



Zertifizierungsschema Y03

Managementsysteme

Compliance/Governance von Organisationen

Ausgabe 7.0:2021-04-15

Medieninhaber und Hersteller

Austrian Standards plus GmbH Heinestraße 38, 1020 Wien

Copyright© Austrian Standards plus GmbH 2021 All rights reserved.

E-Mail: certification@austrian-standards.at

Internet: www.austrian-standards.at

Inhaltsverzeichnis

1 Anwendungsbereich	4
2 Zertifizierungsprozess	4
2.1 Antragstellung	4
2.2 Prüfung des Antrags	5
2.3 Erstzertifizierung	5
2.3.1 Audit – Stufe 1	5
2.3.2 Audit der Stufe 2	6
2.4 Durchführung von Audits	6
2.4.1 Allgemeines	6
2.4.2 Stichprobenprüfung an mehreren Standorten - Multi-site Audits	7
2.4.3 Grundlegende Aufgaben des Auditteams	7
2.4.4 Zu auditierende Funktionen	7
2.4.5 Unterlagenprüfung	7
2.4.6 Kommunikation während des Audits	8
2.4.7 Auditschlussfolgerungen	8
2.4.8 Korrekturmaßnahmen	8
2.4.9 Empfehlungen zur Wirksamkeit des Managementsystems	9
2.4.10 Abschlussbesprechung	9
2.5 Auditbericht zur Erstzertifizierung	9
2.6 Entscheidung über die Zertifizierung	10
2.6.1 Bewertungsprozess	10
2.6.2 Ausstellung des Zertifikates	10
2.7 Überwachungsaktivitäten	10
2.7.1 Überwachungsaudits	10
2.7.2 Bewertung durch die Zertifizierungsstelle	11
2.8 Rezertifizierung	11
2.8.1 Rezertifizierungsprozess	11
2.8.2 Rezertifizierungsaudit	11
2.8.3 Auditbericht zum Rezertifizierungsaudit	11
2.8.4 Zertifikatsausstellung	12
2.9 Außerordentliche Audits	12
2.10 Änderungen der Zertifizierungsgrundlagen	12



2.11 Änderungen im Geltungsbereich von Zertifikaten	12
2.12 Zurückziehung von Zertifikaten	13
2.13 Vorgehensweise bei der Übernahme von Zertifikaten	13
Anhang A Übergangsbestimmungen.....	14

1 Anwendungsbereich

Dieses Zertifizierungsschema legt die Vorgangsweise zur Zertifizierung eines Managementsystems (MS) im Bereich Compliance/Governance von Organisationen durch die Zertifizierungsstelle von Austrian Standards (AS+C) fest.

Für die Durchführung eines Zertifizierungsverfahrens gelten die Anforderungen der Internationalen Norm ISO/IEC 17021-1¹.

Anmerkung: Die Austrian Standard plus GmbH als Zertifizierungsstelle ist akkreditiert für die folgenden Standards:

- ISO 37001:2016-10 Anti-Korruptions-Managementsysteme.

Haftungsausschluss: Die Anwendung der in Abschnitt 2 genannten normativen Dokumente soll Organisationen dabei unterstützen, innerhalb einer Organisation ein wirksames Managementsystem zu implementieren, welches die Wahrscheinlichkeit von Regelverstößen durch Organisationsmitglieder deutlich reduziert. Diese Anwendung, aber auch eine Zertifizierung nach dem vorliegenden Zertifizierungsschema stellt keine Garantie dafür dar, dass alle Mitglieder der zertifizierten Organisation stets konform handeln. Ein Managementsystem und dessen Zertifizierung können vorsätzliches Fehlverhalten und regelwidrige Handlungen von Mitgliedern einer Organisation nicht gänzlich verhindern. Eine Haftung der Austrian Standards plus GmbH und der Auditoren ist ausgeschlossen.

2 Zertifizierungsprozess

2.1 Antragstellung

2.1.1 Der Antragsteller muss die Einleitung des Zertifizierungsverfahrens mittels eines von der Zertifizierungsstelle zur Verfügung gestellten Antragsformulars beantragen.

2.1.2 Der Antragsteller muss eine bevollmächtigte Kontaktperson für die Durchführung des Zertifizierungsverfahrens benennen.

2.1.3 Der Umfang eines beantragten Zertifizierungsverfahrens bestimmt sich durch folgende Parameter:

- Identifikation der juristischen Person, die Inhaber des Zertifikates ist,
- Geltungsbereich des angestrebten Zertifikates in Bezug auf die Organisation bzw. Untereinheiten der Organisation,
- Standorte der zu zertifizierenden Organisation,
- Compliance-Risikobereiche, die in den Geltungsbereich des Zertifikates aufgenommen werden sollen.

Zertifizierungsverfahren von mehreren, miteinander verbundenen juristischen Personen können gebündelt werden.

Zusammen mit dem Antrag muss der Antragsteller folgende Informationen über das zu zertifizierende Managementsystem dokumentieren. Diese Dokumentation muss das folgende umfassen:

- a. den gewünschten Geltungsbereich der Zertifizierung;
- b. die allgemeinen Merkmale der antragstellenden Organisation, einschließlich deren Name sowie die Anschrift(en) ihres/ihrer physischen Standort(e)s, bedeutsame Aspekte ihrer Prozesse und Tätigkeiten sowie alle maßgeblichen rechtlichen Verpflichtungen;
- c. allgemeine Informationen bezüglich der antragstellenden Organisation, die für den beantragten Zertifizierungsbereich relevant sind, wie z. B. ihre Tätigkeiten, personelle und technische Ressourcen, Funktionen und Beziehungen in einer größeren Körperschaft, falls gegeben;

¹ ISO/IEC 17021-1:2015 Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren - Teil 1: Anforderungen

- d. Informationen bezüglich aller ausgegliederten Prozesse, die von der Organisation genutzt werden und die Konformität mit den Anforderungen beeinflussen;
- e. Informationen über das MS betreffende Beratungsleistungen, die von der Organisation in Anspruch genommen wurden, und durch wen diese Leistungen durchgeführt wurden.

2.2 Prüfung des Antrags

2.2.1 Vor Durchführung des Audits prüft die Zertifizierungsstelle den Antrag, um sicherzustellen, dass

- die Informationen über die antragstellende Organisation ausreichend für die Durchführung des Audits sind,
- alle bekannten Differenzen im Verständnis zwischen der Zertifizierungsstelle und der antragstellenden Organisation geklärt werden,
- 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.

2.2.2 Basierend auf dieser Prüfung wird die Zertifizierungsstelle die Kompetenzen ermitteln, die sie in ihrem Auditteam benötigt. Das Auditteam besteht zumindest aus einem Leitenden Auditor sowie aus Co-Auditoren nach Erfordernis.

2.2.3 Wird der Antrag von der Zertifizierungsstelle angenommen, erhält der Antragsteller eine diesbezügliche schriftliche Bestätigung.

2.3 Erstzertifizierung

2.3.1 Audit – Stufe 1

Das Audit der Stufe 1 wird durchgeführt um das eigentliche Zertifizierungsaudit (Audit der Stufe 2 gemäß Abschnitt 2.3.2) vorzubereiten. Das Audit der Stufe 1 wird vor Ort bei der zu zertifizierenden Organisation durchgeführt. Das Audit Stufe 1 kann in begründeten Fällen als Fernaudit durchgeführt werden, sofern alle Informationen zur Erreichung des Auditziels verfügbar sind.

Das Audit der Stufe 1 wird durchgeführt, um

- a. die Dokumentation des Managementsystems der Organisation zu prüfen,
- b. die Risikoanalyse und deren Scope zu überprüfen und daraus folgend die zu auditierenden Funktionen/Personengruppen für das Audit Stufe 2 zu identifizieren,
- c. die spezifischen Bedingungen der Organisation zu beurteilen, sowie Gespräche mit Mitarbeitern zu führen, um die Reife des Systems für das Audit Stufe 2 zu ermitteln,
- d. den Status der Organisation und dessen Verständnis bezüglich der Anforderungen der Normen zu bewerten,
- e. notwendige Informationen bezüglich des Geltungsbereichs des MS zu erfassen, der Prozesse und der Standorte der Organisation,
- f. die Zuteilung der Ressourcen für das Audit der Stufe 2 zu bewerten sowie die Einzelheiten der Audits abzustimmen,
- g. Schwerpunkte für die Planung des Audits der Stufe 2 festzulegen,
- h. zu beurteilen, ob interne Audits und Managementbewertungen geplant und durchgeführt werden,
- i. zu beurteilen, ob der Grad der Implementierung des Managementsystems belegt, dass die Organisation für das Audit der Stufe 2 reif ist.

Auditfeststellungen aus der Stufe 1 werden dokumentiert und dem Kunden mitgeteilt, einschließlich der Hinweise zu identifizierten Schwachstellen, die während des Audits der Stufe 2 als Nichtkonformität eingestuft werden könnten.

Der Leitende Auditor dokumentiert die Ergebnisse des Audits der Stufe 1 mittels der durch die Zertifizierungsstelle vorgegebenen Berichtsvorlage.

Die Zertifizierungsstelle entscheidet auf Basis des Berichts über die weitere Vorgehensweise. Der Abstand zwischen dem Audit der Stufe 1 und Audit der Stufe 2 (siehe 2.3.2) muss mindestens 2 Wochen und darf maximal 6 Monate betragen, wenn im Zuge des Audits der Stufe 1 Schwachstellen identifiziert werden, die im Zuge der Stufe 2 als Nichtkonformitäten eingestuft werden könnten. Werden die Schwachstellen innerhalb der Maximalfrist nicht in geeigneter Weise behoben, wird der Antrag abgewiesen.

2.3.2 Audit der Stufe 2

Der Zweck des Audits der Stufe 2 ist es, die Umsetzung einschließlich der Wirksamkeit des Managementsystems der Organisation zu bewerten und die Konformität des Managementsystems mit den Auditkriterien festzustellen.

Das Audit der Stufe 2 muss an dem/den Standort/en der zu zertifizierenden Organisation stattfinden.

Das Audit der Stufe muss zumindest das folgende umfassen:

- a) Informationen und Nachweise über die Konformität mit allen Anforderungen des zutreffenden Bezugsdokumentes;
- b) Überwachung der Leistung, Messung, Berichterstattung und Überprüfung in Bezug auf Ziele und Vorgaben im Rahmen des Geltungsbereichs des Managementsystems;
- c) die Fähigkeit und die Leistungsfähigkeit des Managementsystems des Kunden im Hinblick auf die Erfüllung geltender gesetzlicher, behördlicher und vertraglicher Anforderungen;
- d) Prüfung der operativen Lenkung der Prozesse des Kunden im Hinblick auf die Umsetzung der Vorgaben des Managementsystems;
- e) Prüfung des internen Audits und der Managementbewertung;
- f) Verantwortlichkeit der Leitung für die Compliance-Politik des Kunden.

2.4 Durchführung von Audits

2.4.1 Allgemeines

Zur Durchführung eines Audits wird von der Zertifizierungsstelle das Auditteam bestellt. Die Zertifizierungsstelle informiert den Kunden über die Namen und relevante Informationen des Auditteams. Der Kunde hat die Möglichkeit, bis spätestens 3 Wochen vor dem Audit, der Bestellung von Auditteammitgliedern schriftlich zu widersprechen.

Zur Planung eines Audits in Kooperation mit dem Kunden wird der Auditplan dem Kunden sowie die Daten zum Audit mit dem Kunden abgestimmt.

Audits müssen eine Eröffnungsbesprechung zu Beginn des Audits und eine Abschlussbesprechung nach Beendigung des Audits umfassen.

Teile des Audits können mit elektronischen Mitteln erfolgen (Remote-Audits). Der Einsatz von Remote-Audits wird von der Zertifizierungsstelle im Rahmen der Festlegung des Auditprogrammes festgelegt. Der während eines solchen Remote-Audits erlangte Nachweis muss ausreichend sein, um den Auditor in die Lage zu versetzen, in Kenntnis der Sachlage eine begründete Entscheidung über die Konformität mit der jeweiligen Anforderung zu treffen.

Audits sind durch eine Begleitperson der Organisation zu begleiten, sofern nichts anderes mit der Organisation vereinbart wird. Die Auditoren haben das Recht, die Begleitperson von einzelnen Teilen (Interviews) auszuschließen, um etwaige Beeinflussungen zu verhindern.

2.4.2 Stichprobenprüfung an mehreren Standorten - Multi-site Audits

Für den Fall, dass eine Organisation mehr als einen Standort betreibt, die unter dem Geltungsbereich des Managementsystem abgedeckt werden, kann eine Stichprobe aus den bestehenden Standorten für die Audits herangezogen werden.

Die Zertifizierungsstelle legt die Anzahl und die Örtlichkeiten der zu auditierenden Standorte fest. Es müssen alle Funktionen der Organisation gemäß Abschnitt 2.4.4 durch das Audit abgedeckt werden können.

Standorte die von Unterauftragnehmern im Namen und Auftrag der Organisation betrieben werden, sind als eigene Standorte der Organisation zu betrachten. Diese Standorte sind in der Planung der Audits zu berücksichtigen.

2.4.3 Grundlegende Aufgaben des Auditteams

Die Aufgaben des Auditteams im Rahmen der Durchführung eines Audits umfassen zumindest das Folgende:

- a) Struktur, grundsätzliche Regelungen, Prozesse, Verfahren, Aufzeichnungen und zugehörige Dokumente der Organisation bezüglich der zutreffenden Bezugsdokumente zu prüfen und zu verifizieren;
- b) festzustellen, dass diese alle relevanten Anforderungen bezüglich des beabsichtigten Geltungsbereichs der Zertifizierung erfüllen;
- c) festzustellen, dass die Prozesse und Verfahren wirksam eingeführt, umgesetzt und aufrechterhalten werden, um Grundlage für das Vertrauen in das Compliance-Managementsystem des Kunden zu schaffen;
- d) dem Kunden in Bezug auf seine eigenen Maßnahmen etwaige Widersprüche zwischen seiner Politik, seinen Zielen und Vorgaben aufzuzeigen.

2.4.4 Zu auditierende Funktionen

Folgende Organisationseinheiten und Funktionen sind –sofern zutreffend– im Rahmen von Audits zumindest zu berücksichtigen und einzubinden:

A Funktionen, die im Rahmen der Etablierung und/oder Aufrechterhaltung des MS Verantwortung tragen bzw. diesbezüglich relevant sind:

- Oberste Organe, z.B. Geschäftsleitung und Aufsichtsorgane
- Compliance Funktionen, regionale oder divisionale Compliance-Beauftragte
- Personalverantwortliche einschließlich Ausbildungsverantwortliche
- Interne Revision, Verantwortliche für interne Kontrollsysteme

B Alle Funktionen der Organisation die -gemäß dem Scope des MS- einem relevanten Compliance-Risiko ausgesetzt sind, wie z.B.:

- Leiter und Mitarbeiter von Vertrieb, Einkauf, Produktion, Vertreter bei Behördenverfahren etc.
- alle im Rahmen des Audits Stufe 1 identifizierten Funktionen bzw. Personengruppen

Grundsätzlich gilt, dass sowohl Führungskräfte als auch betroffene Mitarbeiter in das Audit einzubeziehen sind.

2.4.5 Unterlagenprüfung

Folgende Unterlagen, Dokumente und Aufzeichnungen sind im Rahmen des Audits der Stufe 2 zumindest vom Auditteam zu prüfen und zu verifizieren:

- Management-Handbuch und Handlungsanweisungen, Prozessbeschreibungen im Zusammenhang mit Compliance
- Leitbild, Code of Conduct
- schriftliche Dokumentation der Durchführung einer Risikobewertung und deren Ergebnisse

- Schulungsunterlagen
- Protokolle der Organisationsleitung bzw. des Aufsichtsorgans der Organisation, in welchen Compliance behandelt wird
- Berichte, welche Compliance zum Gegenstand haben, z.B. des Compliance Officers an die Organisationsleitung
- Compliance-Kommunikation an die Organisationsmitglieder
- Überprüfungsberichte, z.B. Auditreports
- Berichte über allfällige Compliance-Verstöße und Darstellung der daraus erfolgten Maßnahmen (sofern zutreffend).

2.4.6 Kommunikation während des Audits

Im Verlauf des Audits wird das Auditteam in regelmäßigen zeitlichen Abständen den Fortschritt des Audits bewerten und Informationen austauschen. Der Auditteamleiter wird bei Bedarf die Aufgaben unter den Mitgliedern des Auditteams neu zu ordnen und den Kunden in regelmäßigen zeitlichen Abständen über den Fortschritt des Audits und alle Bedenken unterrichten.

Falls die verfügbaren Auditnachweise anzeigen, dass die Auditziele nicht erreicht werden können oder ein unmittelbares und erhebliches Risiko bestehen kann, wird der Auditteamleiter dem Kunden und, falls möglich, der Zertifizierungsstelle darüber Bericht erstatten, um die entsprechenden Maßnahmen zu ermitteln. Zu diesen Maßnahmen können die erneute Bestätigung oder die Veränderung des Auditplans, Änderungen an den Auditzielen oder am Auditumfang oder auch der Abbruch des Audits gehören. Der Auditteamleiter wird der Zertifizierungsstelle über die Ergebnisse der ergriffenen Maßnahmen Bericht erstatten.

Der Auditteamleiter wird gemeinsam mit dem Kunden jeglichen Änderungsbedarf am Auditumfang, der sich im Verlauf der Audittätigkeiten vor Ort herausstellt, überprüfen und der Zertifizierungsstelle darüber Bericht erstatten.

2.4.7 Auditschlussfolgerungen

Sollten im Rahmen eines Audits Nichtkonformitäten festgestellt werden, werden vom Auditteam entsprechende Auflagen zur Beseitigung der Abweichungen erteilt. Nichtkonformitäten werden wie folgt klassifiziert:

Untergeordnete Nichtkonformität: Nichtkonformität, die die Fähigkeit des Managementsystems, die beabsichtigten Ergebnisse zu erreichen, nicht beeinträchtigt.

Wesentliche Nichtkonformität: Nichtkonformität, die die Fähigkeit des Managementsystems, die beabsichtigten Ergebnisse zu erreichen, beeinträchtigt.

Anmerkung: In folgenden Fällen könnten Nichtkonformitäten als wesentlich eingestuft werden:

- wenn erhebliche Zweifel daran besteht, dass eine wirksame Prozesslenkung besteht oder dass Compliance Maßnahmen nicht umgesetzt werden;
- mehrere untergeordnete Nichtkonformitäten, die sich auf dieselbe Anforderung oder dasselbe Problem beziehen, könnten einen systembezogenen Fehler darstellen und somit eine wesentliche Nichtkonformität ergeben.

2.4.8 Korrekturmaßnahmen

Für alle untergeordneten Nichtkonformitäten muss die Organisation

1. eine Ursachenanalyse durchführen sowie
2. einen Plan zur Implementierung von Korrekturmaßnahmen erstellen.

Die effektive Implementierung der Korrekturmaßnahmen zu untergeordneten Nichtkonformitäten wird im Rahmen des nachfolgenden regulären Überwachungs- oder Rezertifizierungsaudit verifiziert.

Für alle wesentlichen Nichtkonformitäten muss die Organisation

1. eine Ursachenanalyse durchführen sowie
2. entsprechende Korrekturmaßnahmen implementieren.

Die effektive Implementierung der Korrekturmaßnahmen zu wesentlichen Nichtkonformitäten wird entweder

- durch eine Überprüfung von der Organisation bereitgestellter Unterlagen und Dokumentation oder
- im Rahmen eines teilweisen oder vollständigen Nachaudits verifiziert.

Sollte es nicht möglich sein, die Implementierung von Korrekturmaßnahmen zu einer oder mehrerer wesentlicher Nichtkonformitäten innerhalb von 6 Monaten nach dem letzten Tag des Audits Stufe 2 zu verifizieren, muss in jedem Fall ein erneutes Audit der Stufe 2 durchgeführt werden.

2.4.9 Empfehlungen zur Wirksamkeit des Managementsystems

Über die Feststellung der Konformität hinaus können die Auditoren auch Empfehlungen in Bezug auf die Wirksamkeit und Verbesserungsmöglichkeiten in Bezug auf das Managementsystem abgeben. Diese werden im Auditbericht dokumentiert, haben aber keinen Einfluss auf die Ausstellung des Zertifikates gemäß Abschnitt 2.6.

2.4.10 Abschlussbesprechung

Am Ende des Audits wird eine Abschlussbesprechung gemeinsam mit dem zuständigen Management des Kunden und gegebenenfalls mit den Personen, die die Verantwortung für die zu auditierenden Funktionen oder Prozesse tragen, durchgeführt werden. Die Anwesenheit bei dieser Abschlussbesprechung wird aufgezeichnet.

Der Zweck der Abschlussbesprechung besteht darin, die aus dem Audit gezogenen Schlussfolgerungen einschließlich der Empfehlung hinsichtlich der Zertifizierung vorzustellen. Alle Nichtkonformitäten werden vom Auditteam erläutert sodass sie verstanden werden. Weiters wird folgendes erläutert bzw. vereinbart:

- weitere Vorgehensweise der Zertifizierungsstelle inkl. 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;
- 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 dokumentiert und an die Zertifizierungsstelle weitergeleitet.

2.5 Auditbericht zur Erstzertifizierung

Das Auditteam analysiert und bewertet alle während der Audits der Stufe 1 und der Stufe 2 erfassten Informationen und Auditnachweise, trifft Auditfeststellungen und Auditschlussfolgerungen.

Die Informationen, die das Auditteam der Zertifizierungsstelle für die Zertifizierungsentscheidung bereitstellt, müssen mindestens enthalten:

- a. die Auditberichte einschließlich Aufstellung der untergeordneten und wesentlichen Nichtkonformitäten und, wo zutreffend, zu Korrekturen und Korrekturmaßnahmen, die von der Organisation ergriffen wurden;
- b. Dokumentation der Empfehlungen;
- c. eine Empfehlung, ob die Zertifizierung gewährt werden soll oder nicht, sowie –wenn zutreffend- die Bedingungen hierfür.

2.6 Entscheidung über die Zertifizierung

2.6.1 Bewertungsprozess

Vor der Entscheidung über die Zertifizierung, wird durch die Zertifizierungsstelle eine Bewertung wie folgt durchgeführt:

- a) Prüfung der durch das Auditteam bereitgestellten Informationen im Hinblick auf die Zertifizierungsanforderungen und den Geltungsbereich;
- b) Bewertung, Verifizierung und Freigabe der Korrekturmaßnahmen für alle wesentlichen Nichtkonformitäten;
- c) Bewertung und Freigabe des Plans der Organisation in Bezug auf Korrekturmaßnahmen für alle untergeordneten Nichtkonformitäten.

2.6.2 Ausstellung des Zertifikates

Basierend auf den Ergebnissen der Bewertung gemäß Abschnitt 2.6.1 entscheidet die Zertifizierungsstelle über die Ausstellung des Zertifikates. Der Geltungsbereich eines Zertifikates wird durch die folgenden Angaben bestimmt:

- Identifikation der juristischen Person (einschließlich der Adresse), die Inhaber des Zertifikates ist,
- Geltungsbereich in Bezug auf die Organisation bzw. fallweise Untereinheiten der Organisation in Abhängigkeit von den Ergebnissen des/der Audits,
- Angabe der geographischen Orte der Organisationseinheit(en),
- Compliance-Risiken innerhalb des Geltungsbereiches.

Das Zertifikat hat eine Gültigkeit von 3 Jahren vorausgesetzt, dass die Bedingungen zur Aufrechterhaltung des Zertifikates gegeben sind.

2.7 Überwachungsaktivitäten

2.7.1 Überwachungsaudits

Zur Aufrechterhaltung des Zertifikates sind Überwachungsaudits und andere Überwachungsaktivitäten im Abstand von 1 Jahr durchzuführen.

Änderungen bzgl. der zertifizierten Organisation (Struktur, Rechtspersonen, Standorte u.dgl.) sind im Rahmen von Überwachungsaktivitäten zu berücksichtigen und sind entsprechend zu planen. In Abhängigkeit der Art und des Umfangs der Änderungen wird die Zertifizierungsstelle die erforderlichen Überwachungsmaßnahmen festlegen.

Überwachungsaudits sind Vor-Ort-Audits, stellen aber nicht notwendigerweise vollständige Systemaudits dar, sodass die Zertifizierungsstelle das Vertrauen aufrechterhalten kann, dass das zertifizierte Managementsystem zwischen den Re-Zertifizierungsaudits weiterhin die Anforderungen erfüllt.

Teile des Überwachungsaudits können mit elektronischen Mitteln erfolgen (Remote-Audits). Der Einsatz von Remote-Audits wird von der Zertifizierungsstelle im Rahmen der Festlegung des Auditprogrammes festgelegt. Der während eines solchen Remote-Audits erlangte Nachweis muss ausreichend sein, um den Auditor in die Lage zu versetzen, in Kenntnis der Sachlage eine begründete Entscheidung über die Konformität mit der jeweiligen Anforderung zu treffen.

Das Überwachungsauditprogramm muss mindestens umfassen:

- a. interne Audits und Managementbewertung;
- b. eine Bewertung der ergriffenen Maßnahmen zu Nichtkonformitäten, die im Rahmen des vorhergehenden Audits festgestellt wurden;
- c. Umgang mit Compliancevorfällen und/oder diesbezüglichen Hinweisen
- d. Wirksamkeit des Managementsystems im Hinblick auf das Erreichen der Ziele der zertifizierten Organisation;
- e. Fortschritt bei geplanten Tätigkeiten, die auf eine ständige Verbesserung zielen;
- f. Bewertung von Änderungen und
- g. Nutzung von Zeichen und/oder andere Verweise auf die Zertifizierung.

Über die Durchführung des Überwachungsaudits wird vom Leitenden Auditor ein Bericht erstellt.

2.7.2 Bewertung durch die Zertifizierungsstelle

Dieser Bericht bildet die Basis für die Entscheidung der Zertifizierungsstelle, das Zertifikat aufrechtzuerhalten. In Abhängigkeit der Ergebnisse der Überwachung kann der Geltungsbereich eines Zertifikates erweitert oder eingeschränkt werden.

2.8 Rezertifizierung

2.8.1 Rezertifizierungsprozess

Zur Verlängerung des Zertifikates werden die folgenden Aktivitäten durchzuführen:

1. Prüfung der Überwachungsberichte des vorangegangenen Zertifizierungszyklus und einer Bewertung der Leistung des Managementsystems,
2. die Durchführung eines Rezertifizierungsaudits gemäß 2.8.2.

Für den Fall signifikanter Änderungen der Organisation, des Managementsystems oder des Umfeldes der Organisation, kann die Zertifizierungsstelle auch die Durchführung eines weiteren Audits der Stufe 1 gemäß 2.3.1 anordnen.

2.8.2 Rezertifizierungsaudit

Das Rezertifizierungsaudit muss ein Vor-Ort-Audit beinhalten, welches Folgendes behandelt:

- a. die Wirksamkeit des Managementsystems in seiner Gesamtheit angesichts interner oder externer Änderungen und seine fortgesetzte Bedeutung und Anwendbarkeit im Geltungsbereich der Zertifizierung;
- b. die dargelegte Verpflichtung zur Aufrechterhaltung der Wirksamkeit und Verbesserung des Managementsystems, um die gesamte Leistungsfähigkeit zu steigern;
- c. ob das Betreiben des zertifizierten Managementsystems zum Erreichen von Politik und Zielstellungen der Organisation beiträgt.

Für jede festgestellte wesentliche Nichtkonformität, wird die Zertifizierungsstelle Fristen für umzusetzende Korrekturen und Korrekturmaßnahmen noch vor Ablauf der Zertifizierung festlegen. Solche Korrekturmaßnahmen müssen noch vor dem Ablauf des Zertifikates von der Organisation implementiert und von der Zertifizierungsstelle verifiziert werden.

2.8.3 Auditbericht zum Rezertifizierungsaudit

Die Zertifizierungsstelle trifft die Entscheidungen über die Erneuerung der Zertifizierung auf der Grundlage der Ergebnisse des Rezertifizierungsaudits sowie der Ergebnisse aus der Bewertung des Systems über den Zeitraum der Zertifizierung.

2.8.4 Zertifikatsausstellung

In Abhängigkeit der Ergebnisse der Rezertifizierung kann der Geltungsbereich eines Zertifikates erweitert oder eingeschränkt werden.

Wenn alle Rezertifizierungsaktivitäten vor Ablauf der bestehenden Zertifizierung erfolgreich abgeschlossen werden, dann kann das Ablaufdatum der neuen Zertifizierung auf dem Ablaufdatum der bestehenden Zertifizierung beruhen. Das Ausgabedatum des neuen Zertifikats entspricht dem Tag der Rezertifizierungsentscheidung.

Für den Fall, dass vor Ablauf des Zertifizierungsdatums das Rezertifizierungsaudit nicht abgeschlossen wurde oder es nicht möglich ist, die Umsetzung von Korrekturmaßnahmen für eine wesentliche Nichtkonformität zu verifizieren, dann wird keine Empfehlung für die Rezertifizierung ausgesprochen und die Gültigkeit der Zertifizierung nicht verlängert.

Unter der Voraussetzung, dass die ausstehenden Rezertifizierungstätigkeiten abgeschlossen worden sind, kann innerhalb von 6 Monaten nach Ablauf der Zertifizierung, das Zertifikat wieder ausgestellt werden; andernfalls ist mindestens ein Audit der Stufe 2 (gemäß 2.3.2) durchzuführen. Das Gültigkeitsdatum des Zertifikats muss dem Tag der Rezertifizierungsentscheidung oder einem späteren entsprechen und das Ablaufdatum muss auf dem vorangegangenen Zertifizierungszyklus basieren.

2.9 Außerordentliche Audits

Auf Basis der Ergebnisse eines Erst- oder Rezertifizierungsaudits, eines Überwachungsaudits und/oder auf Basis einer sonstigen Information der Zertifizierungsstelle, kann es erforderlich sein, kurzfristig, anlassbezogen ein Audit zur Überprüfung der Normkonformität des Managementsystems durchzuführen.

Solche außerordentlichen Audits sind unter den folgenden Voraussetzungen durchzuführen.

- es gibt eine Vereinbarung mit dem Kunden;
- der Geltungsbereich und Zweck des Audits ist klar definiert und dem Kunden kommuniziert;
- das Auditteam ist bestimmt und dem Kunden kommuniziert.

Darüber hinaus gelten für die Durchführung dieser Audits und die Festlegung von Ergebnissen analog die Bestimmungen gemäß 2.4, sofern anwendbar.

2.10 Änderungen der Zertifizierungsgrundlagen

Änderungen in den der Zertifizierung zu Grunde liegenden normativen Dokumenten werden von der Zertifizierungsstelle den Zertifikatsinhabern umgehend mitgeteilt.

Dem Zertifikatsinhaber wird bei veränderten Anforderungen an das MS eine Frist von 12 Monaten zur Anpassung an die geänderten Anforderungen eingeräumt. Der Nachweis der Erfüllung der Anforderungen ist im Rahmen eines Überwachungsaudits, zu erbringen. Nach Erbringung des Nachweises wird das Zertifikat mit einer neuen Referenz auf die geänderten normativen Dokumente bzw. dieses Zertifizierungsschema ausgestellt.

2.11 Änderungen im Geltungsbereich von Zertifikaten

Sollte der Zertifikatsinhaber die Erweiterung des Geltungsbereichs in Bezug auf weitere Organisationseinheiten bzw. Compliance relevante Risiken wünschen, muss er dies bei der Zertifizierungsstelle schriftlich beantragen. Die Zertifizierungsstelle wird nach Prüfung der Sachlage die für die Erweiterung des Geltungsbereiches des Zertifikates erforderlichen Prüfungen von Unterlagen und/oder Audits festlegen.

Sollte der Zertifikatsinhaber die Einschränkung des Geltungsbereichs in Bezug auf die zertifizierten Organisationseinheiten bzw. Compliance relevante Risiken wünschen, muss er dies der Zertifizierungsstelle schriftlich mitteilen. Die Zertifizierungsstelle reduziert den Anwendungsbereich des Zertifikates entsprechend. Ab diesem Zeitpunkt darf die Organisation keinerlei Aussagen in Bezug auf die Zertifizierung Ihres MS diesbezüglich mehr tätigen. Die Verifizierung der diesbezüglichen Verpflichtungen des Zertifikatsinhabers findet in jedem Fall im Rahmen der folgenden Überwachungsaudits statt.

Änderungen der Zertifikate in Bezug auf formale Angaben des Zertifikatsinhabers (wie z.B. Änderungen im Firmennamen oder der Adresse) sind der Zertifizierungsstelle schriftlich mitzuteilen. Die Zertifizierungsstelle stellt ohne fachliche Prüfung ein geändertes Zertifikat aus.

Jegliche Änderungen in der juristischen Person des Zertifikatsinhabers, bedingen einen neuen Antrag auf Zertifizierung und die Durchführung eines neuen Zertifizierungsverfahrens.

2.12 Zurückziehung von Zertifikaten

Es gelten die Allgemeinen Geschäftsbedingungen der Zertifizierungsstelle in der jeweils gültigen Fassung.

2.13 Vorgehensweise bei der Übernahme von Zertifikaten

Im Fall eines Wechsels eines Kunden von einer anderen Zertifizierungsstelle zu AS+C ist grundsätzlich im Sinne einer Erstzertifizierung gemäß Abschnitt 2.3 vorzugehen.

AS+C prüft -sofern durch den Kunden bereitgestellt- Auditberichte vorangegangener Audits. Auf Basis des Ergebnisses der Prüfung dieser Auditberichte kann AS+C gegebenenfalls entscheiden, auf die Durchführung eines Audits der Stufe 1 (gemäß Abschnitt 2.3.1) zu verzichten.

Für den Fall, dass ein Kunde sein MS bereits bei einer anderen Zertifizierungsstelle zertifiziert hatte und anlässlich einer Rezertifizierung zu AS+C wechselt, kann AS+C entscheiden im Sinne einer Rezertifizierung vorzugehen, sofern AS+C ausreichend Informationen über das MS des Kunden vorliegen.

Anhang A Übergangsbestimmungen

A.0 Allgemeines

Dieser Anhang legt die Vorgehensweisen für den Übergang bestehender Zertifikate von Compliance-Managementsystemen gemäß ISO 19600:2014-12 auf den Internationalen Standard ISO 37301:2021-04 fest.

A.1 Erstzertifizierungsverfahren

Ab dem 2021-04-15 werden Erstzertifizierungsverfahren ausschließlich gemäß der ISO 37301:2021-04 durchgeführt. Erstzertifizierungsverfahren eines Compliance-Managementsystems gemäß ISO 19600:2014-12 werden ab diesem Zeitpunkt nicht mehr durchgeführt.

A.2 Zertifikate gemäß ISO 19600

A.2.1 Bestehende Zertifikate gemäß ISO 19600:2014-12 bleiben für eine maximale Dauer von 24 Monaten ab 2021-04-15 gültig sofern die Bedingungen zur Aufrechterhaltung der Zertifikate gemäß Abschnitt 2.7 dieses Zertifizierungsschemas gegeben sind.

A.2.2 Für den Umstieg von einem aufrechten Zertifikat gemäß ISO 19600:2014-12 auf ein Zertifikat gemäß ISO 37301:2021-04 ist die Durchführung eines Audits Stufe 1 gemäß Abschnitt 2.3.1 nicht erforderlich.

A.2.3 Die Zertifizierungsstelle führt beim nächstmöglichen Überwachungsaudit das Audit auf Basis der ISO 37301:2021-04 durch, um die Anforderungen der ISO 37301:2021-04 zu prüfen.

A.2.4 Für den Fall, dass das Überwachungsaudit keine Nichtkonformitäten ergibt, wird das Zertifikat für das Compliance-Managementsystem gemäß ISO 19600:2014-12 auf Basis der ISO 37301:2021-04 neu ausgestellt. Die Parameter des Zertifikates wie die Fälligkeiten der Überwachungsaudits sowie das Ablaufdatum werden durch die Neuausstellung nicht verändert.

A.2.5 Für den Fall, dass das Überwachungsaudit Nichtkonformitäten gemäß 2.4.7 ergibt, ist gemäß Abschnitt 2.4.8 vorzugehen. Ein Zertifikat nach ISO 37301:2021-04 wird erst nach erfolgreichem Audit und vollständigem Nachweis aller Korrekturmaßnahmen ausgestellt. Bis zum Umstieg kann das bestehende Zertifikat aufrechterhalten werden, sofern in Bezug auf die Kriterien gemäß ISO 19600:2014-12 keine wesentlichen Nichtkonformitäten festgestellt wurden.

A.2.6 Rezertifizierungsverfahren werden in jedem Fall auf Basis der ISO 37301:2021-04 gemäß Abschnitt 2.8 durchgeführt. Sollte zwischen dem Ablauf eines Zertifikates gemäß ISO 19600:2014-12 und dem Beginn des Rezertifizierungsverfahrens gemäß ISO 37301:2021-04 ein Zeitraum von mehr als 6 Monaten liegen, ist, abweichend von den Festlegungen des Abschnittes A.2.2, die Durchführung eines Audits der Stufe 1 gemäß Abschnitt 2.3.1 erforderlich.