

Richtlinie zur Auditierung

Dokumenteninformation

Version	2.2
Datum der Version	22.09.2026
Inhaltsverantwortlicher	Marc Alexander Luge
Inkrafttreten	17.09.2021

INHALTSVERZEICHNIS

Seite

1. Zweck, Anwendungsbereich und Anwender	1
2. Verantwortlichkeiten im Zertifizierungsprozess	2
2.1. Rolle der RSMCERT	2
2.2. Rolle der Auditoren	2
2.3. Rolle der Fachexperten	3
3. Vorgehensweise Auditierung	4
3.1. Grundlegendes	5
3.1.1. Auditteam	5
3.1.2. Auditplan	5
3.1.3. Grundsätze der Auditierung	6
3.1.4. Dokumentation und Auditnachweise	7
3.1.5. Kommunikation während des Audits	7
3.1.6. Zertifizierungsdokumente	7
3.1.7. Durchführung Remote-Audits	7
3.2. Erstzertifizierungsaudits	8
3.2.1. Stage 1	8
3.2.2. Stage 2	8
3.2.3. Nachbesserungen, Ursachenanalyse, Nachforderungen	8
3.2.4. Zertifikatserteilung	9
3.3. Überwachungsaudits	9
3.4. Rezertifizierungsaudits	10
3.5. Nachaudits und Auditabbrüche	10
3.6. Audits aus besonderem Anlass	11
3.7. Erweiterungsaudits	11
4. Gültigkeit des Zertifikates	12
5. Erweiterung/Einschränkung des Geltungsbereichs des Zertifikates	13
6. Zertifikatsübernahmen	14
7. Aussetzung des Zertifikates	15
8. Entzug/Annullierung des Zertifikates	16

1. Zweck, Anwendungsbereich und Anwender

Das zu zertifizierende Unternehmen (nachfolgend kurz „Mandant“) muss über ein dokumentiertes Managementsystem verfügen und dies der RSMCERT GmbH (nachfolgend kurz „RSMCERT“) nachweisen.

Dieses Dokument beschreibt die Vorgehensweise bei Zertifizierungsleistungen von Managementsystemen nach

- DIN EN ISO/IEC 27001:2024 bzw. ISO/IEC 27001:2022,
- IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG (08/2015) und
- DIN EN ISO 9001:2015.

Spezifisch umfasst dies die Abläufe und Regeln innerhalb des Erstzertifizierungs-, Überwachungs- und Rezertifizierungsverfahrens sowie die

- Erteilung,
- Verweigerung,
- Aufrechterhaltung,
- Erneuerung,
- Erweiterung,
- Einschränkung,
- Aussetzung,
- Zurückziehung oder
- Wiederherstellung

der Zertifizierung in Anlehnung an die gültigen internationalen anwendbaren Normen und Regeln für die akkreditierten Konformitätsbewertungsstellen für Managementsysteme.

Darüber hinaus werden die Zuständigkeiten bei der Zertifizierung von Managementsystemen dargestellt, um sicherzustellen, dass die Tätigkeiten hinsichtlich Personals und Arbeitsmittel nach einheitlichen Verfahren durchgeführt werden.

2. Verantwortlichkeiten im Zertifizierungsprozess

Die Tätigkeiten und Verantwortlichkeiten verteilen sich innerhalb des Zertifizierungsprozesses auf die zuständige Konformitätsbewertungsstelle, sprich die RSMCERT, die durchführenden Auditoren und ggf. einen Fachexperten. Die jeweiligen Verantwortlichkeiten sind im Folgenden kurz dargestellt.

2.1. Rolle der RSMCERT

Die Geschäftsführung der RSMCERT ist die Leitung der Konformitätsbewertungsstelle. Weiterhin involviert sind die internen Auditoren, der Qualitätsmanagementbeauftragte sowie die Auftragnehmer (u. a. externe Auditoren, Fachexperten).

Die RSMCERT ist verantwortlich und besitzt das alleinige Recht für Entscheidungen in Bezug auf die Zertifizierung, einschließlich der Erteilung, Verweigerung und Aufrechterhaltung der Zertifizierung, Erweiterung oder Einschränkung des Geltungsbereichs der Zertifizierung, Erneuerung, Aussetzung oder Wiederherstellung nach einer Aussetzung, oder Zurückziehung der Zertifizierung.

Die Gruppe oder Einzelperson, welche diese Entscheidung trifft, muss die anzuwendende Norm und die Zertifizierungsanforderungen verstehen und muss die hierfür erforderliche Kompetenz besitzen.

2.2. Rolle der Auditoren

Die Prüfung und Bewertung des Managementsystems auf Konformität mit einem Standard werden von qualifizierten Auditoren durchgeführt.

Dies erfolgt durch:

- Prüfung und Bewertung der dokumentierten Beschreibung des Managementsystems,
- Prüfung und Bewertung des angewandten Systems in der Praxis (im Audit): Erstellen einer Auditdokumentation sowie
- Überwachung des angewandten Systems.

Im Auditteam ist der Lead Auditor insbesondere für folgende Aufgaben zuständig:

- Berichterstellung zur Bewertung der Zertifizierungsfähigkeit und der Dokumentation (Stage 1-Bericht) in Abstimmung mit dem Auditteam,
- Auditplanung und Terminabstimmung mit dem Mandanten (Auditplan Stage 1 und 2 erstellen),
- Gesprächsführung im Audit,
- Dokumentation der Auditergebnisse inkl. ggf. vorhandener Non-Conformities,
- Entscheidung über Nachaudit und dessen Umfang oder Auditabbruch sowie
- zeitnahe Übermittlung der Auditdokumentation an die RSMCERT (Richtwert: ca. zwei Wochen nach dem Audit).

2.3. Rolle der Fachexperten

Für die Tätigkeiten und Zuständigkeiten des Fachexperten im Rahmen eines Audits gemäß IT-Sicherheitskatalog § 11 Abs. 1a EnWG verweisen wir auf das Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog (für Netzbetreiber).

3. Vorgehensweise Auditierung

Die Audittätigkeiten werden in Übereinstimmung mit den betreffenden Leitlinien durchgeführt. Mandanten können sich über die Homepage der RSMCERT über den Prozess der Zertifizierung inkl. Laufzeit der Zertifikate, Erst- und Rezertifizierung sowie Überwachungsaudits für die definierten Normen informieren. Zusätzlich werden diese auf Wunsch im Rahmen eines Erstgesprächs – bspw. bei Rückfragen zur Erhebung von Informationen für den Auditierungs- oder Zertifizierungsprozess – darüber informiert.

Zu differenzieren ist zwischen den folgenden Audits:

- Erstzertifizierungsaudits,
 - Stage 1,
 - Stage 2,
- Überwachungsaudits,
- Rezertifizierungsaudits,
- Nachaudits und Auditabbrüche,
- Audits aus besonderem Anlass,
- Kombiniertes und integriertes Audit,
- Multi-Site-/Matrix-Zertifizierung und
- Erweiterungsaudit.

Die Auditziele werden von der RSMCERT festgelegt. Der Auditumfang und die Auditkriterien, einschließlich aller Änderungen, werden von der RSMCERT in Abstimmung mit dem Mandanten festgelegt. In den Auditzielen muss dabei beschrieben sein, was mit Hilfe des Audits erreicht werden soll.

Sie müssen Folgendes beinhalten:

- Feststellung der Konformität des Managementsystems des Mandanten oder von Teilen dieses Managementsystems mit den Auditkriterien,
- Feststellung der Aufrechterhaltung des bestehenden Managementsystems,
- Feststellung der Fähigkeit des Managementsystems, die Erfüllung der anzuwendenden gesetzlichen, behördlichen und vertraglichen Anforderungen durch den Mandanten sicherzustellen,
- Feststellung der Wirksamkeit des Managementsystems, um sicherzustellen, dass der Mandant begründet erwarten kann, seine festgelegten Ziele damit zu erreichen sowie
- falls anwendbar: Die Nennung von Bereichen für mögliche Verbesserungen des Managementsystems.

Der Auditumfang muss das Ausmaß und die Grenzen des Audits beschreiben, wie bspw. Standorte, Organisationseinheiten, Tätigkeiten und Prozesse.

Die Auditkriterien müssen als Referenz verwendet werden, gegen die die Konformität ermittelt wird, und müssen Folgendes beinhalten:

- die Anforderungen eines festgelegten normativen Dokuments zu Managementsystemen und
- die festgelegten Prozesse und Dokumentation des vom Mandanten entwickelten Managementsystems.

3.1. Grundlegendes

3.1.1. Auditteam

Die Antragsprüfer teilen die Auditoren und ggf. Fachexperten für das Audit zu. Diese Person/en führen das Audit im Namen der RSMCERT durch.

Das Auditteam wird formal benannt und mit den erforderlichen Informationen ausgestattet. Der Mandant hat die Möglichkeit, benannte Auditoren und Fachexperten im Vorfeld der Auditierung abzulehnen.

Die Auswahl der Auditoren/Fachexperten erfolgt auf Basis der Kompetenzmatrix bzw. der Übersicht zur personellen Besetzung.

Bei der Entscheidung über die Größe und Zusammensetzung des Auditteams muss Folgendes berücksichtigt werden:

- Auditziele, Auditumfang, Auditkriterien und geschätzter Auditzeitaufwand,
- ob das Audit ein kombiniertes oder integriertes Audit ist,
- die Gesamtkompetenz des Auditteams, die erforderlich ist, um die Auditziele zu erreichen,
- Zertifizierungsanforderungen (inkl. der gesetzlichen, behördlichen oder vertraglichen Anforderungen) sowie
- Sprache und Kultur.

Die Auditzuteilung ist eine Einzelentscheidung und muss im Voraus von der RSMCERT dem Auditor/Fachexperten mitgeteilt werden. Dies erfolgt entweder mündlich oder schriftlich. Mit jedem Auditor/Fachexperten wird ein Vertrag über das zugeteilte Audit abgeschlossen.

Die RSMCERT behält sich vor, das erforderliche Wissen und die erforderlichen Fertigkeiten des Lead Auditoren und der Auditoren durch Fachexperten, Übersetzer und Dolmetscher zu ergänzen.

In einem Audit der RSMCERT können verschiedene externe Parteien mitwirken/Teil haben:

- **Beobachter:** Die Anwesenheit und Begründung von Beobachtern bei einer Audittätigkeit muss vor Durchführung des Audits von der RSMCERT und dem Mandanten zugestimmt werden. Dabei darf der Beobachter den Auditprozess und das Auditergebnis nicht unangemessen behindern oder beeinflussen (bspw. die DAkKS oder Auditoren in Ausbildung).
- **Fachexperte:** Die Rolle von Fachexperten bei einer Audittätigkeit muss vor Durchführung des Audits von der RSMCERT und dem Mandanten vor dem Audit vereinbart werden.
- **Betreuer:** Jeder Auditor muss von einem Betreuer des Mandanten begleitet werden, es sei denn, es besteht eine andere Vereinbarung zwischen dem Lead Auditor und dem Mandanten. Betreuer werden zur Unterstützung des Audits für die Begleitung des Auditteams abgestellt. Das Auditteam muss dabei sicherstellen, dass die Betreuer den Auditprozess und das Auditergebnis nicht behindern oder beeinflussen.

3.1.2. Auditplan

Vor jedem Audit ist ein Auditplan zu erstellen. Der Auditplan muss im Hinblick auf die Auditziele und Auditumfang angemessen sein und dabei mindestens Folgendes beinhalten:

- die Auditziele,
- die Auditkriterien,

- den Auditumfang inkl. Feststellung der zu auditierenden Organisations- und Funktionseinheiten oder Prozesse,
- die Termine und Standorte, an denen Audittätigkeiten vor Ort durchgeführt werden, ggf. inkl. der Besuche von temporären Standorten und Audittätigkeiten, die remote durchgeführt werden,
- die vorgesehene Dauer der Audittätigkeiten vor Ort,
- die Rollen und Verantwortlichkeiten der Mitglieder des Auditteams und der Begleitpersonen, bspw. Beobachter sowie
- die Aufteilung der Auditoren (falls mehr als ein Auditor) nach gemeinsam und getrennt zu auditierenden Bereichen.

Insbesondere bei getrenntem Vorgehen der Auditoren muss der regelmäßige Informationsaustausch sichergestellt werden. Abhängig von der Gesamtdauer des Audits, sollte zumindest am Ende eines jeden Tages (bzw. bei kürzeren Audits zur Hälfte des Audits) ein Informationsaustausch im Auditteam erfolgen und auch der Mandant bzgl. des Auditfortschritts informiert werden.

Die an das Auditteam übertragenen Aufgaben müssen eindeutig definiert sein und erfordern vom Auditteam:

- die Struktur, grundsätzliche Regelungen, Prozesse, Verfahren, Aufzeichnungen und zugehörige Dokumente des Mandanten bzgl. der Managementsystemnorm zu prüfen und zu verifizieren,
- festzustellen, dass diese alle relevanten Anforderungen bzgl. des beabsichtigten Geltungsbereichs der Zertifizierung erfüllen,
- festzustellen, dass die Prozesse und Verfahren wirksam eingeführt, umgesetzt und aufrechterhalten werden, um Grundlage für das Vertrauen in das Managementsystem des Mandanten zu schaffen sowie
- dem Mandanten für seine eigenen Maßnahmen jeglichen Widerspruch zwischen der Politik des Mandanten, seiner Ziele und Vorgaben zu vermitteln.

Der Auditplan muss dem Mandanten vorab mitgeteilt werden und die Daten mit dem Mandanten abgestimmt werden.

Falls Remote-Audits durchgeführt werden, sind diese Tätigkeiten im Auditplan eindeutig zu kennzeichnen.

3.1.3. Grundsätze der Auditierung

Für Audits der RSMCERT gelten die folgenden vertrauensbildenden Grundsätze:

- **Unparteilichkeit:** Die RSMCERT stellt sicher, dass keine Interessenskonflikte zwischen der RSMCERT, den Auditoren und dem Mandanten bestehen. Alle relevanten Teilprozesse sind im Hinblick auf dieses Ziel überprüft.
- **Kompetenz:** Die RSMCERT 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 RSMCERT.
- **Vertraulichkeit:** Alle vom Mandanten, der den Antrag auf Konformitätsbewertung gestellt hat, für die Zertifizierung zur Verfügung gestellten Informationen werden, soweit nicht explizit aufgeführt, vertraulich behandelt.

- **Beschwerdemöglichkeit:** Die RSMCERT verfügt über ein Verfahren, mit dem Beschwerden bezüglich des Zertifizierungsprozesses aufgenommen und konstruktiv bearbeitet werden.

Ein Audit beginnt stets mit einem Einführungsgespräch und endet mit einem Abschlussgespräch.

Eine offizielle Eröffnungsbesprechung muss gemeinsam mit dem Management des Mandanten und gegebenenfalls mit den Personen, die die Verantwortung für die zu auditierenden Funktionen oder Prozesse tragen, durchgeführt werden. Der Zweck der Eröffnungsbesprechung, die üblicherweise vom Lead Auditor durchgeführt wird, besteht darin, kurz zu erläutern, auf welche Art und Weise die Audittätigkeiten durchgeführt werden.

Eine offizielle Abschlussbesprechung muss gemeinsam mit dem Management des Mandanten und gegebenenfalls mit den Personen, die die Verantwortung für die zu auditierenden Funktionen oder Prozesse tragen, durchgeführt werden.

3.1.4. Dokumentation und Auditnachweise

Die Auditierung der Auditoren erfolgt risikoorientiert auf Basis von Stichproben. Hinsichtlich der erfolgten Aufbau- sowie Wirksamkeitsprüfungen kommen verschiedene Prüfungsmethoden zum Einsatz.

3.1.5. Kommunikation während des Audits

Im Verlauf des Audits muss das Auditteam in regelmäßigen zeitlichen Abständen den Fortschritt des Audits bewerten und Informationen austauschen. Der Lead Auditor muss bei Bedarf die Aufgaben unter den Mitgliedern des Auditteams neuordnen und den Mandanten 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 (z. B. Sicherheit) bestehen kann, muss der Lead Auditor dem Mandanten und, falls möglich, der RSMCERT 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 Lead Auditor muss der RSMCERT über die Ergebnisse der ergriffenen Maßnahmen Bericht erstatten.

Der Lead Auditor muss gemeinsam mit dem Mandanten jeglichen Änderungsbedarf am Auditumfang, der sich im Verlauf der Audittätigkeiten vor Ort herausstellt, überprüfen und der RSMCERT darüber Bericht erstatten.

3.1.6. Zertifizierungsdokumente

Die Zertifizierungsdokumente dürfen nationale und internationale Normen als Quelle(n) referenzieren, die in der Erklärung zur Anwendbarkeit des Mandanten nach ISO/IEC 27001:2024, 6.1.3 d), als notwendig ermittelt werden.

3.1.7. Durchführung Remote-Audits

Es ist zulässig das Audit remote durchzuführen. Die RSMCERT hat ein Verfahren bestimmt, im Rahmen dessen der Umfang von Fernaudittätigkeiten („Fernaudits“) festgelegt wurde, die zum Auditieren eines Mandanten eingesetzt werden können.

Die Analyse muss vor der Durchführung eines Fernaudits durchgeführt werden. Die Ergebnisse der Analyse und die Begründung für den Einsatz eines Fernaudits während des Zertifizierungszyklus müssen dokumentiert werden.

Der Auditplan und der Auditbericht müssen eindeutige Hinweise darauf enthalten, ob Fernauditaktivitäten durchgeführt wurden.

Fernaudits dürfen nicht eingesetzt werden, wenn die Risikobeurteilung für die Wirksamkeit des Auditprozesses nicht annehmbare Risiken ermittelt.

3.2. Erstzertifizierungsaudits

Bei Erstzertifizierungen von Managementsystemen wird das Zertifizierungsaudit, gemäß DIN EN ISO/IEC 17021-1:2015-11, in zwei Stufen (Stages) gegliedert.

3.2.1. Stage 1

Stage 1 wird in der Regel durch den vorgesehenen Lead Auditor durchgeführt. In begründeten Fällen kann nach Abstimmung mit der RSMCERT davon abgewichen werden.

Vor dem Audit ist ein Auditplan zu erstellen und dem Mandanten rechtzeitig zu übersenden.

Ziel des Stage 1-Audits ist es, die Zertifizierungsfähigkeit des Mandanten, Reife des Managementsystems, besondere Gefährdungen und Risiken, gesetzliche und behördliche Aspekte und die standortspezifischen Bedingungen festzustellen.

Bei der Ermittlung des Abstands zwischen Stage 1 und Stage 2 werden die Erfordernisse des Mandanten berücksichtigt, um Lösungen zu den identifizierten Schwachstellen zu finden. In der Regel sollte der Abstand mindestens zwei Wochen und höchstens sechs Monate betragen. Ausnahmefälle sind zu dokumentieren.

Wird in Stage 1 festgestellt, dass das Unternehmen nicht ausreichend aufgestellt ist, kann nach Rücksprache mit dem Mandanten die Stage 1 auch wiederholt werden.

3.2.2. Stage 2

Ziel des Audits der Stage 2 ist es, die Umsetzung einschließlich der Wirksamkeit des Managementsystems des Mandanten zu beurteilen. Das Audit der Stage 2 findet an dem/den Standort/en des Mandanten statt. Am Audittag werden im Einführungsgespräch gemäß dem mit dem Mandanten abgestimmten Auditplan die Vorgehensweise und die Ziele etc. erörtert. Während des Audits überzeugt sich das Auditteam, ob die schriftlichen Festlegungen des Managementsystems auch entsprechende Anwendung finden und das Managementsystem den Anforderungen der Bezugsnorm/en entspricht. Dies erfolgt durch Begehungen, Interviews mit der Geschäftsführung und den Mitarbeitern sowie durch Einsichtnahme und Prüfung von Managementsystemdokumenten, Aufzeichnungen, Richtlinien etc.

3.2.3. Nachbesserungen, Ursachenanalyse, Nachforderungen

Sofern Nachbesserungen aufgrund von Major Non-Conformities, welche die Wirksamkeit des Betriebes des Managementsystems beeinträchtigen, erforderlich sind, stellt die RSMCERT den Mandanten ein Template zur Ursachenbeschreibung und zu den zu planenden Korrekturmaßnahmen zur Verfügung.

Wenn eine Verifizierung der Umsetzung der Korrekturen und Korrekturmaßnahmen zu Major Non-Conformities innerhalb von sechs Monaten nach dem letzten Tag des Stage 2-Audits nicht möglich ist, muss ein erneutes Stage 2-Audit durchgeführt werden.

3.2.4. Zertifikatserteilung

Bei positivem Auditergebnis und der Behebung aller Major Non-Conformities im festgelegten Zeitraum empfiehlt der Lead Auditor/das Auditteam die Zertifikatserteilung. Das Verfahren wird von unabhängiger Stelle in Form einer fachlichen Prüfung geprüft und somit die Entscheidung zur Zertifikatserstellung unterstützt.

Die Zertifizierung kann nur dann erfolgen, wenn alle Major Non-Conformities behoben sind und eine Abnahme in Form der fachlichen Prüfung der RSMCERT vorliegt. Das bedeutet bei einem Nachaudit, dass auch dieses erfolgreich durchgeführt worden sein und eine positive Bewertung evtl. beizubringender neuer Unterlagen stattgefunden haben muss.

Das Zertifikat wird durch die RSMCERT erstellt. Die Zertifikate haben eine Gültigkeit von drei Jahren. Für das Ende der Gültigkeit ist der Zeitpunkt der Zertifizierungsentscheidung maßgebend. Die Beschriftung der Zertifikate erfolgt entsprechend der Zertifikatsvorlagen.

3.3. Überwachungsaudits

Innerhalb der Gültigkeit des Zertifikates werden einmal jährlich Überwachungsaudits durchgeführt. Nach drei Jahren ist ein vollständiges Audit (Rezertifizierungsaudit) erforderlich. Überwachungsaudits müssen einmal im Kalenderjahr erfolgen. Unabhängig vom regulären Zertifizierungszyklus kann die RSMCERT jederzeit eine Überwachung anordnen, wenn dies in begründeten Fällen erforderlich erscheint, z. B. bei wesentlichen Änderungen oder Beschwerden.

Darüber hinaus ist die RSMCERT berechtigt, sich jederzeit nach Terminvereinbarung durch geeignete Überwachungsmaßnahmen davon zu überzeugen, dass die Kriterien zur Zertifizierung eingehalten werden (Überprüfung von Webseiten, Werbematerial des Mandanten, Aufforderung zur Bereitstellung von Dokumenten und Aufzeichnungen etc.).

Das Auditprogramm für den Zertifizierungszyklus stellt die RSMCERT in ihren Auditberichten den Mandanten zur Verfügung, sodass der Mandant einsehen kann, wann welche Kontrollen auditiert werden.

Bei Bedarf (z. B. wegen Änderung der Mitarbeiterzahlen, der Komplexität der Prozesse etc.) wird der Umfang der Überwachung neu festgelegt und dem Mandanten mitgeteilt. Zu diesem Zweck erfolgt eine jährliche Validierung auf Änderungen. Wenn nicht mitgeteilte Änderungen vom Auditteam im Rahmen des Audits festgestellt werden, müssen diese der RSMCERT sofort gemeldet werden. Die Auditzeiten werden entsprechend angepasst.

Bei Identifikation von Major Non-Conformities im Rahmen der Überwachungsaudits verfährt der Auditor wie im Zertifizierungsaudit. Der Auditor hat ein Nachaudit anzusetzen, wenn die zugesagten Unterlagen nicht zum vereinbarten Termin eingereicht werden bzw. inhaltlich unzureichend sind. Durch das Vorhandensein von Major Non-Conformities, besteht die Möglichkeit eines Zertifikatsentzuges.

Das 1. Überwachungsaudit nach der Erstzertifizierung muss spätestens 12 Monate nach dem Tag der Zertifizierungsentscheidung durchgeführt und abgeschlossen werden. Die Karenzzeit für das Überwachungsaudit beträgt bezogen auf den Tag der Zertifizierungsentscheidung -3/+0 Monate.

Das 2. Überwachungsaudit muss 24 Monate nach dem Tag der Zertifizierungsentscheidung durchgeführt werden, wobei hier eine Karenzzeit von -3/+3 Monaten bezogen auf den Tag der Zertifizierungsentscheidung festgelegt ist, sofern die Anforderung eingehalten wird, dass pro Kalenderjahr ein Audit absolviert wurde.

Die Aussetzung von Zertifikaten, die im Rahmen des IT-Sicherheitskatalogs § 11 Abs. 1a EnWG vergeben werden, werden von der RSMCERT unmittelbar der BNetzA gemeldet.

3.4. Rezertifizierungsaudits

Zweck des Rezertifizierungsaudits ist es, die kontinuierliche Konformität und Wirksamkeit des Managementsystems als Ganzes sowie seine anhaltende Bedeutung und Anwendbarkeit auf den Geltungsbereich der Zertifizierung zu bestätigen. Die Leistungsfähigkeit des Managementsystems wird über den Zeitraum der Zertifizierung berücksichtigt.

Das Rezertifizierungsaudit beinhaltet die Dokumentenprüfung und ein Vor-Ort-Audit, das die Wirksamkeit des Managementsystems in seiner Gesamtheit prüft. Der Umfang des Rezertifizierungsaudits entspricht etwa zwei Drittel des Erstzertifizierungsaudits und sollte sich insbesondere auf durchgeführte Korrekturmaßnahmen konzentrieren (Berücksichtigung der Auditergebnisse des letzten Zertifizierungszyklus). Es werden alle Normen Anforderungen auditiert.

Wenn während eines Rezertifizierungsaudits Fälle von Major Non-Conformities oder mangelnde Nachweise für die Konformität identifiziert werden, so muss die RSMCERT Fristen für umzusetzende Korrekturen und Korrekturmaßnahmen noch vor Ablauf der Zertifizierung bestimmen. Ist die Maßnahmenumsetzung bis dahin nicht möglich, muss der Mandant darüber informiert werden, dass er ab dem Ende der Laufzeit kein gültiges Zertifikat mehr besitzt (inklusive aller Konsequenzen bzgl. Nutzungsrecht von Zertifikat und Logo). Zudem wird der Mandant informiert, wie die Zertifizierung wiederhergestellt werden kann.

Die Entscheidung über die Rezertifizierung wird unter Berücksichtigung der Empfehlung des Auditteams, der Ergebnisse aus der Bewertung des Systems über den Zeitraum der Zertifizierung und von beim Mandanten eingegangenen Beschwerden getroffen.

Grundsätzlich gilt, dass das Rezertifizierungsaudit vor dem Ablauf des Zertifikats stattfinden und abgeschlossen sein muss. Bei Überschreitung der Gültigkeit schließt das Folgezertifikat trotz des verspäteten Rezertifizierungsaudits lückenlos an das vorherige Zertifikat an (d. h. das Ablaufdatum des Zertifikates entspricht dem des vorherigen Zertifikats + 3 Jahre). Gültig wird das Zertifikat mit dem Tag der Zertifizierungsentscheidung. Ab einer Überschreitung von mehr als sechs Monaten, ist eine Neuzertifizierung mit entsprechendem Auditaufwand durchzuführen. Auch im Falle signifikanter Änderungen für das Managementsystem, z. B. gesetzliche oder betriebliche Änderungen oder signifikanten Änderungen am/im Geltungsbereich, oder im Zuge einer Zertifikatsübernahme kann bei einer Rezertifizierung ein Audit der Stage 1 erforderlich werden.

3.5. Nachaudits und Auditabbrüche

Ein Nachaudit ist erforderlich, wenn z. B.

- eine oder mehrere Non-Conformities als wesentlich (Major) bewertet werden und die damit zum Versagen des Managementsystems führen und/oder
- eine dokumentierte Regelung und durchgehende Umsetzung von Normenforderungen fehlen.

Führt eine Major Non-Conformity zu einer wesentlichen Einschränkung der Prozesse, ist es unerheblich, ob die Non-Conformity sich auf eine oder mehrere Organisationseinheiten oder eine oder mehrere Normenforderungen beziehen.

Die Entscheidung über ein Nachaudit wird durch den Lead Auditor in Abstimmung mit dem Auditor gefällt. Beim Nachaudit erfolgt im Wesentlichen die Auditierung der Umsetzung und damit Behebung der Non-Conformities.

Der zeitliche Abstand zwischen Zertifizierungsaudit und Nachaudit richtet sich nach dem Umfang der Non-Conformities. Das begrenzte Nachaudit muss aber maximal sechs Monate nach dem Zertifizierungs-, Überwachungs- oder Rezertifizierungsaudit stattfinden. Wurden auch im Nachaudit Major Non-Conformities festgestellt, kann der Mandant in einem angemessenen Zeitraum die Zertifizierung neu beantragen (siehe hierzu auch Kapitel 7).

3.6. Audits aus besonderem Anlass

In ausgewählten Situationen besteht die Notwendigkeit eines Audits aus besonderem Anlass. Dazu kann bspw. eine Sitzverlagerung zählen.

Es kann für die RSMCERT zudem erforderlich sein, kurzfristig angekündigte Audits bei einem zertifizierten Mandanten durchzuführen,

- um Beschwerden zu untersuchen und damit die mögliche Aufrechterhaltung der Zertifizierung prüfen/bestätigen zu können,
- als Konsequenz von Änderungen, die das Managementsystem beeinträchtigen können, um die Aufrechterhaltung der Zertifizierung prüfen/bestätigen zu können sowie
- als Konsequenz auf ausgesetzte Mandantenzertifizierungen, um eine Neubewertung des Managementsystems und die Rückgabe der Zertifizierung zu ermöglichen.

In solchen Fällen muss die RSMCERT

- die Bedingungen, unter denen solche Audits durchgeführt werden, beschreiben und den zertifizierten Mandanten im Voraus bekannt machen sowie
- bei der Benennung des Auditteams zusätzliche Sorgfalt walten lassen, da dem Mandanten die Möglichkeit fehlt, gegen Mitglieder des Auditteams Einwand zu erheben.

3.7. Erweiterungsaudits

Soll der Umfang der bestehenden Zertifizierung erweitert werden, so kann die Einbeziehung der Erweiterung durch ein Erweiterungsaudit erfolgen. Die Durchführung des Erweiterungsaudits kann im Rahmen eines Überwachungsaudits, Rezertifizierungsaudits oder zu einem eigens angesetzten Termin erfolgen.

Erweiterungen können beinhalten

- Änderung/Erweiterung der Norm,
- wesentliche Änderungen der Ausschlüsse,
- Änderung des Geltungsbereiches,
- Aufnahme zusätzlicher Standorte.

Vom Auditor/Auditteam werden die für den erweiterten Bereich relevanten Managementsystemdokumente geprüft und alle für die Erweiterung relevanten Normenforderungen auditiert. Das Erweiterungsaudit wird im Auditbericht mit allen Anlagen dokumentiert. Wie beim Zertifizierungsaudit ist der RSMCERT die Auditdokumentation zur Prüfung und ggf. zur Zertifikatserteilung einzureichen.

Für das Erstzertifizierungsaudit des neuen Anwendungsbereichs muss der Zeitaufwand basierend auf der Anzahl an Personen und Standorten, die zum bereits bestehenden Anwendungsbereich hinzugefügt werden, berechnet werden.

4. Gültigkeit des Zertifikates

Die Gültigkeit der ausgegebenen Zertifikate beträgt drei Jahre ab Ausstellungsdatum auf Basis positiver Zertifizierungsentscheidung, sofern sämtliche Bedingungen zur Aufrechterhaltung der Gültigkeit vom Mandanten erfüllt werden.

Zwingende Voraussetzung zur Aufrechterhaltung der Gültigkeit des Zertifikates und der damit verbundenen Berechtigung zur Führung des Zertifikates und zur Nutzung des Zertifizierungszeichens sind insbesondere die Durchführung eines jährlichen Überwachungsaudits mit positiver Überwachungsentscheidung sowie ein aufrechtes Vertragsverhältnis.

Die Zertifikate sind während deren Gültigkeit Eigentum der RSMCERT und gehen nach deren Ablauf ins Eigentum des Mandanten über.

Der Auditbericht ist Eigentum der RSMCERT.

5. Erweiterung/Einschränkung des Geltungsbereichs des Zertifikates

Die Erweiterung/Einschränkung des Zertifikats auf/um weitere/wegfallende Tätigkeiten oder Standorte muss vom Unternehmen bei der RSMCERT beantragt und ein aktualisierter oder neuer Informations- und Erhebungsbogen und alle nötigen Dokumente über die Erweiterung/Einschränkung und die Einbindung/Entfernung ins/aus dem Managementsystem zur Verfügung gestellt werden. Die RSMCERT überprüft zeitnah die Dokumente.

Im Falle einer Einschränkung des Geltungsbereichs oder bspw. Aufgabe eines Standortes muss das Zertifikat entsprechend geändert werden. Eine Einschränkung des Geltungsbereichs findet auch statt, wenn einige Teile der Normanforderungen dauerhaft oder schwerwiegend nicht mehr erfüllt werden.

Bei der Einschränkung des Zertifikats hat das Unternehmen alle Werbemittel dementsprechend zu ändern.

Bei Erweiterung des Geltungsbereichs muss die RSMCERT als Konsequenz auf eine beantragte Erweiterung des Geltungsbereichs einer schon erteilten Zertifizierung eine Bewertung des Antrags vornehmen und alle erforderlichen Audittätigkeiten festlegen, um zu entscheiden, ob eine Erweiterung erteilt werden kann oder nicht. Dies darf im Zusammenhang mit einem Überwachungsaudit erfolgen.

Eine Erweiterung des Geltungsbereichs und/oder Aufnahme neuer Standorte kann nach einer Begutachtung vor Ort erfolgen, die im Rahmen des nächsten Überwachungsaudits oder Rezertifizierungsaudits durchgeführt werden kann. Nach erfolgreichem Audit und erneuter Zertifizierungsentscheidung wird das Zertifikat erweitert.

6. Zertifikatsübernahmen

Sofern eine Zertifikatsübernahme im Rahmen eines 1. oder 2. Überwachungsaudits oder einer Rezertifizierung erfolgt, ist eine Bewertung vorzunehmen. Die Vorgaben gehen aus dem IAF-Dokument „Verbindliches Dokument für die Übertragung akkreditierter Zertifizierungen von Managementsystemen“ (IAF MD2 in der jeweils aktuellen Version) hervor.

Seitens der RSMCERT ist ein Verfahren eingerichtet, um ausreichende Informationen zu erhalten, um eine Zertifizierungsentscheidung treffen zu können und um den zu übertragenden Mandanten über den Prozess zu informieren. Eine Zertifikatsübernahmebewertung darf ausschließlich durch kompetentes Personal erfolgen. Die RSMCERT führt die Bewertung durch internes Personal durch.

7. Aussetzung des Zertifikates

Die RSMCERT wird Zertifikate aussetzen, wenn

- der zertifizierte Mandant die Durchführung der planmäßigen Überwachungs- oder Rezertifizierungsaudits nicht gestattet,
- ein zertifiziertes Managementsystem eines Mandanten die Zertifizierungsanforderungen (einschließlich der Anforderungen an die Wirksamkeit des Managementsystems) dauerhaft oder schwerwiegend nicht erfüllt,
- Non-Conformities nicht im vereinbarten Zeitraum abgestellt werden,
- Verstöße gegen die Anzeigepflicht bei wesentlichen Änderungen vorliegen sowie
- der zertifizierte Mandant es wünscht.

Bei Aussetzung ist die Zertifizierung zeitweise außer Kraft gesetzt. Das Unternehmen hat die Werbung, Verweise und sonstige Nutzung des Zertifikats bei Aussetzung unverzüglich einzustellen. Die Information über das Aussetzen des Zertifikats wird von der RSMCERT öffentlich zugänglich gemacht.

Wenn die Probleme, die zur Aussetzung geführt haben, binnen vier bis acht Wochen nicht gelöst worden sind, kann das Unternehmen eine Neubewertung beantragen. Dieses Verfahren muss spätestens sechs Monate nach Aussetzung des Zertifikates abgeschlossen sein. Erfolgt sie nicht, gibt es nur noch die Möglichkeit einer Neuzertifizierung.

8. Entzug/Annullierung des Zertifikates

Die RSMCERT ist verpflichtet, das Zertifikat zu jeder Zeit während der Gültigkeitsdauer vorübergehend auszusetzen oder dauerhaft zu entziehen, wenn sie Kenntnis davon erlangt, dass die Zertifizierungsvoraussetzungen vorübergehend oder dauerhaft nicht mehr vorliegen. Die RSMCERT kann Zertifikate entziehen/annullieren, wenn

- Zertifikate missbräuchlich verwendet werden. Missbrauch liegt vor, wenn
 - die Zertifikatswerbung den Eindruck vermittelt, dass Produkte zertifiziert wurden oder Bereiche bzw. Tätigkeiten zertifiziert wurden, für die das Zertifikat nicht gilt,
 - das Zertifikat auf Dritte oder Nachfolger übertragen wird und
 - das Zertifikat für nicht zertifizierte Unternehmensbereiche verwendet wird.
- Angaben bzgl. des Managementsystems, der Organisation oder Verwendung des Zertifikates unvollständig oder unwahr sind,
- Überwachungsaudits ergeben, dass sich wesentliche Voraussetzungen für die Zertifikatserteilung geändert haben,
- die Gültigkeitsdauer des Zertifikats abgelaufen ist,
- gegen geltendes Recht verstoßen wird,
- die erstellte und versandte Rechnung für die Zertifizierung bzw. für die Überwachung trotz Mahnung nicht spätestens zwei Monate nach Ausstellung der jeweiligen Rechnung beglichen wurde sowie
- die antragstellende Organisation notwendige Korrekturmaßnahmen während der vereinbarten Frist nicht durchgeführt hat.

Bei Missbrauch wird das Zertifikat sofort entzogen.

Bei Entzug/Annullierung des Zertifikates wird das Mandat sofort benachrichtigt, aus der Liste der zertifizierten Mandate gelöscht und die Information über den Entzug von der RSMCERT öffentlich zugänglich gemacht. Das Unternehmen hat die Werbung, Verweise auf und sonstige Nutzung des Zertifikates und des Zertifizierungszeichens unverzüglich einzustellen.

Spezifisch beim IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG: Die RSMCERT informiert die Bundesnetzagentur unverzüglich über die Aussetzung bzw. Rücknahme des Zertifikats mit E-Mail an it-sicherheitskatalog@bnetza.de. Dies erfolgt durch den Geschäftsführer, den Prokuristen oder den Qualitätsmanagementbeauftragten.