

Inhaltsverzeichnis

1. Einleitung
2. Vorbereitung auf die Zertifizierung
3. Der Weg zum Zertifikat
4. Der Zertifizierungszyklus
5. Besondere Szenarien
6. Unparteilichkeit und Vertraulichkeit
7. Zeichennutzung
8. Beschwerden und Einsprüche
9. Änderungsmanagement

1. Einleitung

Dieser Leitfaden gibt Ihnen einen umfassenden Überblick um den gesamten Zertifizierungsprozess nachvollziehen und verstehen zu können. Wir begleiten Sie durch alle Phasen der Zertifizierung und stehen Ihnen für Rückfragen jederzeit zur Verfügung. Wir möchten Sie als unseren Kunden bestmöglich informieren und sicherstellen, dass Sie genau wissen, womit Sie im Rahmen Ihrer Zusammenarbeit mit der Advanced Audit and Analytics GmbH (AAA) rechnen können und welche Leistungen Sie von uns erhalten.

Als Kunde der AAA erhalten Sie transparente Informationen über:

- den Ablauf der Zertifizierung
- Ihre Rechte und Pflichten
- unsere Verfahren und Anforderungen
- den Umgang mit Ihrer Organisation während des gesamten Zertifizierungszyklus

2. Vorbereitung auf die Zertifizierung

2.1 Anfrage

Zur Vorbereitung der Zertifizierung Ihres Managementsystems auf Grundlage der geltenden Normen sind einige detaillierte Angaben zu Ihrem Unternehmen erforderlich. Bitte füllen Sie hierfür den vorgesehenen Antragsfragebogen vollständig und wahrheitsgemäß aus. Die von Ihnen gemachten Angaben verwenden wir ausschließlich zur Erstellung eines für Sie kostenfreien und unverbindlichen Angebots. Mit der Übermittlung des Antrags entsteht kein rechtsverbindliches Vertragsverhältnis.

Gerne bieten wir Ihnen ein kostenloses Informationsgespräch an, in dem wir gemeinsam mögliche Rückfragen zum Antragsverfahren und zum Fragebogen klären.

2.2 Der Zertifizierungsantrag

Für eine Zertifizierung benötigen wir von Ihnen folgende Informationen:

2.2.1 Organisationsinformationen

- Geltungsbereich der Zertifizierung mit relevanten Einzelheiten:
 - Standorte und Adressen
 - Spezifische Anforderungen des Zertifizierungsprogramms
 - Namen der Verantwortlichen
 - Prozesse und Tätigkeiten
 - Verfügbare Ressourcen
 - Organisationsstrukturen und Beziehungen
 - Rechtliche Verpflichtungen

2.2.2 Managementsystem-spezifische Angaben

- Normen und Standards, nach denen eine Zertifizierung angestrebt wird
- Ausgegliederte Prozesse, die die Konformität beeinflussen
- Beratungsleistungen bezüglich des zu zertifizierenden Managementsystems (falls in Anspruch genommen)

2.2.3 Besonderheiten für ISO/IEC 27001-Zertifizierungen

Bei ISMS-Zertifizierungen ist zusätzlich zu klären:

- Ob vertrauliche/sensible ISMS-bezogene Daten dem Auditteam nicht zur Verfügung gestellt werden können
- Begründung für eventuelle Einschränkungen
- AAA entscheidet, ob trotz fehlender Informationen ordnungsgemäß geprüft werden kann
- Vorabprüfung, ob sensible Daten über sichere elektronische Kanäle übertragen werden können. Bei Einschränkungen bzgl. vertraulicher Informationen wird ein hybrider Ansatz (Off-Site + On-Site) gewählt.

3.3 Antragsprüfung und Angebotserstellung

Nach Eingang Ihres Antrags prüfen wir:

3.3.1 Bewertungskriterien

- Vollständigkeit der Unterlagen
- Erfüllung der Zertifizierungsvoraussetzungen
- Vereinbarkeit mit unserem Akkreditierungsbereich
- Verfügbare Ressourcen (Personal, Fachkompetenz)
- Terminliche Machbarkeit

3.3.2 Mögliche Entscheidungen

Annahme des Antrags:

- Erstellung eines individuellen Angebots

Ablehnung des Antrags bei:

- Mangelnder Vorbereitung oder Verständnis

- Nichterfüllung der Zertifizierungsvoraussetzungen
- Fehlenden Ressourcen oder Engagement der Führungsebene
- Unvereinbarkeit mit dem Geltungsbereich der AAA
- Vertraglichen oder finanziellen Gründen
- Gefährdung der Unparteilichkeit
- Schwerwiegenden Verstößen gegen gesetzliche Anforderungen
- Erheblichen Sicherheits- oder Qualitätsrisiken
- Fehlender Kooperationsbereitschaft

Bei Ablehnung erhalten Sie eine schriftliche Begründung und Hinweise zu erforderlichen Voraussetzungen für eine spätere Antragstellung.

3.4 Zertifizierungsvereinbarung

Bei Annahme unseres Angebots wird eine Zertifizierungsvereinbarung in Form eines Vertrags abgeschlossen, der enthält:

- Alle vorgesehenen Audittätigkeiten
- Gebühren und Zahlungsmodalitäten
- Rechte und Pflichten beider Parteien
- Vertragsbedingungen
- Laufzeit und Kündigungsbestimmungen

4. Der Weg zum Zertifikat – Überblick über den Ablauf

4.1 Auditplanung

4.1.1 Auditprogramm-Entwicklung

Wir erstellen für Ihren gesamten Zertifizierungszyklus ein Auditprogramm, das umfasst:

- Erstzertifizierung (Stufe 1 und 2)
- Überwachungsaudits
- Re-Zertifizierungsaudit

4.1.2 Auditorenauswahl

Qualifizierte Auditoren werden basierend auf folgenden Kriterien ausgewählt:

- Fachkompetenz in Ihrer Branche
- Erfahrung mit der entsprechenden Norm
- Verfügbarkeit und Unabhängigkeit
- Sprachkenntnisse (falls erforderlich)

Ihr Recht auf Ablehnung: Sie können vorgeschlagene Auditoren aus sachlich gerechtfertigten Gründen ablehnen.

4.1.3 Terminplanung

- Stufe 1-Audit: Dokumentenprüfung und Bereitschaftsbewertung
- Zeitabstand: Zwischen Stufe 1 und 2 sollten mindestens 4 Wochen liegen
- Stufe 2-Audit: Wirksamkeitsprüfung vor Ort

4.2 Audit-Durchführung

Die AAA führt Audits bevorzugt off-site durch, um Effizienz zu steigern, die Umwelt zu schonen und Kosten zu optimieren. Dabei kommen elektronische Mittel nach ISO/IEC 17021-1 zum Einsatz:

- Remote-Dokumentenprüfung über sichere Datenübertragung
- Virtuelle Standortbeurteilung via Videokonferenz-Technologie
- Online-Gespräche mit Führungskräften und Mitarbeitern
- Digitale Bewertung der internen Audits und Managementbewertung
- Remote-Zugang zu relevanten elektronischen Systemen (soweit möglich)

Normkonformität und Qualitätssicherung:

- Auditoren verfügen über angemessene Kompetenz für elektronische Auditverfahren
- Ausreichende Nachweise werden erlangt für fundierte Konformitätsbewertung
- Zusätzliche On-Site-Beurteilungen erfolgen bei Bedarf zur Sicherstellung der Auditqualität
- Datenschutz und Informationssicherheit werden während der gesamten Remote-Auditierung gewährleistet

On-Site-Beurteilungen erfolgen bei Stufe-2-Audit und Stichprobenprüfungen bei Multi-Site-Organisationen und dann, wenn:

- Die elektronischen Mittel nicht ausreichende Nachweise liefern
- Spezielle technische Infrastruktur vor Ort beurteilt werden muss
- Komplexe organisatorische Strukturen eine physische Begutachtung erfordern
- Der Kunde ausdrücklich eine Vor-Ort-Bewertung wünscht

4.2.1 Teilnahme von Beobachtern

Bei Audits können Beobachter anwesend sein, z. B.

- DAkkS-Begutachter zur Überwachung der Zertifizierungsstelle
- Auditoren in Ausbildung (Trainee) als Teil ihrer Qualifikation
- Interne Qualitätssicherer der Advanced Audit and Analytics GmbH

Der Teilnahme der Beobachter muss zugestimmt und gleiche Zugänge wie für Auditoren ermöglicht werden. Beobachter nehmen nicht aktiv am Audit teil und unterliegen denselben Vertraulichkeitsverpflichtungen als Auditoren.

4.3 Stufe 1-Audit (Dokumentenprüfung)

4.3.1 Ziele des Stufe 1-Audits

- Bewertung der dokumentierten Informationen zum Managementsystem
- Standortbeurteilung und Bewertung der standortspezifischen Bedingungen
- Feststellung der Auditbereitschaft für Stufe 2
- Bewertung des Reifegrads des Managementsystems
- Informationssammlung über Geltungsbereich, Prozesse und Standorte
- Überprüfung gesetzlicher Anforderungen

4.3.2 Ergebnis

- Auditbericht mit Feststellungen zur Auditbereitschaft
- Empfehlungen für Verbesserungen vor Stufe 2
- Identifizierte Schwachstellen und erforderliche Maßnahmen

4.4 Stufe 2-Audit (Wirksamkeitsprüfung)

4.4.1 Ziele des Stufe 2-Audits

- Konformitätsprüfung mit allen Normanforderungen
- Wirksamkeitsbewertung des Managementsystems
- Leistungsüberwachung und Zielerreichung
- Operative Lenkung der Prozesse
- Compliance-Bewertung bezüglich gesetzlicher Anforderungen

4.4.2 Durchführung

- Vor-Ort-Audit mit Begehungen und Interviews
- Dokumentenprüfung (vertieft gegenüber Stufe 1)
- Stichprobenprüfungen in verschiedenen Bereichen
- Bewertung der Managementbewertung und internen Audits

4.5 Abweichungsmanagement

4.5.1 Klassifizierung von Abweichungen

Wesentliche Nichtkonformität (NC 1):

- Beeinträchtigung der Managementsystemziele
- Systemversagen oder mehrere zusammenhängende Nebenabweichungen

Untergeordnete Nichtkonformität (NC 2):

- Keine Beeinträchtigung der Systemziele
- Isolierte Einzelfälle

4.5.2 Behandlung von Abweichungen

- Mitteilung aller festgestellten Nichtkonformitäten beim Abschlußgespräch
- Fristsetzung für Korrekturmaßnahmen (in der Regel 90 Kalendertage)
- Ursachenanalyse und Maßnahmenplanung durch Kunde

- Verifikation der Maßnahmen durch AAA

Bei wesentlichen Nichtkonformitäten: Nachweis der erfolgreichen Umsetzung vor Zertifikatserstellung erforderlich

Bei untergeordneten Nichtkonformitäten: Überprüfung im weiteren Zertifizierungsprozess

4.6 Zertifizierungsentscheidung

4.6.1 Entscheidungsprozess

Treffen von Zertifizierungsentscheidungen inkl. Ergebnisse (z. B. Erteilung, Ablehnung, Auflagen) auf Basis vollständiger schlüssiger Entscheidungsgrundlagen durch einen Lead Auditor.

Es gilt das Trennungsprinzip: Lead Auditoren dürfen keine Entscheidung über Audits treffen, bei denen sie selbst beteiligt waren.

4.6.2 Entscheidungsgrundlagen

- Vollständige Auditberichte
- Nachweis der Schließung aller Hauptabweichungen
- Bewertung der Systemwirksamkeit
- Konformität mit allen Normanforderungen

4.6.3 Mögliche Entscheidungen

- Zertifikatserstellung bei vollständiger Konformität
- Bedingte Zertifizierung mit Auflagen bei: Nebenabweichungen, die im weiteren Zyklus geschlossen werden.
- Verweigerung der Zertifizierung bei:
 - Nicht geschlossenen Hauptabweichungen nach Ablauf der Frist (6 Monate nach Stufe 2-Audit).
 - Schwerwiegendem Systemversagen
 - Unzureichender Systemwirksamkeit
 - Mangelnder Kooperationsbereitschaft während des Audits

Bei Verweigerung:

- Schriftliche Begründung
- Hinweis auf Einspruchrecht
- Möglichkeit der Neubeantragung nach Behebung der Mängel

4.7 Zertifikatsausstellung

4.7.1 Zertifikatsinhalte

- Organisationsname und -adresse
- Geltungsbereich der Zertifizierung
- Zugrunde liegende Norm(en)
- Zertifikatnummer
- Ausstellungs- und Ablaufdatum

- Gültigkeitsdauer (3 Jahre)
- Standorte (bei Multi-Site-Zertifizierung im Anhang)

4.7.2 Eigentumsverhältnisse

Zertifikate bleiben Eigentum der AAA.

Zertifikatskopien können auf Wunsch erstellt werden.

5. Der Zertifizierungszyklus

5.1 Übersicht

Ein vollständiger Zertifizierungszyklus umfasst 3 Jahre mit folgenden Audits:

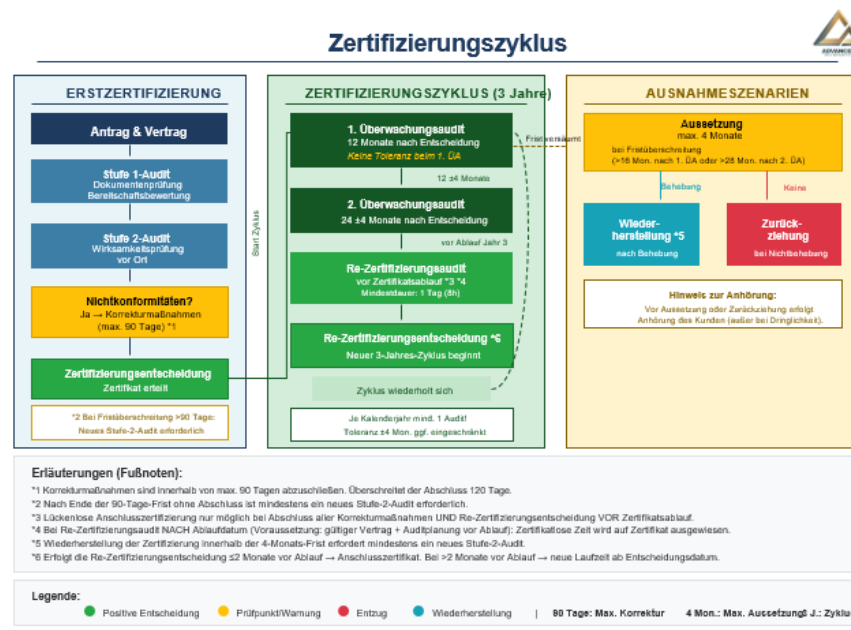
Erstzertifizierung (Stufe 1 + 2), Zertifizierungsentscheidung = Beginn des Zertifizierungszyklus

Jahr 1: 1. Überwachungsaudit

Jahr 2: 2. Überwachungsaudit

Jahr 3: Re-Zertifizierungsaudit (neuer Zyklus)

Die Re-Zertifizierungsaudit muss vor Ablauf des Zertifikates mit der Re-Zertifizierungsentscheidung abgeschlossen sein. Es beginnt ein neues Zertifizierungszyklus mit der Planung des Auditprogramms.



5.2 Überwachungsaudits

Überwachungsaudits können ebenfalls bevorzugt off-site durchgeführt werden, sofern die Normanforderungen erfüllt und ausreichende Nachweise erlangt werden. Bei kritischen Feststellungen oder auf Kundenwunsch erfolgen On-Site-Beurteilungen.

5.2.1 Zweck und Häufigkeit

- Jährliche Durchführung (12 ±3 Monate)
- Aufrechterhaltung der Zertifikatsgültigkeit
- Kontinuierliche Überwachung der Systemkonformität

5.2.2 Auditumfang

- Wesentliche Prozesse des Managementsystems
- Interne Audits und deren Wirksamkeit
- Managementbewertung und Folgeaktivitäten
- Korrekturmaßnahmen aus vorherigen Audits
- Änderungen am System oder der Organisation

5.3 Re-Zertifizierung

5.3.1 Zeitpunkt und Umfang

- Vor Ablauf der 3-jährigen Gültigkeit
- Vollständige Auditierung aller Systemelemente
- Überprüfung der kontinuierlichen Verbesserung

5.3.2 Besonderheiten

- Nahtlose Verlängerung bei rechtzeitiger Durchführung (Zertifikat ist gültig)
- Erstzertifizierung erforderlich bei verspäteter Durchführung (Zertifikat ungültig)

5.4 Sonderaudits

Sonderaudits können je nach Anlass sowohl off-site als auch on-site durchgeführt werden. Die Entscheidung richtet sich nach der Art der zu untersuchenden Sachverhalte und der Verfügbarkeit elektronischer Nachweise. Es muss eine Mitteilung des Kunden erfolgen, die den veränderten Sachverhalt erläutert. Dann folgt eine Bewertung der neuen Situation. Möglicherweise kann diese Bewertung mit einem Überwachungsaudit kombiniert werden. Dem folgt eine Entscheidung, die eine Aktualisierung des Zertifikatsstatus erfordert.

5.4.1 Anlässe

- Kundenbeschwerden bezüglich zertifizierter Organisationen
- Größere Systemänderungen
- Hinweise auf schwerwiegende Abweichungen
- Behördliche Anforderungen
- Erweiterung oder Einschränkung des Geltungsbereichs

5.4.2 Transferaudits

Bei Übernahme von gültigen Zertifikaten anderer akkreditierter Stellen:

- Prüfung der Vollständigkeit aller Unterlagen
- Sicherstellung identischer Geltungsbereiche
- Keine offenen Hauptabweichungen
- Erstzertifizierung bei nicht erfüllten Voraussetzungen

Bei abgelaufenen Zertifikaten ist ein vollständiges Erstzertifizierungsaudit erforderlich.

5.5 Aussetzung, Wiederherstellung und Zurückziehung der Zertifizierung

5.5.1 Gründe für Aussetzung

- Versäumnisse der Überwachungsaudit-Fristen (> 3 Monate Verzögerung)
- Nicht fristgerechte Schließung von Hauptabweichungen
- Missbrauch des Zertifikats oder der Zeichen
- Verweigerung

Verfahrensweise:

Schriftliche Mitteilung an den Kunden mit Begründung, Fristsetzung zur Behebung (max. 6 Monate), Öffentliche Bekanntgabe der Aussetzung, Verbot der Zeichennutzung während der Aussetzung

5.5.2 Voraussetzungen für Wiederherstellung

- Behebung der Aussetzungsgründe innerhalb der Frist
- Nachweis der Konformität
- Ggf. Sonderaudit zur Verifizierung

Verfahrensweise:

Prüfung der Nachweise, Entscheidung über Wiederherstellung, Öffentliche Bekanntgabe, Fortführung des Zertifizierungszyklus

5.5.3 Gründe für Zurückziehung

- Nichtbehebung der Aussetzungsgründe innerhalb der Frist
- Schwerwiegende oder wiederholte Verstöße gegen Zertifizierungsanforderungen
- Fortgesetzter Missbrauch des Zertifikats
- Auflösung des zertifizierten Unternehmens
- Freiwillige Rückgabe durch den Kunden

Verfahrensweise:

Schriftliche Mitteilung mit Begründung, Öffentliche Bekanntgabe, Rückgabe aller Zertifizierungsdokumente, Sofortiges Verbot der Zeichennutzung, ggf. rechtliche Schritte bei weiterem Missbrauch

6. Besondere Szenarien

6.1 Multi-Site-Zertifizierungen

6.1.1 Voraussetzungen nach IAF MD 1

- Zentrale Steuerung aller Standorte
- Einheitliche Managementsysteme und Prozesse
- Interne Audits an allen Standorten
- Gemeinsame Managementbewertung

6.1.2 Stichprobenverfahren

Erstzertifizierung: - Stichprobengröße: $\sqrt{n}$ (aufgerundet) - Mindestens 25% zufällig ausgewählt

Überwachungsaudits: - Stichprobengröße: $0,6 \times \sqrt{n}$ (aufgerundet)

Re-Zertifizierung: - Stichprobengröße: $0,8 \times \sqrt{n}$ (bei bewährtem System)

6.1.3 Besonderheiten

- Zentrale wird immer auditiert
- Stichprobenauswahl liegt bei der AAA
- Auswahlkriterien: Ergebnisse interner Audits, Beschwerden, Standortgröße
- Strukturänderungen erfordern Anpassung der Stichprobe

6.2 Kombinierte Audits

Bei Zertifizierungsverfahren zu mehreren Managementsystemen wird zusätzlich geprüft:

- Integrierte Auditplanung zur Effizienzsteigerung
- Qualifizierte Auditoren für alle relevanten Bereiche
- Separate Bewertung jedes Standards

7. Unparteilichkeit und Vertraulichkeit

7.1 Unparteilichkeitsmanagement

7.1.1 Grundsätze

Die AAA verpflichtet sich zur strikten Wahrung der Unparteilichkeit durch:

- Identifikation, Bewertung und Behandlung von Interessenskonflikten
- Unabhängige Zertifizierungsentscheidungen
- Trennung von Beratungs- und Zertifizierungstätigkeiten

7.1.2 Präventive Maßnahmen

- Risikobasierte Überwachung aller Zertifizierungsprozesse
- Regelmäßige Überprüfung der Unparteilichkeit

- Verhaltenskodex für alle Mitarbeiter und Auditoren
- Beschwerdemechanismen für Interessenskonflikte

7.2 Vertraulichkeit und Datenschutz

7.2.1 Verpflichtungen

- Alle Personen die in die Zertifizierungstätigkeit einbezogen sind, sind zur Vertraulichkeit verpflichtet
- Datenschutzerklärung wird strikt eingehalten
- Informationssicherheit nach aktuellen Standards
- Zugriffsbeschränkungen auf need-to-know-Basis

7.2.2 Informationsmanagement

10-jährige Archivierung aller Zertifizierungsunterlagen

- Sichere Datenübertragung und -speicherung
- Regelmäßige Löschung nicht mehr benötigter Daten
- Audit-Trail für alle Zugriffe

8. Zeichennutzung

8.1 Berechtigungen

Nach erfolgreicher Zertifizierung dürfen Sie:

- Das AAA-Zertifizierungszeichen in Verbindung mit der Zertifikatnummer verwenden
- Auf die Zertifizierung hinweisen in Geschäftsdokumenten und Marketing – Das Zertifikat präsentieren in vollständiger Form

8.2 Einschränkungen

Nicht erlaubt ist:

- Verwendung der Zeichen bei ausgesetzter oder entzogener Zertifizierung
- Veränderung der Zeichen oder des Zertifikats
- Produktkennzeichnung mit Zertifizierungszeichen (außer bei Prozesszertifizierung)
- Irreführende Darstellung des Zertifizierungsumfangs

8.3 Zeichensatzung

Korrekte Verwendung:

- Zusammen mit Organisationsname und Zertifikatnummer
- Nur bei gültigem Zertifikat
- In der ursprünglichen Gestaltung
- Mit Bezug auf den zertifizierten Geltungsbereich

Detaillierte Regelungen finden Sie in unserer Zeichennutzungsregelung.

9. Beschwerden und Einsprüche

9.1 Beschwerdemanagement

9.1.1 Definition

Eine Beschwerde ist ein Ausdruck der Unzufriedenheit einer dritten Partei gegenüber:

- Einer zertifizierten Organisation
- Dem Vorgehen der AAA
- Dem Verhalten von Auditoren

9.1.2 Beschwerdeverfahren

- Entgegennahme und Bestätigung der Beschwerde in Textform
- Bewertung durch unabhängige Personen
- Untersuchung des Sachverhalts
- Maßnahmenentwicklung und -umsetzung
- Rückmeldung an den Beschwerdeführer
- Dokumentation und Trend-Analyse

9.2 Einspruchsverfahren

9.2.1 Definition

Ein Einspruch ist ein formaler Widerspruch gegen:

- Eine Zertifizierungsentscheidung
- Dem Auditergebnis
- Andere Entscheidungen der AAA

9.2.2 Einspruchsverfahren

- Entgegennahme und Bestätigung des Einspruchs in Textform innerhalb von 3 Wochen
- Prüfung durch unabhängiges Personal
- Bewertung aller relevanten Informationen
- Entscheidung über den Einspruch
- Mitteilung des Ergebnisses
- Umsetzung eventueller Korrekturmaßnahmen

9.2.3 Fristen

- Einspruchsfrist: 6 Wochen nach Zugang der Entscheidung
- Bearbeitungszeit: Angemessen je nach Komplexität
- Mitteilungszeit: Unverzüglich nach Entscheidung

10. Änderungsmanagement

10.1 Mitteilungspflichten des Kunden

Sie sind verpflichtet, uns unverzüglich zu informieren über:

10.1.1 Organisatorische Änderungen

- Änderung der Firmierung, Rechtsform oder Eigentümerschaft

- Veränderung von Schlüsselpositionen oder Fachpersonal
- Änderung von Kontaktadressen oder Standorten

10.1.2 System-bezogene Änderungen

- Änderungen im Geltungsbereich des Managementsystems
- Wesentliche Veränderungen in Kernprozessen
- Übernahme ausgelagerter Prozesse oder neue Outsourcing-Aktivitäten

10.1.3 Besondere Ereignisse

- Für ISO/IEC 27001: Sicherheitsvorfälle mit potenziellem Systembezug
- Rechtliche Änderungen mit Systembezug

10.2 Änderungen seitens der AAA

Wir informieren Sie unverzüglich über:

- Änderungen der Zertifizierungsregelungen
- Normüberarbeitungen mit Auswirkung auf Ihr Zertifikat
- Änderungen in der Akkreditierung - Modifikationen unserer Verfahren

10.3 Auswirkungen von Änderungen

Je nach Art der Änderung können folgende Maßnahmen erforderlich sein:

- Sonderaudit zur Bewertung der Auswirkungen
- Anpassung des Geltungsbereichs
- Zusätzliche Dokumentenprüfung
- Vorgezogenes Überwachungsaudit
- Aussetzung bei schwerwiegenden Änderungen ohne rechtzeitige Mitteilung

Kontaktinformationen

Advanced Audit and Analytics GmbH
Nägelsbachstraße 26
91052 Erlangen
Telefon: 0151/28900421
E-Mail: katrin.vogl@aaa.ms
Website: www.aaa-cert.org
Geschäftsführung: Larissa
Vogt

Dieser Leitfaden wird regelmäßig überprüft und bei Bedarf aktualisiert. Änderungen werden allen Kunden rechtzeitig mitgeteilt.

