Dokumentation

Infoblatt Auditierung und Zertifizierung

Autor PwC Certification Services GmbH
Version 3.1
Status Freigegeben

ÖFFENTLICH

Inhaltsverzeichnis

Dokumentenhistorie

Version	Datum	Änderung	Autor
0.1	6. Februar 2012	Dokument neu erstellt	Prof. Dr. Rainer Rumpel
0.2	6. Februar 2012	Dokument ergänzt	Prof. Dr. Rainer Rumpel
0.3	7. Februar 2012	Dokument überarbeitet	Prof. Dr. Rainer Rumpel
1.0	7. Februar 2012	Freigabe	Prof. Dr. Vladimir
1.1	24. September 2014	Anpassung ISO 27001:2013	Dr. Werner Otto
1.2	01. Oktober 2014	Erweiterung auf ISO 20000-1	Dr. Werner Otto
1.3	06. Oktober 2014	Freigabe	Knut Haufe
1.4	10. November 2016	Aktualisierung	Knut Haufe
2.0	7. Januar 2017	Qualitätssicherung und Freigabe	Vladimir Stantchev
3.0	22. Mai 2017	Umfirmierung	Stefanie Dzimkowski
(3.0)	05. Mai 2018	Umfirmierung	Dominik Hansen
3.1	31. Mai 2018	Qualitätssicherung und Freigabe	Vladimir Stantchev

1 Einleitung

1.1 Zielsetzung und Anwendung

Das vorliegende Prüfschema für Audits nach den Normen ISO/IEC 27001, ISO 20000-1 in ihrer jeweils aktuellen Fassung (im Folgenden auch „ISO-Normen“ genannt) beschreibt die Voraussetzungen und Vorgehensweise, welche für die Erlangung eines Zertifikats erfüllt beziehungsweise eingehalten werden müssen. Das Schema deckt wesentliche Anforderungen für Zertifizierungsstellen gemäß der Norm ISO/IEC 17021 ab und ist in Übereinstimmung mit dieser Norm. Auch die Norm ISO/IEC 19011 wurde berücksichtigt, da sie in weiten Teilen nicht nur auf Qualitätsmanagementsysteme und Umweltmanagementsysteme, sondern auf Managementsysteme aller Art anwendbar ist.

1.2 Adressat

Der Adressat des Prüfschemas sind Kunden mit dem Ziel ihr Managementsystem der ISO-Normen zertifizieren zu lassen. Interessenten soll die Vorgehensweise des Auditprozesses sowie Details zur Zertifizierungstätigkeit erläutert werden.

1.3 Begrifflichkeiten

Die in diesem Dokument verwendeten Begrifflichkeiten, die im Kontext dieses Prüfungsschemas eine besondere Bedeutung haben, sind im Folgenden näher erläutert.

Geltungsbereich der Zertifizierung

Der Geltungsbereich bzw. Anwendungsbereich (im Folgenden auch „Scope“ genannt) definiert, für welchen Teil der zu zertifizierenden Organisation das Managementsystem Anwendung findet.

Zertifizierungsstelle

Eine Zertifizierungsstelle ist autorisiert, eine Organisation auf die Einhaltung von Normen zu prüfen, für die sie akkreditiert ist. Man spricht auch von Konformitätsbewertungsstelle. Sie kann im Namen der ISO Zertifikate ausfertigen. Die Zertifizierungsstelle ist hier die zuständige Stelle innerhalb der PwC Certification Services GmbH.

Zertifikat

Das Zertifikat ist das offizielle Dokument, das als Konformitätsnachweis für eine erfolgreiche Prüfung dient.

Audit

Systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Auditnachweisen und zu deren objektiver Auswertung, um zu ermitteln, inwieweit die Auditkriterien erfüllt sind.

Auditee

Eine Organisation, die den Antrag auf Konformitätsbewertung gestellt hat.

Auditnachweis

Aufzeichnungen, Tatsachenfeststellungen oder andere Informationen, die für die Auditkriterien relevant und verifizierbar sind. Stichprobenumfang sowie Auswahl von quantitativen und qualitativen Nachweisen obliegt dem Auditteamleiter.

Auditteam

Ein Auditteam besteht aus einem oder mehreren Auditoren, die ein Audit durchführen.

Auditor

Person mit der gegenüber der Zertifizierungsstelle nachgewiesenen Qualifikation, ein Audit durchzuführen.

Auditteamleiter

Der Auditteamleiter ist Auditor und fachlicher Leiter des Auditteams. Er ist für den Auditprozess weisungsbefugt gegenüber den sonstigen Auditoren im Auditteam.

Fachexperte

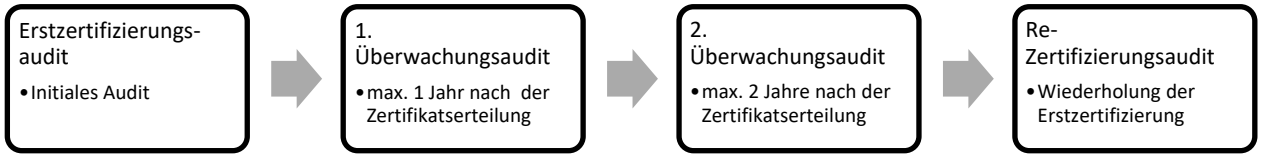
Zum Auditteam können auch Fachexperten gehören, die entweder spezielle Branchenkenntnisse oder sehr gute technische Fachkenntnisse besitzen.

2 Der Beginn der Zertifizierung

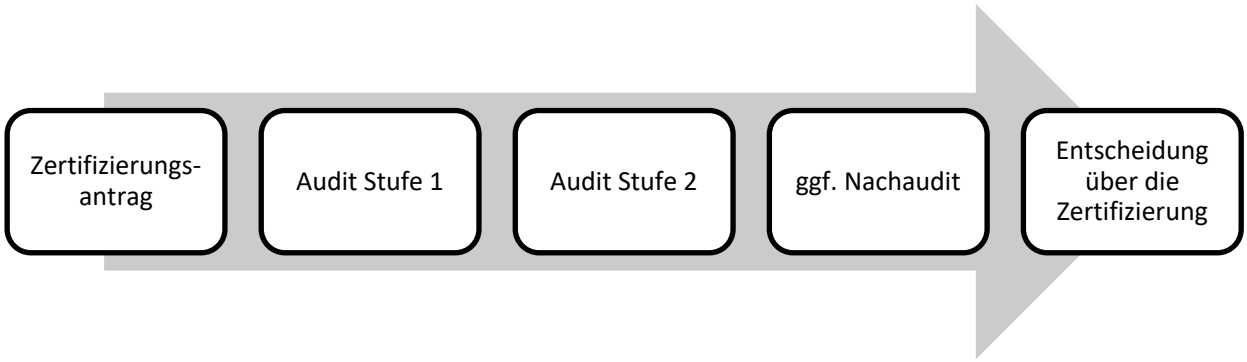
Dieses Kapitel bietet eine Einführung in den Zertifizierungsablauf und beschreibt die Anforderungen, die vor Aufnahme der Prüfungstätigkeiten erfüllt sein müssen.

2.1 Zertifizierungsprozess

Das vorliegende Prüfungsschema hat Lenkungsfunktion für den Zertifizierungsprozess. Erteilung, Erhaltung und Erneuerung des Zertifikats sind die unterschiedlichen Lebensphasen, die während des Zertifizierungsprozesses zur Anwendung kommen.



Die Erstzertifizierung beinhaltet fünf Schritte, die in ihrer Abfolge in der nachstehenden Grafik dargestellt sind. Die einzelnen Schritte sind im vorliegenden Prüfschema beschrieben.



Die Prüfungsschritte und -methoden in den Überwachungsaudits sowie im Re-Zertifizierungsaudit weichen nicht erheblich vom Erstzertifizierungsaudit ab.

2.2 Auditgrundsätze

Für Audits von Zertifizierungsstellen gelten die folgenden vertrauensbildenden Grundsätze:

- Unparteilichkeit: Die Zertifizierungsstelle stellt sicher, dass keine Interessenskonflikte zwischen der Zertifizierungsstelle, den Auditoren und dem Auditee bestehen. Alle relevanten Teilprozesse sind im Hinblick auf dieses Ziel überprüft.
- Kompetenz: Die Zertifizierungsstelle stellt durch einen geeigneten Auswahl- und Überwachungsprozess sicher, dass die für die Zertifizierung notwendigen Ressourcen über die notwendigen Kompetenzen und Fachkenntnisse verfügen.

- Verantwortung: Die Gesamtverantwortung für den Zertifizierungsprozess liegt bei der Leitung der Zertifizierungsstelle.
- Vertraulichkeit: Alle vom Auditee für die Zertifizierung zur Verfügung gestellten Informationen werden, soweit nicht explizit aufgeführt, vertraulich behandelt.
- Beschwerdemöglichkeit: Die Zertifizierungsstelle verfügt über ein Verfahren, mit dem Beschwerden bezüglich des Zertifizierungsprozesses aufgenommen und konstruktiv bearbeitet werden.

2.3 Zertifizierungsantrag

Die Zertifizierungsstelle stellt ein Antragsformular zur Verfügung, das vom Interessenten auszufüllen ist. Die Zertifizierungsstelle kann die Annahme eines Zertifizierungsantrags verweigern, sofern Anhaltspunkte für Interessenskonflikte bestehen. Alle Regelungen zur Vermeidung von Interessenskonflikten der PwC finden Anwendung. Ein angenommener Antrag ist Voraussetzung für die Einleitung der Auditaktivitäten.

2.4 Scope der Zertifizierung

Der Scope der Zertifizierung wird bei der Beantragung festgelegt. Bei der Fixierung des Scopes ist darauf zu achten, dass auf die Organisation mit ihren Geschäftsprozessen beziehungsweise Fachverfahren, ihren Standorten, ihren Werten (Assets) und ihren Technologien Bezug genommen wird. Durch die Zertifizierungsstelle wird geprüft, ob der zu prüfende Bereich sich ausreichend scharf von anderen Bereichen, wie zum Beispiel einzelnen Geschäftseinheiten, anderen Standorten und eingesetzten technischen Systemen des zu zertifizierenden Unternehmens abgrenzen lässt. Außerdem wird beurteilt, ob der Scope eine ausreichende Mindestgröße – auch im Verhältnis zur Organisation – hat. Er muss insbesondere substantiell zum Funktionieren der Organisation oder eines wesentlichen Teils davon beitragen.

Zusätzlich bildet der Scope die Grundlage für die Risikobeurteilung und Risikobehandlungsoptionen, welche an den Anforderungen des Scope ausgerichtet sein müssen. Die Zertifizierungsstelle hat das Recht, den Scope abzulehnen beziehungsweise Nachbesserung zu fordern.

2.5 Rechtliche Voraussetzungen

Der Vereinbarung zwischen Auditee und Zertifizierungsstelle muss ein schriftlicher Vertrag zugrunde liegen, der auf dem Zertifizierungsantrag basiert. Der Vertrag muss den gesamten Geltungsbereich des dem Zertifikat zugrundeliegenden Anwendungsbereichs umfassen.

2.6 Auswahl der Auditoren

Die Auswahl der Auditoren, die mit dem Zertifizierungsaudit beauftragt werden, obliegt der Zertifizierungsstelle. Eine Auswahl durch den Antragsteller ist ausgeschlossen. Die Qualifikation der Auditoren ist über entsprechende Fachkundenachweise sichergestellt. Die Prüfungsplanung erfolgt zwischen dem Auditteamleiter und dem Auditee.

2.7 Leistungsabgrenzung

Beratungsleistungen zur Informationssicherheit, insbesondere die Mitwirkung bei internen Audits des Auditees sowohl vor als auch während der Prüfung sind ausgeschlossen. Dieser Ausschluss beschränkt sich auf Beratungstätigkeiten, die innerhalb von zwei Jahren vor dem Zertifizierungsantrag oder einem Überwachungsaudit stattgefunden haben. Die Umsetzung der während der Prüfung als notwendig identifizierten Maßnahmen ist ebenfalls nicht Bestandteil der Leistung. Die Umsetzung wird auch außerhalb der Zertifizierungstätigkeit von der PwC Certification Services GmbH nicht als Leistung angeboten.

3 Der Zertifizierungsprozess

Für eine Auditierung nach den ISO-Normen existieren drei unterschiedlichen Audittypen:

- Erstzertifizierung: Das initiale Audit, das zur ersten Vergabe des Zertifikats führt. Das Zertifikat hat eine Gültigkeit von drei Jahren ab Ausstellungsdatum.
- Überwachungsaudit: Während der Gültigkeitsdauer des Zertifikats muss in jährlichen Abständen ein Überwachungsaudit stattfinden. Dies stellt sicher, dass die im Informationssicherheitsmanagementsystem definierten Prozesse effektiv und effizient umgesetzt sind.
- Re-Zertifizierungsaudit: Bis zum Ablauf der Zertifikatsgültigkeit muss eine Re-Zertifizierung erfolgen. Ansonsten ist der Zertifizierungszyklus unterbrochen.

Die drei Arten sind im Folgenden näher beschrieben.

3.1 Erstzertifizierungsaudit

Die vom Antragsteller vorgelegten Referenzdokumente werden gesichtet und anhand der folgenden Kriterien bewertet. Alle Bewertungen der Referenzdokumente werden in den Auditbericht übernommen. Die durchgeführten Prüfungen müssen angemessen und reproduzierbar sein. Die Prüfungsergebnisse und Bewertungen müssen im Auditbericht verständlich und nachvollziehbar dokumentiert werden.

Das Erstzertifizierungsaudit umfasst zwei Stufen, die zeitlich wie logisch aufeinander aufbauen.

3.1.1 Audit Stufe 1

Die Stufe 1 des Audits prüft die generelle Bereitschaft des Auditees, ob eine Auditierung der Stufe 2 überhaupt durchführbar ist. Hierzu wird in Stufe 1 beurteilt:

- ob die Dokumentation des Managementsystems des Auditees ausreichend ist,
- ob der Standort sowie die standortspezifischen Bedingungen des Kunden ausreichende Berücksichtigung finden,
- ob die Mitarbeiter des Kunden ausreichend auf die Stufe 2 vorbereitet sind,
- ob der Auditee die Anforderungen, die aus den ISO-Normen heraus an ihn gestellt werden, hinreichend verstanden hat. Dies gilt insbesondere für wesentliche Aspekte wie die Identifikation von Schlüsselleistungen, zentralen Prozessen und Zielen sowie den Betrieb des Managementsystems,
- ob alle notwendigen Informationen über den Geltungsbereich des Auditees vorliegen, insbesondere in rechtlicher Hinsicht sowie unter Compliance-Aspekten,
- ob der Auditee ausreichende Ressourcen für die Stufe 2 bereitstellt,
- welche Schwerpunkte für das Audit der Stufe 2 festgelegt werden und
- ob interne Audits sowie Managementbewertungen belegen, dass der Grad der Umsetzung des Managementsystems entsprechend ausreichend ist, um mit dem Audit der Stufe 2 zu beginnen.

Als Ergebnis der Stufe 1 erhält der Auditee eine Bewertung, welche Schwachstellen während der Stufe 2 als Nichtkonformität eingestuft werden könnten. Hier müssen auch Zeitaufwand und Umfang der Arbeiten für Stufe 1 enthalten sein.

Zwischen Stufe 1 und Stufe 2 muss ausreichend zeitlicher Abstand bestehen, damit dem Auditee die Möglichkeit gegeben wird, angemessene Lösungen für die identifizierten Schwachstellen zu finden. Hierbei darf es jedoch nicht dazu kommen, dass die Stufe 1 als Vorbereitung und Hilfestellung für die

Erlangung des Zertifikats in Stufe 2 genutzt wird. Prüfungsfeststellungen aus Stufe 1 müssen entsprechend im Zertifikatsbericht enthalten sein.

Die Leitung der Zertifizierungsstelle prüft den Bericht zur Stufe 1 und entscheidet auf Basis der Empfehlung des Auditteamleiters, ob mit Stufe 2 fortgefahren werden kann, oder ob das Audit abgebrochen wird.

3.1.2 Audit Stufe 2

Mit den dokumentierten Ergebnissen der Stufe 1 sowie der Entscheidung zur Weiterführung beginnt das Audit der Stufe 2. Die Voten werden im Auditbericht dokumentiert und an die Zertifizierungsstelle kommuniziert.

Die Stufe 2 beinhaltet immer ein Audit vor Ort und umfasst alle relevanten Standorte der zu zertifizierenden Organisation. Vor Beginn dieses Audits wird dem Auditee ein Auditplan zur Verfügung gestellt. Dieser Schritt umfasst immer auch eine Eröffnungs- und eine Abschlussbesprechung.

Stufe 2 soll sicherstellen, dass:

- die zu zertifizierende Organisation ihren eigenen Richtlinien, Maßgaben und Prozessen in der täglichen Umsetzung folgt sowie
- die Konformität zwischen den Anforderungen der ISO-Normen und dem implementierten Managementsystem in Anlehnung an die Organisationsziele gegeben ist,

und umfasst mindestens die folgenden Prüfungshandlungen:

- Beurteilung der Risikoanalyse hinsichtlich Vergleichbarkeit, Nachvollziehbarkeit sowie Reproduzierbarkeit der Ergebnisse,
- Auswahl der Prüfungsfragen und Kontrollen anhand der Risikoanalyse und dem daraus resultierenden Risikobehandlungsplan,
- Sichtung der Nachweise zur Konformität des Managementsystems mit den Anforderungen der ISO-Normen,
- Messung und Überprüfung der Leistungserbringung in Bezug auf die definierten Schlüsselziele,
- Messung der Leistungsfähigkeit des ISMS in Bezug auf relevante gesetzliche und regulatorische Anforderungen,
- Prüfung der Ablauforganisation beim Auditee,
- Nachweise über interne Audits und darauf aufbauende Managementbewertungen des Managementsystems
- Nachweis über die explizite Verantwortlichkeit der Leitungsebene für die Aufbau- und Ablauforganisation des Auditees sowie
- Prüfung der im Kontext des Managementsystems sonstigen relevanten normativen, gesetzlichen und regulatorischen Anforderungen. Hierbei muss insbesondere überprüft werden, ob alle relevanten gesetzlichen und regulatorischen Anforderungen bei der Risikobeurteilung und der Auswahl der Maßnahmen berücksichtigt wurden.

3.1.3 Nachbesserungen und Nachforderungen

Nachbesserungen

Sowohl in Stufe 1 wie in Stufe 2 können sich Abweichungen ergeben. Diese müssen sachgerecht behoben werden. Dabei gibt es verschiedene Stufen der Behandlung von Abweichungen, je nach Schwere:

- Schwerwiegende Abweichungen sind Mängel, ohne deren Behebung nicht sichergestellt werden kann, dass das Managementsystems effektiv und effizient funktioniert. Daher müssen diese Abweichungen vor Ausstellung des Zertifikats behoben werden.
- Geringfügige Abweichungen sind zu kennzeichnen und mit einer Frist zur Behebung – üblicherweise bis zum nächsten Überwachungsaudit - zu versehen. Eine Ausstellung des Zertifikates kann unter Umständen trotzdem erfolgen. Mehrere geringfügige Abweichungen können allerdings in der Summe eine schwerwiegende Abweichung darstellen.

Nachforderungen

Im Einzelfall kann es zutreffen, dass die Zertifizierungsstelle Dokumente und Nachweise anfordert, deren Einsicht zur abschließenden Beurteilung über eine Zertifikatsvergabe notwendig ist und bislang der Zertifizierungsstelle nicht vorliegen. Die Nachforderungen und deren Erfüllung sind im Auditbericht festzuhalten.

Die Nachforderungen sind in Art und Umfang nicht begrenzt.

3.1.4 Kriterien für die Zertifikatsvergabe

Nach Abschluss der Audittätigkeiten werden vom Auditteamleiter alle relevanten Informationen zur Prüfung bei der Zertifizierungsstelle eingereicht. Dies umfasst im Wesentlichen:

- den Auditbericht,
- die wesentlichen Feststellungen zur Effektivität des Managementsystems,
- Feststellungen zur Nichtkonformität,
- durch den Kunden geplante oder eingeleitete oder abgeschlossene Korrekturmaßnahmen,
- die Bestätigung, dass die in Stufe 1 geforderten Informationen vorliegen,
- eine Empfehlung, ob das Zertifikat gewährt werden soll sowie eventuell damit verbundene Bedingungen und Auflagen.

Bei Abweichungen verbunden mit einer positiven Empfehlung ist für jeden Einzelfall zu begründen, warum das Zertifikat trotz der festgestellten Mängel erteilt werden sollte.

3.2 Überwachungstätigkeiten

Nach Erteilung des Zertifikats, das eine Gültigkeit von drei Jahren besitzt, müssen geeignete Maßnahmen seitens der Zertifizierungsstelle geplant werden, um die kontinuierliche Konformität des Auditees für alle für den maßgeblichen Bereich relevanten Tätigkeiten hinreichend sicherstellen zu können.

Neben jährlichen Überwachungsaudits werden die folgenden Tätigkeiten durchgeführt:
- Befragung des Auditees bezüglich wesentlicher Aspekte der Zertifizierung,
- Bewertung der erhaltenen Informationen,
- Bewertung des Umgangs mit zertifizierungsbezogenen Werbemaßnahmen sowie
- Sichtung von unterjährig vom Auditee bereitgestellten Dokumenten und Aufzeichnungen.

Zusätzliche Tätigkeiten werden nach den jeweiligen Erfordernissen gestaltet.

3.2.1 Überwachungsaudit

Um hinreichende sicherzustellen, dass die Effizienz und Effektivität des Managementsystems während der gesamten Gültigkeitsdauer des Zertifikats aufrechterhalten werden, werden jährliche Überwachungsaudits vor Ort beim Auditee durchgeführt. Hierbei wird nicht notwendigerweise ein komplettes Systemaudit durchgeführt. Es werden jedoch mindestens die folgenden Aspekte beurteilt:

- geplante und durchgeführte Maßnahmen bei festgestellter Nichtkonformität in Teilbereichen,
- Wirksamkeit des Managementsystems,
- Änderungen des Managementsystems, speziell des Scopes,
- vom Kunden durchgeführte interne Audits,
- Maßnahmen im Rahmen eines kontinuierlichen Verbesserungsprozesses,
- Verfahren, die auf Compliance mit Regelungen zum Managementsystem hinzielen,
- Änderungsmanagement sowie
- Verwendung der Zertifizierungsnachweise durch den Auditee.

Planung und Durchführung der Überwachungsaudits erfolgen analog der Vorgehensweise zur Erstzertifizierung in zwei Phasen. Änderungsvorschläge bezüglich der Planung der Überwachungsaudits sind der Zertifizierungsstelle rechtzeitig anzuzeigen. Insbesondere betrifft dies Verschiebungen von Fertigstellungs- und Lieferterminen von Auditdokumenten.

Die Referenzdokumente werden vom Auditor unter anderem daraufhin geprüft, ob aus dem vorhergehenden Audit resultierende offene Punkte bzgl. der Dokumentation bei der Aktualisierung der Referenzdokumente eingearbeitet worden sind. Dies betrifft beispielsweise geringfügige Abweichungen, deren Frist zur Behebung seit dem letzten Audit abgelaufen ist. Der Auditbericht zum ersten Überwachungsaudit muss der Zertifizierungsstelle mehr als zwei Jahre vor Ablauf des Zertifikats vorliegen, der Bericht zum zweiten Überwachungsaudit mehr als ein Jahr vor Ablauf des Zertifikats.

3.3 Re-Zertifizierungsaudit

Mit Ablauf des dritten Jahres nach Erteilung des Zertifikats verliert dieses seine Gültigkeit. Eine Verlängerung im Sinne von zusätzlichen Überwachungsaudits ist nicht möglich. Stattdessen existiert die Möglichkeit, ein Re-Zertifizierungsaudit durchzuführen. Ein Re-Zertifizierungsaudit muss geplant und durchgeführt werden, um die anhaltende Erfüllung aller Anforderungen der ISO-Normen 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.

Um einen nahtlosen Übergang zwischen den beiden Zertifikaten zu erreichen, muss eine Beantragung zur Re-Zertifizierung rechtzeitig erfolgen.

Das Re-Zertifizierungsaudit muss neben der Neuzertifizierung die Leistungsfähigkeit des Managementsystems während des Zeitraums der zurückliegenden Zertifizierung berücksichtigen und eine Überprüfung früherer Auditberichte zu Überwachungsaudits beinhalten. Daneben wird im Wesentlichen die Stufe 2 der Erstzertifizierung wiederholt.

Tätigkeiten zu Re-Zertifizierungsaudits können zudem ein Audit der Stufe 1 erfordern, wenn es signifikante Änderungen im Managementsystem, im geschäftlichen Umfeld des Auditees oder im Zusammenhang mit der Arbeitsweise des Managementsystems, zum Beispiel durch Veränderungen in der Gesetzgebung, gibt. Bei Änderungen an dem für ein Zertifikat relevanten Scopes des Managementsystems entscheidet die Zertifizierungsstellet über eine Re-Zertifizierung auch vor Ablauf der Gültigkeit des Zertifikats.

Das Re-Zertifizierungsaudit muss einen Prüfungsteil vor Ort beinhalten, welcher Folgendes behandelt:

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

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

Die Entscheidung über die Erneuerung des Zertifikats liegt bei der Zertifizierungsstelle. Hierzu werden neben den Ergebnissen des Re-Zertifizierungsaudits auch die Ergebnisse aus der Bewertung des Managementsystems über den Zeitraum der Zertifizierung und der von den Nutzern der Zertifizierung erhaltenen Beschwerden treffen. Im Sinne des kontinuierlichen Verbesserungsprozesses muss eine Verbesserung des Managementsystems erkennbar sein.

Eine Re-Zertifizierung muss beantragt werden.

3.4 Bereitschaftsaudit

Die Zertifizierungsstelle ist berechtigt, vor dem Beginn eines Zertifizierungsaudits ein Bereitschaftsaudit durchzuführen. Dieses Audit hat ausschließlich den Zweck festzustellen, ob der Auditte für ein Zertifizierungsaudit hinreichend vorbereitet ist. Eine begleitende Beratungsaktivität ist ausgeschlossen. Das Audit enthält keine Elemente, die das Zertifizierungsaudit verkürzen.

3.5 Verbundzertifizierung

Die Verbundzertifizierung beschreibt die Prüfung mehrerer Managementsysteme in einem einzelnen Audit. Diese Art der Prüfung wird von der PwC Certification Services GmbH i.d.R. als Verbund aus ISO/IEC 27001- und ISO/IEC 20000-1-Zertifizierung angeboten. Der Aufwand kann hier gegenüber der Summe aus den Einzelzertifizierungen geringer ausfallen. Der Aufwand wird im Rahmen der Angebotserstellung ermittelt.

3.6 Aussetzung, Zurückziehung und Einschränkung von Zertifizierungen

Abweichungen, die nach Prüfung des Einzelfalls zur Zurückziehung oder zur Annullierung der Zertifizierung führen können, liegen zum Beispiel vor, wenn:

- gesetzliche oder behördliche Vorgaben nicht eingehalten werden, ohne dass die zuständigen Behörden darüber informiert wurden und geeignete Korrekturmaßnahmen mit höchster Priorität eingeleitet sind,
- die Nichteinhaltung von Vorgaben durch das interne Auditsystem nicht erkannt wurde,
- die Nichteinhaltung von Vorgaben den Auditoren verschwiegen wurde,
- das interne Auditsystem generell nicht wirksam ist,
- die IT-Sicherheitsziele und -programme nicht umgesetzt werden, ohne dass es dazu triftige Gründe gibt,
- der benannte Vertreter und die übrigen Verantwortlichen für das Managementsystem ihre Aufgaben nicht erfüllen oder
- Schlussfolgerungen aus Abweichungen an einem Standort an anderen Standorten des Auditees nicht angemessen berücksichtigt werden.

Eine Aussetzung der Zertifizierung kann erfolgen, wenn

- ☐ bei einem Überwachungsaudit festgestellt wird, dass der Auditee von den Anforderungen abweicht, ohne dass diese Abweichung(en) kurzfristig behoben werden können,
- ☐ der Auditee die Durchführung der Überwachungs- oder Re- Zertifizierungsaudits, die in der erforderlichen Häufigkeit durchzuführen sind, nicht gestattet, oder
- ☐ der Auditee freiwillig um eine Aussetzung gebeten hat.

Wurde die Zertifizierung bereits fünf Monate ausgesetzt, so wird dem Auditee eine Frist von vier Wochen gesetzt, um die Prüfung des Managementsystems zu gestatten beziehungsweise zu beauftragen. Erfolgt keine Beauftragung, wird die Zertifizierung zurückgezogen.

Ist eine dauerhafte Konformitätsabweichung in bestimmten Teilen des Anwendungsbereichs nachgewiesen, so ist eine Einschränkung des Geltungsbereichs vorzunehmen. Als Konsequenz sind in jeder Beschreibung des Anwendungsbereichs die Einschränkungen zu dokumentieren. Dabei ist zu beachten, dass eine deutliche Abgrenzung zum weiterhin wirksamen Managementsystem möglich sein sollte.

Bei Aussetzung, Zurückziehung oder Einschränkung von Zertifizierungen ist der Status in der Liste der veröffentlichten Zertifizierungen zu ändern. Werbung mit der ursprünglichen Zertifizierung ist nicht mehr gestattet.

3.7 Besondere Pflichten des Zertifikatsinhabers

Zertifikatsinhaber sind verpflichtet,

- die hier bekannt gemachten Termine eigenständig einzuhalten und
- die Zertifizierungsstelle bei wesentlichen Änderungen des Scopes (Wegfall von relevanten Objekten, Erweiterungen und so weiter) unverzüglich zu informieren.