 zu bewerten sowie die Einzelheiten der Audits der Stufe 2 mit dem Kunden abzustimmen,
- einen Schwerpunkt für die Planung des Audits der Stufe 2 zu schaffen, indem ausreichendes Verständnis des ISMS des Kunden sowie zu den Standorttätigkeiten zusammen mit möglichen signifikanten Aspekten erlangt werden,
- zu beurteilen, ob die internen Audits und Managementbewertungen geplant und durchgeführt werden (mindestens ein durchgeführtes internes Audit über den Geltungsbereich des ISMS und eine durchgeführte Managementbewertung) und ob der Grad der Umsetzung des ISMS belegt, dass der Kunde für das Audit der Stufe 2 bereit ist.

Um die oben genannten Ziele zu erreichen, werden mindestens Teile des Audits der Stufe 1 auf dem Betriebsgelände des Kunden durchgeführt.
Auditfeststellungen aus der Stufe 1 werden dokumentiert und dem Kunden mitgeteilt. In dieser Audit-Stufe werden Auditschlussfolgerungen abweichend zum regulären Auditprozess nicht als „Nichtkonformität“ bezeichnet. Die hier verwendeten Bezeichnungen sind „Schwachstelle“ bzw. „Handlungsempfehlung“. Dabei bedeutet „Schwachstelle“ eine mögliche Einstufung als Abweichung im Audit Stufe 2 und „Handlungsempfehlung“ identifiziertes Verbesserungs-potenzial.

Treten bedeutende Änderungen auf, die das ISMS beeinflussen würden, muss die Notwendigkeit in Betracht gezogen werden, die gesamte Stufe oder Teile von Stufe 1

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

zu wiederholen. Der Kunde wird darüber informiert, ob die Ergebnisse von Stufe 1 zu einer Verschiebung oder zu einer Stornierung von Stufe 2 führen können.

Der zeitliche Abstand der Audits zwischen Stufe 1 und Stufe 2 berücksichtigt die Erfordernisse des Kunden, um Lösungen zu Schwachstellen zu finden, die während des Audits der Stufe 1 identifiziert wurden. Ggf. sind die Festlegungen für das Audit der Stufe 2 durch die ConformityZert GmbH zu überarbeiten. Das Audit der Stufe 2 wird erst geplant und durchgeführt, nachdem der Auditbericht aus Stufe 1 durch die Zertifizierungsstelle freigegeben wurde.

Der Zweck des **Audits der Stufe 2** ist es, die Umsetzung, einschließlich der Wirksamkeit des ISMS des Kunden zu bewerten. Das Audit der Stufe 2 wird an dem/den Standort/en der/des Kunden durchgeführt. Der Auditplan berücksichtigt dabei die Ergebnisse aus Stufe 1. Zusätzlich zur Bewertung der wirksamen Umsetzung des ISMS, ist zu überprüfen, ob der Kunde seine eigenen Richtlinien, Ziele und Verfahren beachtet.

Dabei sind folgende Aspekte zu berücksichtigen:

- Informationen und Nachweise über die Konformität mit allen Anforderungen der DIN ISO/IEC 27001:2015 und anderen normativen Dokumenten;
- Überwachung der Leistung, Messung, Berichterstellung und Überprüfung nach Schlüsselleistungs-Zielen und –Vorgaben (übereinstimmend mit den Erwartungen der DIN ISO/IEC 27001:2015 oder anderen normativen Dokumenten);
- das ISMS des Kunden und dessen Leistungsfähigkeit in Bezug auf Gesetzestreue;
- Betriebssteuerung/-lenkung der Prozesse des Kunden;
- internes Auditieren und Managementbewertung;
- Verantwortlichkeit der Leitung für die grundsätzlichen Regelungen des Kunden;
- Verbindungen zwischen normativen Anforderungen, Politik, Leistungszielen und -vorgaben (übereinstimmend mit den Erwartungen in der DIN ISO/IEC 27001:2015 oder anderen normativen Dokumenten), alle anwendbaren gesetzlichen Anforderungen, Verantwortlichkeiten, Kompetenz des Personals, Tätigkeiten/ Arbeitsweise, Verfahren, Leistungsdaten und Feststellungen sowie Schlussfolgerungen aus internen Audits
- das Top-Management zeigt Führung und Engagement für die Informationssicherheitspolitik und der Informationssicherheitsziele,
- die Dokumentation der Anforderungen der DIN ISO/IEC 27001:2015;

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

- Beurteilung der Informationssicherheit im Zusammenhang mit Risiken und konsistente, valide und vergleichbare Ergebnisse bei Wiederholung der Beurteilung,

- Festlegung von Maßnahmenzielen und Maßnahmen auf Grundlage der Informationssicherheits-Risikobewertung und -Behandlung,

- Leistungsfähigkeit der Informationssicherheit und Wirksamkeit des ISMS, Beurteilung aufgrund der Informationssicherheitsziele,

- Übereinstimmung zwischen den ermittelten Maßnahmen, der Erklärung zur Anwendbarkeit und den Ergebnissen der Informationssicherheits-Risikobewertung und -Risikobehandlung sowie der Informationssicherheits-Politik und -Ziele

- die Umsetzung der Maßnahmen, unter Berücksichtigung des externen und internen Kontextes sowie der damit verbundenen Risiken, der Überwachung durch die Organisation, der Messung und Analyse der Informationssicherheits-Prozesse und Maßnahmen, um festzustellen, ob die Maßnahmen umgesetzt und wirksam sind um die entsprechenden Informationssicherheits-Ziele zu erreichen;

- Programme, Prozesse, Verfahren, Aufzeichnungen, interne Audits und Bewertungen der Wirksamkeit des ISMS um sicherzustellen, dass diese den Management-Entscheidungen und der Informationssicherheits-Politik und den -Zielen entsprechen.

4.7.2. Re-Zertifizierungsaudits

Ein Re-Zertifizierungsaudit wird geplant und durchgeführt, um die anhaltende Erfüllung aller Anforderungen der DIN ISO/IEC 27001:2015 oder eines anderen normativen Dokuments zu beurteilen. Zweck des Re-Zertifizierungsaudits ist es, die kontinuierliche Konformität und Wirksamkeit des Managementsystems als Ganzes sowie seiner anhaltenden Bedeutung und Anwendbarkeit auf den Geltungsbereich der Zertifizierung zu bestätigen. Dies wird rechtzeitig geplant und durchgeführt, um die fristgerechte Erneuerung des Zertifikats vor dessen Ablaufdatum zu ermöglichen

Das Re-Zertifizierungsaudit berücksichtigt auch die Leistungsfähigkeit des ISMS über den Zeitraum der Zertifizierung und eine Überprüfung früherer Auditberichte zu Überwachungsaudits.
Tätigkeiten zu Re-Zertifizierungsaudits können ein Audit der Stufe 1 erfordern, wenn es signifikante Änderungen im ISMS, beim Kunden oder im Zusammenhang mit der Arbeitsweise des ISMS gibt (z. B. Veränderungen in der Gesetzgebung).
Wenn Mehrfach-Standort- oder Mehrfach-ISMS-Zertifizierungen durch die ConformityZert GmbH durchgeführt werden, so stellt die Auditplanung — um Vertrauen in die Zertifizierung zu schaffen — einen ausreichenden Umfang des Vor-Ort-Audits sicher.

Grundsätzlich wird für die Durchführung der Re-Zertifizierungsaudits der Auditprozess für Zertifizierungsaudits angewendet. Hierbei sind jedoch folgende Besonderheiten zu

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

beachten:

- die Wirksamkeit des ISMS in seiner Gesamtheit angesichts interner oder externer Änderungen und seine fortgesetzte Bedeutung und Anwendbarkeit im Geltungsbereich der Zertifizierung werden überprüft;

- die dargelegte Verpflichtung zur Aufrechterhaltung der Wirksamkeit und Verbesserung des ISMS, um die gesamte Leistungsfähigkeit zu steigern, sind nachzuweisen;

- das Betreiben des zertifizierten ISMS muss zum Erreichen von Politik und Zielstellungen der Organisation beitragen.

Wenn während eines Re-Zertifizierungsaudits Fälle von Nichtkonformitäten oder mangelnde Nachweise für die Konformität identifiziert werden, so bestimmt die ConformityZert GmbH Fristen für umzusetzende Korrekturen und Korrekturmaßnahmen noch vor Ablauf der Zertifizierung.

Wenn die Re-Zertifizierungstätigkeiten vor Ablauf der bestehenden Zertifizierung erfolgreich abgeschlossen werden, beruht das Ablaufdatum der neuen Zertifizierung auf dem Ablaufdatum der bestehenden Zertifizierung. Das Ausgabedatum des neuen Zertifikats entspricht dem Tag der Re-Zertifizierungsentscheidung. Wird das Re-Zertifizierungsaudit vor Ablauf des Zertifizierungsdatums nicht abgeschlossen oder ist es nicht möglich, die Umsetzung von Korrekturen und Korrekturmaßnahmen für eine beliebige wesentliche Nichtkonformität zu verifizieren, dann wird keine Empfehlung für die Re-Zertifizierung ausgesprochen und die Gültigkeit der Zertifizierung nicht verlängert. Der Kunde wird informiert und die Konsequenzen werden erläutert. Unter der Voraussetzung, dass die ausstehenden Re-Zertifizierungstätigkeiten abgeschlossen worden sind, wird die Zertifizierung innerhalb von 6 Monaten nach deren Ablauf wiederhergestellt; danach ist mindestens die Stufe 2 eines Zertifizierungsaudits zu durchlaufen. Das Gültigkeitsdatum des Zertifikats entspricht dann dem Tag der Re-Zertifizierungsentscheidung und das Ablaufdatum basiert auf dem vorangegangenen Zertifizierungszyklus.

4.7.3. Audits aus besonderem Anlass

Als Konsequenz auf eine beantragte Erweiterung des Geltungsbereichs einer schon erteilten Zertifizierung nimmt die ConformityZert GmbH eine Bewertung des Antrags vor und legt alle erforderlichen Audittätigkeiten fest, um zu entscheiden, ob eine Erweiterung erteilt werden kann oder nicht. Dies kann im Zusammenhang mit einem Überwachungsaudit erfolgen.

Um Beschwerden zu untersuchen kann es erforderlich sein, kurzfristig angekündigte Audits bei den zertifizierten Kunden durchzuführen. Ebenso als Konsequenz von Änderungen oder als Konsequenz auf ausgesetzte Kundenzertifizierungen. In solchen Fällen

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

- beschreibt die ConformityZert GmbH die Bedingungen, unter denen diese kurzfristigen Begehungen durchgeführt werden und macht diese dem Kunden bekannt

- wird bei der Benennung des Auditteams zusätzliche Sorgfalt walten lassen, da dem Kunden die Möglichkeit fehlt, gegen Mitglieder des Auditteams Einwand zu erheben.

4.7.4. Kommunikation zum Audit

- Die **Aufgaben des Audit-Teams** sind eindeutig definiert und werden dem Kunden vor Durchführung der Audits bekannt gegeben:

    - Struktur, grundsätzliche Regelungen, Prozesse, Verfahren, Aufzeichnungen und zugehörige Dokumente der Organisation des Kunden bezüglich des Managementsystems prüfen und verifizieren,

    - feststellen, dass diese alle relevanten Anforderungen bezüglich des beabsichtigten Geltungsbereichs der Zertifizierung erfüllen,

    - feststellen, dass die Prozesse und Verfahren wirksam eingeführt, umgesetzt und aufrechterhalten werden, um Grundlage für das Vertrauen in das Managementsystem des Kunden zu schaffen, und

    - dem Kunden für seine eigenen Maßnahmen jeglichen Widerspruch zwischen den grundsätzlichen Regelungen des Kunden, seiner Ziele und Vorgaben (in Übereinstimmung mit den Erwartungen der relevanten Managementnormen oder anderen normativen Dokumenten) und den Ergebnissen zu vermitteln.

- Die **Namen der Mitglieder des Auditteams** und, wenn gewünscht, Hintergrundinformationen zu jedem Mitglied des Auditteams werden dem Kunden vorab zur Verfügung gestellt, so dass dem Kunden genügend Zeit bleibt, der Benennung eines bestimmten Auditors oder Fachexperten zu widersprechen und der Audit-Bereich der ConformityZert GmbH das Team auf einen begründeten Einspruch neu zusammenstellen kann.

- Der **Auditplan** wird der auftraggebenden Organisation/dem Kunden vorab mitgeteilt und die Daten zum Audit werden vorab mit dem Kunden abgestimmt.

4.7.5. Durchführung der Eröffnungsbesprechung

Die Eröffnungsbesprechung wird mit dem Management der zu auditierenden Organisation oder gegebenenfalls mit den Verantwortlichen für die zu auditierenden Funktionsbereiche oder Prozesse durchgeführt. Die Anwesenheit bei dieser Eröffnungsprechung wird protokolliert.

Zweck der Eröffnungsbesprechung:

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

- Vorstellung der Teilnehmer einschließlich einer Kurzdarstellung ihrer Rollen;
- Bestätigung des Geltungsbereichs der Zertifizierung;
- Bestätigung des Auditplans (einschließlich Art des Audits und Auditumfang, Auditziele und Auditkriterien), aller Änderungen und sonstiger relevanter Vereinbarungen mit dem Kunden, wie z. B. Datum und Uhrzeit der Abschlussbesprechung bzw. der Zwischenbesprechungen zwischen dem Auditteam und der Leitung des Kunden;
- Bestätigung der offiziellen Kommunikationskanäle zwischen Auditteam und Kunde;
- Bestätigung, dass die vom Auditteam benötigten Ressourcen und Einrichtungen zur Verfügung stehen;
- Bestätigung von Angelegenheiten, die sich auf Vertraulichkeit beziehen;
- Bestätigung der für das Auditteam zutreffenden Arbeitsschutz-, Notfall- und Sicherheitsverfahren;
- Bestätigung der Verfügbarkeit, Rollen und Identitäten von etwaigen Betreuern und Beobachtern;
- Methoden der Berichterstattung einschließlich der Einstufung der Audit-feststellungen;
- Informationen zu den Bedingungen, die zum vorzeitigen Abbruch des Audits führen können;
- Bestätigung, dass der Auditteamleiter und das Auditteam in Vertretung der ConformityZert GmbH die Verantwortung für das Audit tragen und die Leitungs-funktion für die Ausführung des Auditplans einschließlich der Audittätigkeiten und des Auditpfades innehaben
- Bestätigung des Status von Auditfeststellungen aus der vorangegangenen Überprüfung bzw. aus den vorangegangenen Audits, falls zutreffend;
- Bestätigung der für das Audits zu gebrauchenden Sprache;
- Bestätigung, dass der Kunde während des Audits über dessen Fortschritt und alle auftretenden Probleme auf dem Laufenden gehalten wird;
- Möglichkeit für den Kunden, Fragen zu stellen.

4.7.6. Kommunikation während des Audits

Teilnehmer während der Durchführung des Vor-Ort-Audits werden protokolliert.

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

Im Verlauf des Audits bewertet das Auditteam in regelmäßigen zeitlichen Abständen den Fortschritt des Audits und tauscht Informationen aus. Der Auditteamleiter ordnet bei Bedarf die Aufgaben unter den Mitgliedern des Auditteams neu zu und informiert den Kunden in regelmäßigen zeitlichen Abständen über den Fortschritt des Audits und alle Bedenken.

Falls die verfügbaren Auditnachweise anzeigen, dass die Auditziele nicht erreicht werden können, oder ein unmittelbares und erhebliches Risiko (z. B. Sicherheit) bestehen kann, erstattet der Auditteamleiter dem Kunden und, falls möglich, der ConformityZert GmbH darüber Bericht, um die entsprechenden Maßnahmen zu ermitteln. Zu diesen Maßnahmen können die erneute Bestätigung oder die Veränderung des Auditplans, Änderungen an den Zielen oder am Auditumfang oder auch der Abbruch des Audits gehören.

Der Auditteamleiter überprüft gemeinsam mit dem Kunden jeglichen Änderungsbedarf am Auditumfang, der sich im Verlauf der Audittätigkeiten vor Ort herausstellt, und erstattet der ConformityZert GmbH darüber Bericht.

4.7.7. Beobachter und Betreuer

Der Anwesenheit und Begründung von **Beobachtern** bei einer Audittätigkeit muss vor Durchführung des Audits von der ConformityZert GmbH und dem Kunden zugestimmt werden. Das Auditteam stellt sicher, dass Beobachter den Auditprozess und das Auditergebnis weder behindern noch beeinflussen.

Jeder Auditor muss von einem **Betreuer** begleitet werden, es sei denn, es besteht eine andere Vereinbarung zwischen dem Auditteamleiter und dem Kunden. Der (Die) Betreuer ist (werden) zur Unterstützung des Audits für die Begleitung des Auditteams abgestellt. Das Auditteam stellt sicher, dass die Betreuer den Auditprozess und das Auditergebnis weder behindern noch beeinflussen.

4.7.8. Sammlung und Verifizierung von Informationen

Während des Audits werden Informationen, die für die Auditziele, den Auditumfang und die Auditkriterien von Bedeutung sind (einschließlich Informationen zu den Schnittstellen zwischen Funktionen, Tätigkeiten und Prozessen), durch angemessene Stichproben erfasst und verifiziert, um sie als Auditnachweise verwenden zu können.

Als Verfahren für die Sammlung von Informationen werden genutzt

- Befragungen;

- Beobachtung von Prozessen und Tätigkeiten;

- Auswertung von Dokumentationen und Aufzeichnungen.

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

4.7.9. Ermittlung und Aufzeichnung der Auditfeststellungen

Auditfeststellungen, die die Konformität zusammenfassen und Nichtkonformitäten in ihren Einzelheiten beschreiben, und die diese Ergebnisse stützenden Auditnachweise werden aufgezeichnet und berichtet, um eine Zertifizierungsentscheidung auf Grundlage von Informationen treffen oder die Zertifizierung aufrecht erhalten zu können.

Verbesserungsmöglichkeiten werden ermittelt und aufgezeichnet, dabei ist zu berücksichtigen, dass Nichtkonformitäten, nicht als Verbesserungsmöglichkeiten aufgezeichnet werden dürfen.

Nichtkonformitäten werden bezüglich einer bestimmten Anforderung der Auditkriterien aufgezeichnet und enthalten eine klare Angabe der Nichtkonformität, sowie die objektiven, im Einzelnen beschriebenen Nachweise für die Nichtkonformität. Nichtkonformitäten werden mit dem Kunden erörtert, um sicherzustellen, dass die dafür gefundenen Nachweise korrekt sind und diese Nichtkonformitäten verstanden werden. Dabei muss sich der Auditor zurückhalten, Ursachen von Nichtkonformitäten zu erklären oder deren Lösungen vorzuschlagen.

Der Auditteamleiter ist gehalten, alle eventuellen Meinungsverschiedenheiten zwischen Auditteam und Kunden in Bezug auf Auditnachweise oder Auditfeststellungen aufzulösen, wobei ungelöst bleibende Punkte aufgezeichnet werden.

4.7.10. Erarbeiten der Auditschlussfolgerungen

Tätigkeiten des Auditteams vor der Abschlussbesprechung:

- Bewertung der Auditfeststellungen und aller sonstigen im Verlauf des Audits gesammelten geeigneten Informationen gegenüber den Auditzielen
- Ziehen der Auditschlussfolgerungen unter Berücksichtigung von Ungewissheiten bezüglich des Auditprozesses
- Ermittlung aller erforderlichen Auditfolgemaßnahmen
- Bestätigung der Eignung des Auditprogramms oder Ermittlung aller erforderlichen Veränderungen (z. B. Auditumfang, Auditdauer, den für das Audit gewählten Zeitraum, die Überwachungshäufigkeit, Kompetenzen).

4.7.11. Durchführen der Abschlussbesprechung

Die offizielle Abschlussbesprechung wird gemeinsam mit dem Management des Kunden und gegebenenfalls mit den Personen, die die Verantwortung für die zu auditierenden Funktionen oder Prozesse tragen, durchgeführt. Die Anwesenheit bei dieser Abschlussbesprechung wird protokolliert. Der Zweck der Abschlussbesprechung, die üblicherweise vom Auditteamleiter geleitet wird, besteht darin, die aus dem Audit gezogenen Schlussfolgerungen einschließlich der Empfehlung hinsichtlich der Zertifizierung vorzustellen. Alle Nichtkonformitäten werden so dargestellt, dass sie verstanden werden. Ein Zeitrahmen für deren Beantwortung wird vereinbart

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

Darüber hinaus umfasst die Abschlussbesprechung folgende Aspekte:

- Hinweis an den Kunden, dass die gesammelten Auditnachweise auf einer Stichprobe an Informationen basieren und daher ein gewisses Unsicherheitselement beinhalten;
- Methode und Zeitraum der Berichterstattung einschließlich Einstufung der Auditfeststellungen;
- Prozess der ConformityZert GmbH für die Behandlung von Nichtkonformitäten einschließlich aller Konsequenzen, die den Status der Zertifizierung des Kunden betreffen;
- Zeitrahmen, innerhalb dessen der Kunde einen Plan für Korrekturen und Korrekturmaßnahmen in Bezug auf die im Verlauf des Audits ermittelten Nichtkonformitäten vorlegen muss;
- nach dem Audit erfolgende Tätigkeiten der ConformityZert GmbH;
- Informationen zu den Prozessen für die Behandlung von Beschwerden und Einsprüchen.

Der Kunde erhält die Möglichkeit, Fragen zu stellen. Alle Meinungsverschiedenheiten zwischen dem Auditteam und dem Kunden in Bezug auf die Auditfeststellungen oder die aus dem Audit gezogenen Schlüsse werden erörtert und wenn möglich ausgeräumt. Alle nicht gelösten Meinungsverschiedenheiten werden aufgezeichnet und an die ConformityZert GmbH weitergeleitet.

4.7.12. Erstellen des Auditberichts

Die ConformityZert GmbH erstellt für jedes Audit einen schriftlichen Bericht (s. Template Auditbericht). Das Auditteam darf Verbesserungsmöglichkeiten aufzeigen, aber keine zielgerichteten Lösungen empfehlen. Das Eigentumsrecht am Auditbericht bleibt bei der ConformityZert GmbH.

Der Auditteamleiter stellt sicher, dass der Auditbericht erstellt wird. Er trägt die Verantwortung für dessen Inhalt. Der Auditbericht gibt eine korrekte, kurzgefasste und klare Aufzeichnung des Audits wieder, damit eine Zertifizierungsentscheidung auf Grundlage von Informationen getroffen werden kann.

Er enthält Folgendes bzw. nimmt Bezug darauf:
- Benennung der ConformityZert GmbH
- Name und Anschrift des Kunden und des Beauftragten der Leitung des Kunden
- Audittyp (z. B. Erst-, Überwachungs- oder Re-Zertifizierungsaudit)
- Auditkriterien
- Auditziele

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

- Auditumfang und besonders die Angabe der auditierten Organisations- oder Funktionseinheiten oder -prozesse und die Auditdauer
- jede Abweichung vom Auditplan und die Gründe dafür
- jeder bedeutende Aspekt, der einen Einfluss auf das Auditprogramm besitzt
- Benennung des Auditteamleiters, der Mitglieder des Auditteams und aller Begleitpersonen
- Termine und Orte, an denen die Audittätigkeiten (vor Ort oder außerhalb des Kunden) durchgeführt wurden
- Auditfeststellungen, Auditnachweise und Auditschlussfolgerungen in Übereinstimmung mit den Anforderungen des betreffenden Audittyps
- bedeutende Änderungen, sofern vorhanden, die das ISMS des Kunden beeinflussen, seitdem das letzte Audit stattgefunden hat
- alle ungelösten Aspekte, sofern solche festgestellt wurden.
- einen Haftungsausschluss, der angibt, dass die Auditierung auf einem Stichprobenahmeverfahren der verfügbaren Informationen basiert;
- Empfehlung vom Auditteam;
- der auditierte Kunde kontrolliert wirksam die Verwendung von Zertifizierungsdokumenten und -zeichen, sofern zutreffend;
- Verifizierung der Wirksamkeit von ergriffenen Korrekturmaßnahmen bezüglich vorangegangener identifizierter Nichtkonformitäten, falls zutreffend.;

Zusätzlich ist Folgendes im Auditbericht zu dokumentieren bzw. darauf zu referenzieren:

- eine Beschreibung des Audits inkl. einem Summary der Dokumentenprüfung;
- eine Beschreibung des Zertifizierungsaudits bezüglich des Informationssicherheits-Risikomanagements des Kunden;
- Abweichungen vom Auditplan (z. B. mehr oder weniger Zeit für bestimmte geplante Aktivitäten);
- der Geltungsbereich des ISMS
- signifikante Auditvorgehensweisen und genutzte Auditmethoden;
- Beobachtungen, sowohl positiv (z. B. bemerkenswerte Eigenschaften) als auch negativ (z. B. mögliche Nichtkonformitäten).
- die Kommentierung zur Konformität des ISMS des Kunden mit den Zertifizierungsanforderungen mit einer klaren Aussage zu Nichtkonformitäten, ein Verweis auf die Version der Erklärung zur Anwendbarkeit und gegebenenfalls alle nützlichen Vergleiche mit den Ergebnissen früherer Zertifizierungsaudits des Kunden.

Ausgefüllte Fragebögen, Checklisten, Beobachtungen, Protokolle oder Audit-Notizen können ein integraler Bestandteil des Auditberichts sein. Wenn diese Methoden verwendet werden, müssen diese Unterlagen der Zertifizierungsstelle als Nachweise vorgelegt werden, um die Zertifizierungsentscheidung zu unterstützen.

Informationen zu den während des Audits bewerteten Stichproben sind ebenso im Auditbericht oder in anderen Zertifizierungsdokumenten enthalten. Im Bericht wird die Angemessenheit der internen Organisation und der Verfahren, die geeignet sind das Vertrauen in die ISMS des Kunden sicherzustellen, betrachtet.

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

Abschließend umfasst der Auditbericht:

- - eine Zusammenfassung der wichtigsten Beobachtungen, sowohl positiv als auch negativ in Bezug auf die Umsetzung und Wirksamkeit der ISMS-Anforderungen und Maßnahmen,
- - die Empfehlung des Auditteams, ob das ISMS des Kunden zertifiziert werden sollte zertifiziert oder nicht, mit Informationen, die diese Empfehlung untermauern.

4.8. Beurteilung der Audit-Feststellungen und -schlussfolgerungen

4.8.1. Analyse der Ursachen von Nichtkonformitäten und Bewertung von Korrekturen

Die ConformityZert GmbH fordert vom Kunden, die Ursachen zu analysieren und die spezifischen, durchgeführten oder geplanten Korrekturen und Korrekturmaßnahmen zu beschreiben, um die erkannten Nichtkonformitäten in einem festgelegten Zeitraum zu beseitigen.
Die ConformityZert GmbH bewertet die vom Kunden vorgelegten Korrekturen und Korrekturmaßnahmen, um festzustellen ob sie annehmbar sind. Die Wirksamkeit aller durchgeführten Korrekturen und Korrekturmaßnahmen wird verifiziert. Die erlangten Nachweise, die zeigen, dass die Nichtkonformitäten behoben wurden, werden aufgezeichnet. Der Kunde wird über das Ergebnis der Überprüfung und Verifizierung informiert
Die auditierte Organisation wird ebenso informiert, wenn ein zusätzliches vollständiges Audit, ein zusätzliches eingeschränktes Audit oder dokumentierte Nachweise (zu bestätigen während zukünftiger Überwachungsaudits) erforderlich sind, um wirksame Korrekturen und Korrekturmaßnahmen nachprüfen zu können.

4.8.2. Maßnahmen vor der Zertifizierungsentscheidung

Bevor die Entscheidung getroffen wird, bestätigt die ConformityZert GmbH, dass:

- die durch das Auditteam bereitgestellten Informationen im Hinblick auf die Zertifizierungsanforderungen und den Geltungsbereich ausreichend sind;

- sie die Durchführung zufriedenstellender Korrekturen und Korrekturmaßnahmen für alle diejenigen Nichtkonformitäten bewertet, angenommen und verifiziert hat, die einen der folgenden Punkte darstellen:
  a) das Nichteinhalten einer oder mehrerer Anforderungen der ISO/IEC 27001:2013 oder
  b) eine Situation, die erhebliche Zweifel an der Fähigkeit des ISMS des Kunden aufwirft, die beabsichtigten Ergebnisse zu erreichen;

- sie für alle anderen Nichtkonformitäten die geplanten Korrekturen und Korrekturmaßnahmen bewertet und angenommen hat.

4.8.3. Information als Grundlage zur Erteilung der Erstzertifizierung

Die Informationen, die das Auditteam der ConformityZert GmbH für die Zertifizierungsentscheidung bereitstellt, enthalten:

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

- die Auditberichte;
- Anmerkungen zu den Nichtkonformitäten und, wo zutreffend, zu Korrekturen und Korrekturmaßnahmen, die vom Kunden ergriffen wurden;
- Bestätigung der an die ConformityZert GmbH gelieferten Informationen, die in der Antragsprüfung verwendet wurden und
- eine Empfehlung, ob die Zertifizierung gewährt werden soll oder nicht, zusammen mit Bedingungen bzw. Beobachtungen.

4.9. Zertifizierungsentscheidung/ Erteilung der Zertifizierung

Die ConformityZert GmbH trifft die Entscheidung über die Zertifizierung auf der Grundlage der Beurteilung der Auditfeststellungen und Schlussfolgerungen sowie weiterer relevanter Informationen (z. B. öffentliche Informationen, Stellungnahmen des Kunden zum Auditbericht).
Die ConformityZert GmbH trifft Entscheidungen über die Erneuerung der Zertifizierung auf der Grundlage der Ergebnisse des Re-Zertifizierungsaudits sowie der Ergebnisse aus der Bewertung des Systems über den Zeitraum der Zertifizierung und der von den Nutzern der Zertifizierung erhaltenen Beschwerden.

Die Zertifizierungsstelle stellt sicher, dass die Personen oder Ausschüsse, die die Entscheidung über die Erteilung oder Verweigerung der Zertifizierung, Erweiterung oder Einschränkung des Geltungsbereichs der Zertifizierung, Aussetzung oder Wiederherstellung der Zertifizierung, Zurückziehung der Zertifizierung oder Erneuerung der Zertifizierung treffen, andere sind als diejenigen, die die Audits durchgeführt haben. Personen, die dazu benannt sind, über die Zertifizierung zu entscheiden, verfügen über die geeigneten Kompetenzen (s. Kompetenzbewertung und -beurteilung, CZ_Personal-Einsatz-Prozess).

Alle Personen, die von der Zertifizierungsstelle beauftragt werden, eine Zertifizierungsentscheidung zu treffen, sind bei der Zertifizierungsstelle angestellt.

Die Personen oder Gremien, die die Zertifizierungsentscheidung treffen, richten sich in der Regel auch nach einer negativen Empfehlung des Auditteams. Die Zertifizierungsstelle dokumentiert die Grundlage für eine der Empfehlung nicht entsprechenden Entscheidung sowie deren Rechtfertigung.

Die Zertifizierung wird Kunden nicht gewährt, bis genügend Nachweise vorliegen, dass Planungen für Management-Reviews und interne ISMS-Audits durchgeführt wurden, diese wirksam sind und beibehalten werden.

4.9.1. Erteilung der Zertifizierung

Der Auditbericht sowie alle gesammelten Auditnachweise werden nach Abschluss aller Audittätigkeiten an die ConformityZert GmbH übergeben. Im Rahmen des

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

Zertifizierungsprozesses wird eine entsprechende Zertifizierungsentscheidung getroffen.

Die Zertifizierungsstelle zeichnet jede Zertifizierungsentscheidung einschließlich zusätzlicher Informationen oder Klarstellungen, die vom Auditteam oder von anderen Quellen erfragt wurden, auf. Die Aufzeichnungen sind in der jeweiligen Kundenakte abgelegt.

4.10. Durchführung von Überwachungstätigkeiten

4.10.1. Aufrechterhaltung der Zertifizierung

Die Zertifizierungsstelle erhält die Zertifizierung aufgrund der Darlegung, dass der Kunde weiterhin die Anforderungen der DIN ISO/IEC 27001:2015 erfüllt, aufrecht.

Die Zertifizierung eines Kunden wird auf der Grundlage einer positiven Schlussfolgerung des Auditteamleiters im Rahmen des Überwachungsaudits ohne weitere unabhängige Bewertung und Entscheidung aufrechterhalten werden. Voraussetzungen hierzu sind:

- dass die Regelungen, die zu einer Aussetzung oder zur Zurückziehung der Zertifizierung führen könnten, berücksichtigt sind. In einem solchen Fall berichtet der Auditteamleiter an die Zertifizierungsstelle und fordert, dass eine Bewertung durch kompetentes Personal notwendig ist. Dieses Personal unterscheidet sich von dem, welches das Audit durchgeführt hat. Im Rahmen der Bewertung wird ermittelt, ob die Zertifizierung aufrechterhalten werden kann

- kompetentes Personal der Zertifizierungsstelle überprüft deren Überwachungstätigkeiten, einschließlich der Überwachung der Berichterstellung durch die Auditoren, um zu bestätigen, dass die Zertifizierungstätigkeiten in wirksamer Weise durchgeführt wurden.

Änderungen bezüglich des zertifizierten Kunden und seines ISMS werden berücksichtigt.

Grundsätzlich verfolgen die Überwachungstätigkeiten zur Aufrechterhaltung der Zertifizierung die folgenden Ziele:

- Feststellung der Wirksamkeit des ISMS hinsichtlich der Erreichung der Ziele der Informationssicherheitspolitik;

- Feststellung der Funktionsfähigkeit der Verfahren für die regelmäßige Bewertung sowie Überprüfung der Einhaltung der einschlägigen Gesetze und Vorschriften;

- Feststellung von Änderungen an den ermittelten Maßnahmen, und die daraus resultierenden Änderungen der SoA;

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

- Feststellung der Umsetzung und der Wirksamkeit der Maßnahmen in Übereinstimmung mit dem Auditprogramm.

Das Überwachungsprogramm kann hinsichtlich der Informationssicherheitsaspekte in Bezug zu Risiken und Auswirkungen auf den Kunden angepasst werden. Die Anpassung wird entsprechend dokumentiert und begründet.

4.10.2. Überwachungstätigkeiten

Die Überwachungstätigkeiten der ConformityZert GmbH beinhalten insbesondere Vor-Ort-Audits zur Begutachtung des ISMS des zertifizierten Kunden bezüglich der spezifischen Anforderungen DIN ISO/IEC 27001:2015.

Weitere Überwachungstätigkeiten sind:

- Anfragen an den zertifizierten Kunden zu Aspekten der Zertifizierung,
- Bewertung der Angaben des Kunden im Hinblick auf seine Tätigkeiten (z.B. Werbematerial, Webseiten),
- Aufforderungen an den Kunden zur Bereitstellung von Dokumenten und Aufzeichnungen (auf Papier oder elektronischen Medien), und
- andere Mittel zur Überwachung der Leistungsfähigkeit des zertifizierten Kunden.

4.10.3. Überwachungsaudits

Überwachungsaudits werden mindestens einmal im Jahr durchgeführt. Das Datum des ersten Überwachungsaudits, das der Erstzertifizierung folgt, darf nicht mehr als 12 Monate nach dem letzten Tag des Audits der Stufe 2 liegen.

Überwachungsaudits sind Vor-Ort-Audits, stellen aber nicht notwendigerweise vollständige Systemaudits dar und werden zusammen mit den anderen Überwachungstätigkeiten geplant, sodass die ConformityZert GmbH das Vertrauen aufrecht erhalten kann, dass das zertifizierte ISMS zwischen den Re-Zertifizierungsaudits weiterhin die Anforderungen erfüllt.

Das Verfahren der Überwachungsaudits ist konsistent zu den Kriterien für das Verfahren für Zertifizierungsaudits.

Überwachungsaudits werden durchgeführt,

- um zu bestätigen, dass das zertifizierte ISMS weiterhin umgesetzt wird,
- die Auswirkungen von Änderungen am ISMS als Folge von Änderungen im Geschäftsbetrieb des Kunden entstanden sind und
- um die kontinuierliche Einhaltung der Zertifizierungsanforderungen zu bestätigen.

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

Das Überwachungsaudit-Programm umfasst:

- die Aufrechterhaltung der ISMS-Elemente wie Informationssicherheits-Risikobewertung und Aufrechterhaltung von Maßnahmen, internes ISMS-Audit, Managementbewertung und Korrekturmaßnahmen
- eine Bewertung der ergriffenen Maßnahmen zu Nichtkonformitäten, die während des vorhergehenden Audits festgestellt wurden,
- Mitteilungen von externen Parteien gem. DIN ISO/IEC 27001:2015 und anderen für die Zertifizierung relevanten Vorgaben
- Änderungen des dokumentierten Systems
- Einzelne ISMS-Bereiche, soweit Änderungen vorliegen
- Einzelne, ausgewählte Anforderungen der DIN ISO/IEC 27001:2015
- Andere, ausgewählte Bereiche, falls erforderlich
- Aufzeichnungen zur Behandlung von Beschwerden und Einsprüchen sowie entsprechender Korrekturmaßnahmen,
- Wirksamkeit des ISMS im Hinblick auf das Erreichen der Ziele des zertifizierten Kunden,
- Fortschritt bei geplanten Tätigkeiten, die auf eine ständige Verbesserung zielen,
- anhaltende Betriebssteuerung/-lenkung;
- Bewertung von Änderungen, und
- Nutzung von Zeichen und/oder andere Verweise auf die Zertifizierung.

Der Überwachungs-Auditbericht enthält insbesondere Informationen über die Behebung von Nichtkonformitäten, den aktuellen Stand der SoA und wichtige Änderungen zum vorhergehenden Audit. Sie decken hierbei mindestens vollständig die Inhalte des Auditprogramms ab.

4.10.4. Aussetzung, Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung

Die ConformityZert GmbH setzt die Zertifizierung in den Fällen aus, wenn

- ein zertifiziertes ISMS eines Kunden die Zertifizierungsanforderungen – einschließlich der Anforderungen an die Wirksamkeit des Managementsystems – dauerhaft oder schwerwiegend nicht erfüllt,

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

- der zertifizierte Kunde die Durchführung der Überwachungs- oder Re-Zertifizierungsaudits, die in der erforderlichen Häufigkeit durchzuführen sind, nicht gestattet, oder

- der zertifizierte Kunde freiwillig um eine Aussetzung gebeten hat.

Bei Aussetzung ist die Zertifizierung des ISMS des Kunden zeitweise außer Kraft gesetzt. Wenn die Probleme, die zur Aussetzung geführt haben, in einem von der ConformityZert GmbH vorgegebenen Zeitraum nicht gelöst worden sind, führt dies zur Zurückziehung oder Einschränkung des Geltungsbereichs der Zertifizierung.

Der Geltungsbereich der Zertifizierung des Kunden wird eingeschränkt, um diejenigen Teile auszuschließen, die die Anforderungen nicht erfüllen, wenn der zertifizierte Kunde es dauerhaft oder schwerwiegend versäumt hat, die Zertifizierungsanforderungen für diese Teile des Geltungsbereichs der Zertifizierung zu erfüllen. Eine solche Einschränkung erfolgt in Übereinstimmung mit den Anforderungen der DIN ISO/IEC 27001:2015.

4.11. Stichprobenprüfung bei Multi-Standort-Organisationen

4.11.1. Festlegung von Stichproben

Diese Regelung behandelt keine Organisationen mit mehreren Standorten, in denen mehrere Managementsysteme in der Organisation eingesetzt werden. Für diesen Fall ist jeder Standort als Organisation mit einem Standort zu erachten und entsprechend zu auditieren.
Diese Regelung gilt nicht in den Fällen, in denen unabhängige Organisationen von einer anderen unabhängigen Organisation (z. B. einem Beratungsunternehmen oder einer künstlichen Organisation) unter dem Dach eines einzigen Managementsystems zusammengefasst werden.

Eine Muti-Standort-Organisation ist eine Organisation mit einem einzigen Managementsystem, die eine festgelegte Zentrale hat (nicht notwendigerweise der Hauptsitz der Organisation), in der bestimmte Prozesse/Tätigkeiten geplant und kontrolliert werden, sowie eine Reihe von (permanenten, temporären oder virtuellen) Standorten, an denen solche Prozesse/Tätigkeiten vollständig oder teilweise ausgeführt werden.

Der Scope eines einzelnen Standorts kann derselbe sein, wie der vollständige Scope einer Multi-Standort-Organisation, er kann aber auch nur ein kleiner Teil des Scopes der Multi-Standort-Organisation sein.

Eine Multi-Standort-Organisation muss keine einzelne Rechtsperson sein, allerdings müssen alle Standorte eine rechtliche oder vertragliche Bindung mit der Zentrale der Organisation haben, und einem gemeinsamen Managementsystem unterliegen, das durch die Zentrale festgelegt und eingerichtet wird und der regelmäßigen Überwachung sowie interner Audits durch die Zentrale unterliegt. Das bedeutet, dass die Zentrale das

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

Recht besitzt, von den Standorten zu fordern, Korrekturmaßnahmen umzusetzen, wenn dies an einem Standort erforderlich ist. Gegebenenfalls sollte dies in der formellen Vereinbarung zwischen der Zentrale und den Standorten festgehalten werden.

Eine sachgerechte Stichprobe von Standorten ist auf die Standorte beschränkt, die sehr gleichartige Prozesse/Tätigkeiten durchführen und die zum Geltungsbereich der Organisation gehören.

Die Eignung einer Multi-Standort-Organisation für die Zertifizierung wird im Rahmen des Zertifizierungsantrags und des hierzu auszufüllenden Fragebogens (Anhang B des Zertifizierungsantrags) überprüft.

Stichprobenverfahren werden dann eingeschränkt, wenn diese nicht angemessen sind, ausreichend Vertrauen in die Effektivität des zu auditierenden Managementsystems zu schaffen. Solche Einschränkungen sind im Hinblick auf folgende Faktoren festgelegt:

- Geltungsbereiche oder Prozesse/Tätigkeiten (d. h. basierend auf der Beurteilung der Risiken oder der mit dem Bereich oder den Tätigkeiten verbundenen Komplexität),
- Größe der Standorte, die für die Multi-Standort-Auditierung geeignet sind,
- Abweichungen bei der lokalen Umsetzung des Managementsystems, um unterschiedliche Prozesse/Tätigkeiten oder vertragliche oder rechtliche Gegebenheiten zu berücksichtigen, und
- Nutzung zeitweiliger Standorte, die unter dem Managementsystem der Organisation tätig sind, auch wenn sie nicht in den Zertifizierungsdokumenten aufgeführt sind.

Die Festlegung der Stichproben erfolgt zum Teil selektiv auf Basis der nachstehenden Faktoren und zum Teil nach dem Zufallsprinzip; sie gewährleistet im Ergebnis eine repräsentative Auswahl der unterschiedlichen Standorte und stellt sicher, dass alle im Zertifizierungsumfang enthaltenen Prozesse auditiert werden.

Mindestens 25 % der Stichproben werden nach dem Zufallsprinzip ausgewählt.

Unter Berücksichtigung der nachstehend genannten Bestimmungen wird der Rest so ausgewählt, dass die Unterschiede der Standorte, die über den Gültigkeitszeitraum des Zertifikats ausgewählt werden, so groß wie möglich sind.

Bei der Auswahl der Standorte werden u. a. folgende Aspekte beachtet:

- Ergebnisse interner Audits an den Standorten und Managementbewertungen oder frühere Zertifizierungsaudits,
- Aufzeichnungen zu Beschwerden und anderen relevanten Aspekten zu Korrektur- und vorbeugenden Maßnahmen,
- signifikante Unterschiede in der Größe der Standorte,
- Unterschiede im Geschäftszweck der Standorte,
- Abweichungen in Schichtmodellen und Arbeitsverfahren,
- Unterschiede in den durchgeführten Aktivitäten

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

- Unterschiede in der Gestaltung und dem Betrieb der Maßnahmen
- Komplexität des Managementsystems und der Prozesse, die an den Standorten durchgeführt werden,
- mögliche Wechselwirkungen mit kritischen Informationssystemen oder Informationssystemen, die sensible Informationen verarbeiten
- Modifikationen seit dem letzten Zertifizierungsaudit,
- Reifegrad des Managementsystems und Kenntnisse über die Organisation,
- Risikosituation der Standorte
- Sicherheitsvorfälle an den spezifischen Standorten
- Unterschiede in der Kultur, Sprache und den gesetzlichen Regelungen und
- geografische Standortverteilung und
- handelt es sich um permanente, temporäre oder virtuelle Standorte.

Die Auswahl muss nicht zu Beginn des Auditprozesses erfolgen. Sie kann auch erfolgen, wenn die Auditierung in der Zentrale abgeschlossen ist. Auf jeden Fall muss die Zentrale über die Standorte informiert werden, die Teil der Stichprobenprüfung sein sollen. Dies kann relativ kurzfristig erfolgen, sollte aber ausreichend Zeit zur Vorbereitung auf das Audit lassen.

Die Mindestanzahl an Standorten, die pro Audit zu begehen sind, ist:

- Erstaudit: der Umfang der Stichprobe muss die Quadratwurzel der Anzahl der Standorte sein: ($y=\sqrt{x}$), gerundet auf die höhere ganze Zahl, wobei y = die Anzahl an Standorten ist, die in die Stichprobe aufzunehmen sind und x = die Gesamtanzahl an Standorten.

- Überwachungsaudit: der Umfang der jährlichen Stichprobe muss die Quadratwurzel der Anzahl der Standorte sein, multipliziert mit dem Faktor von 0,6 als Koeffizient ($y=0{,}6\ \sqrt{x}$), aufgerundet auf die nächste ganze Zahl.

- Re-Zertifizierungsaudit: der Umfang der Stichprobe muss der gleiche sein, wie bei einem Erstaudit. Dennoch kann, wenn sich das Managementsystem über den Zertifizierungszeitraum als effektiv erwiesen hat, der Umfang der Stichprobe reduziert werden auf $y=0{,}8\ \sqrt{x}$, aufgerundet auf die nächste ganze Zahl.

Die Zentrale wird während jeder Erstzertifizierung und jedem Re-Zertifizierungsaudit und mindestens einmal pro Kalenderjahr als Teil der Überwachung auditiert.

Wenn die Organisation ein hierarchisches System von Zweigniederlassungen hat (z. B. eine Hauptniederlassung (Zentrale), nationale Geschäftsstellen, regionale Geschäftsstellen, lokale Zweigstellen), so wird das oben definierte Stichprobenmodell für das Erstaudit auf jeder Ebene angewendet.

Das Stichprobenverfahren ist Teil des Managements des Auditprogramms. Die Zertifizierungsstelle überprüft zu jeder Zeit (d. h. vor der Planung des Überwachungsaudits oder wenn ein Standort der Organisation seine Struktur ändert bzw. bei der Übernahme eines neuen Standorts/mehrerer neuer Standorte, die in den

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

Zertifizierungsrahmen aufgenommen werden) die im Auditprogramm vorgesehenen Stichproben, um festzustellen, ob im Hinblick auf die Aufrechterhaltung der Zertifizierung Anpassungen am Umfang der Stichprobe erforderlich sind.

Bei Beantragung der Aufnahme neuer Standorte oder einer neuen Gruppe von Standorten in eine bestehende zertifizierte Multi-Standort-Organisation legt die Zertifizierungsstelle die erforderlichen Tätigkeiten fest, bevor der/die neue(n) Standort(e) in das Zertifikat aufgenommen werden kann/können. Dazu gehört die Erwägung, ob der/die neue(n) Stand-ort(e) zu auditieren ist/sind oder nicht. Nach der Aufnahme des neuen Standorts/der neuen Standorte in das Zertifikat, wird der Umfang der Stichprobe für zukünftige Überwachungs- oder Re-Zertifizierungsaudits festgelegt.

4.11.2. Auditierung einer Multi-Standort-Organisation, bei der das Strichprobenverfahren nach 4.11.1 nicht geeignet ist

Das Auditprogramm sieht ein Erstaudit und ein Re-Zertifizierungsaudit für alle Standorte vor. Bei Überwachungsaudits werden 30 % aller Standorte, gerundet auf die nächste ganze Zahl, in einem Kalenderjahr auditiert. Jedes Audit umfasst die Zentrale. Die für das zweite Überwachungsaudit ausgewählten Standorte unterscheiden sich in der Regel von denjenigen Standorten, die für das erste Überwachungsaudit ausgewählt wurden.
Das Auditprogramm ist so gestaltet, dass alle vom Geltungsbereich der Zertifizierung umfassenden Prozesse in jedem Zyklus auditiert werden.

Bei Beantragung der Aufnahme eines neuen Standorts in eine bereits zertifizierte Multi-Standort-Organisation wird dieser Standort neben der Aufnahme in das Auditprogramm der Organisation auditiert, bevor er in das Zertifikat aufgenommen wird. Nach der Aufnahme des neuen Standorts in das Zertifikat, wird der Standort zu den vorhandenen hinzugezählt, um die Auditzeit für zukünftige Überwachungs- und Re-Zertifizierungsaudits festzulegen.

4.11.3. Auditierung von Multi-Standort-Organisationen, zu denen eine Kombination aus Standorten gehören, die für das Stichprobenverfahren geeignet sind und Standorten, die nicht für das Stichprobenverfahren geeignet sind

Das Auditprogramm wird mit Hilfe der Angaben in 4.11.1 für diejenigen Standorte festgelegt, die für das Stichprobenverfahren geeignet sind und 4.11.2 gilt für den übrigen Teil der Organisation, wenn 4.11.1 nicht angewendet werden kann.

4.11.4. Audit und Zertifizierung

Bei der Festlegung des Auditprogramms kalkuliert die Zertifizierungsstelle ausreichend zusätzliche Zeit für Tätigkeiten ein, die nicht Teil der berechneten Auditzeit sind, wie Reisen, Kommunikation unter den Mitgliedern des Auditteams, Sitzungen nach dem Audit usw., die auf Grund der besonderen Konfiguration der zu auditierenden Organisation erforderlich sind.

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

Wenn das Auditteam, bestehend aus mehr als einem Mitglied, zu unterschiedlichen Zeitpunkten eingesetzt wird, ermittelt die Zertifizierungsstelle, gemeinsam mit dem Teamleiter die technischen Kompetenzen, die für jeden Teil des Audits bzw. für jeden Standort erforderlich sind und weist dementsprechend die geeigneten Teammitglieder für jeden Teil des Audits zu.

Zusätzlich zu der Anforderung in ISO/IEC 17021-1:2015 Abschnitt 9.2.3 berücksichtigt die Zertifizierungsstelle bei der Erstellung des Auditplans mindestens Folgendes:

- den Geltungsbereich der Zertifizierung und Teilbereiche für jeden Standort,
- die Managementsystemnormen für jeden Standort, sofern mehrere Managementsystemnormen Berücksichtigung finden,
- die zu auditierenden Prozesse/Tätigkeiten,
- die Auditzeit für jeden Standort, und
- das zugewiesene Auditteam

Erstaudit: Stufe 1
Während der Stufe 1 hat das Auditteam die Informationen zu vervollständigen, um

- das Auditprogramm zu bestätigen,
- die Stufe 2 zu planen, wobei die an jedem Standort zu auditierenden Prozesse/Tätigkeiten zu berücksichtigen sind, und
- zu bestätigen, dass das Auditteam der Stufe 2 über die erforderliche Kompetenz verfügt.

Erstaudit: Stufe 2
Mit dem Ergebnis des Erstaudits dokumentiert das Auditteam, welche Prozesse in jedem besuchten Standort auditiert wurden. Diese Informationen werden verwendet, um das Auditprogramm entsprechend zu ändern und die Auditpläne für nachfolgenden Überwachungsaudits zu erstellen.

4.11.5. Nichtkonformitäten und Zertifizierung

Wenn, wie in ISO/IEC 17021-1:2015 definiert, Nichtkonformitäten an einzelnen Standorten gefunden werden, entweder während des internen Audits der Organisation oder während der Auditierung durch die Zertifizierungsstelle, muss ermittelt werden, ob die anderen Standorte ebenfalls betroffen sein können. Aus diesem Grund fordert die Zertifizierungsstelle von der Organisation, dass diese ihre Nichtkonformitäten überprüft, um festzustellen, ob diese ein allgemeines Defizit des Gesamtsystems, welches auch auf andere Standorte zutrifft, darstellen oder nicht. Falls festgestellt wird, dass dies der Fall ist, so müssen Korrekturmaßnahmen durchgeführt und geprüft werden, und zwar sowohl in der Zentrale, als auch an den einzelnen betroffenen Standorten. Falls festgestellt wird, dass dies nicht der Fall ist, muss die Organisation in der Lage sein, gegenüber der Zertifizierungsstelle nachzuweisen, dass eine Einschränkung der Folgemaßnahmen gerechtfertigt ist.

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

Die Zertifizierungsstelle fordert den Nachweis dieser Maßnahmen und erhöht die Häufigkeit ihrer Stichproben und/oder den Umfang der Stichproben, bis sie sich überzeugt hat, dass die Kontrolle wieder hergestellt ist.

Falls zum Zeitpunkt des Entscheidungsprozesses einer der Standorte eine wesentliche Nichtkonformität aufweist, wird die Zertifizierung gegenüber der gesamten Multi-Standort-Organisation verweigert, bis zufriedenstellende Korrekturmaßnahmen umgesetzt wurden.

Es ist nicht erlaubt, dass die Organisation einen „problematischen“ Standort während des Zertifizierungsprozesses ausschließt, um die Hindernisse, die durch die Existenz einer Nichtkonformität bei einem einzelnen Standort aufgetreten sind, zu überwinden.

4.11.6. Zertifizierungsdokumente

Die Zertifizierungsdokumente enthalten den Geltungsbereich der Zertifizierung und die Standorte/Rechtspersonen (falls erforderlich), die durch die Multi-Standort-Zertifizierung abgedeckt sind.

Die Zertifizierungsdokumente enthalten den Namen und die Adresse aller Standorte und spiegeln die Organisation wider, auf die sich die Zertifizierungsdokumente beziehen. Der Geltungsbereich oder die sonstigen Referenzen auf diesen Dokumenten machen deutlich, dass die zertifizierten Tätigkeiten durch die auf der Liste aufgeführten Standorte ausgeführt werden. Wenn Aktivitäten eines Standortes nur einen Teil des Geltungsbereiches der Organisation beinhalten, beinhaltet das Zertifizierungsdokument den Teilbereich des Standortes. Wenn zeitweilige Standorte in den Zertifizierungsdokumenten aufgeführt sind, so werden diese als zeitweilige Standorte gekennzeichnet.

Wenn Zertifizierungsdokumente nur für einen Standort ausgestellt werden, enthalten sie Folgendes:

- dass es sich bei dem zertifizierten Managementsystem um das der gesamten Organisation handelt,
- dass die Zertifizierung die Tätigkeiten abdeckt, die an diesem besonderen Standort/der Rechtsperson ausgeführt werden,
- die Rückverfolgbarkeit mit dem Hauptzertifikat, z. B. einen Code und
- eine Erklärung, aus der hervorgeht, dass „die Gültigkeit dieses Zertifikats von der Gültigkeit des Hauptzertifikats abhängig ist“.

Dieses Zertifizierungsdokument wird unter keinen Umständen auf den Namen des Standorts/der Rechtsperson ausgestellt oder deutet an, dass dieser Standort/die Rechtsperson zertifiziert ist (zertifiziert ist die Kundenorganisation). Darin kann auch keine Konformitätserklärung der Prozesse/Tätigkeiten des Standorts mit dem normativen Dokument enthalten sein.

Die Zertifizierungsdokumentation wird vollständig zurückgezogen, falls auch nur ein Standort die erforderlichen Bestimmungen zur Aufrechterhaltung der Zertifizierung nicht mehr erfüllt.

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de

4.11.7. Überwachungsaudit

Die Überwachung von Multi-Standort-Organisationen, die für das Stichprobenverfahren geeignet sind, wird gemäß 4.11.1 auditiert. Die Auditzeit pro Standort wird gemäß 4.11.1 berechnet.

Die Überwachung von Multi-Standort-Organisationen, die nicht gemäß 4.11.1 für das Stichprobenverfahren geeignet sind, erfolgt durch die Auditierung von 30 % der Standorte zuzüglich der Zentrale. Die für die zweite Überwachung eines Zertifizierungszyklus ausgewählten Standorte dürfen normalerweise keine Standorte enthalten, die im Rahmen des ersten Überwachungsaudits in die Stichprobenprüfung aufgenommen wurden. Die Auditzeit pro Standort ist gemäß 4.11.1 zu berechnen.

4.11.8. Re-Zertifizierungsaudits

Die Re-Zertifizierung von Multi-Standort-Organisationen, die für das Stichprobenverfahren geeignet sind, erfolgt durch ein Audit, das gemäß 4.11.1 erfolgt. Die Auditzeit pro Standort ist gemäß 4.11.1 zu berechnen.

Die Re-Zertifizierung von Multi-Standort-Organisationen, die nicht für das Stichprobenverfahren geeignet sind, hat durch ein Audit zu erfolgen, das wie ein Erstaudit durchgeführt wird, d. h. alle Standorte und die Zentrale sind zu auditieren. Die Auditzeit pro Standort und für die Zentrale ist gemäß 4.11.1 zu berechnen.

ConformityZert GmbH
Geschäftsführung: Daniela Schmidt
Amtsgericht Mainz HRB 49019, USt-ID: DE307883888

Tel +49(0) 6138 / 94298-0
Fax +49(0) 6138 / 94298 -999
kontakt@conformityzert.de
www.conformityzert.de