Zertifizierungsleitfaden von Managementsystemen

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 Vertrauliche und sensible Informationen (ISO/IEC 27001)

Vor dem Zertifizierungsaudit ist 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. Ist ein angemessenes Audit ohne diese Informationen nicht möglich, kann das Zertifizierungsaudit erst stattfinden, wenn geeignete Zugangsregelungen vereinbart sind (ISO/IEC 27006-1, 8.4.2).

2.3 Antragsprüfung und Angebotserstellung

Nach Eingang Ihres Antrags prüfen wir:

2.3.1 Bewertungskriterien

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

2.3.2 Mögliche Entscheidungen

Annahme des Antrags:

- Erstellung eines individuellen Angebots

Ablehnung des Antrags bei:

- Mangelnder Vorbereitung oder mangelndem 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 Informationssicherheitsrisiken oder Qualitätsrisiken
- Fehlender Kooperationsbereitschaft

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

2.4 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

3. Der Weg zum Zertifikat – Überblick über den Ablauf

3.1 Auditplanung

3.1.1 Auditprogramm-Entwicklung

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

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

3.1.2 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.

3.1.3 Terminplanung

- Stufe 1-Audit: Dokumentenprüfung und Bereitschaftsbewertung
- Zeitabstand: Zwischen Stufe 1 und 2 liegen in der Regel mindestens 3 Wochen (bei geringem Korrekturaufwand verkürzbar) und höchstens 6 Monate; liegt Stufe 1 länger zurück, wird sie ganz oder teilweise wiederholt
- Stufe 2-Audit: Wirksamkeitsprüfung vor Ort

3.2 Audit-Durchführung

Die AAA führt Audits bevorzugt remote (off-site) durch, um Effizienz zu steigern, die Umwelt zu schonen und Kosten zu optimieren. Der Umfang der Remote-Tätigkeiten wird vor jedem Audit auf Basis einer dokumentierten Risikoanalyse festgelegt. Der Einsatz von IKT wird vorab mit Ihnen vereinbart, einschließlich der Regelungen zu Informationssicherheit und Datenschutz; kommt keine Einigung zustande, wird vor Ort auditiert. Dabei kommen elektronische Mittel nach ISO/IEC 17021-1, ISO/IEC 27006-1 und IAF MD 4 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 (Präsenz) erfolgen beim Stufe-2-Audit der Erstzertifizierung 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

3.2.1 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 wie Auditoren.

3.3 Stufe 1-Audit (Dokumentenprüfung)

3.3.1 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

3.3.2 Ergebnis

- Kurzbericht Audit Stufe 1 mit Problembereichen, die in Stufe 2 als Nichtkonformität eingestuft werden könnten
- Festgestellte Schwachstellen sind vor dem Stufe-2-Audit zu beheben

3.4 Stufe 2-Audit (Wirksamkeitsprüfung)

3.4.1 Ziele des Stufe 2-Audits

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

3.4.2 Durchführung

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

3.5 Abweichungsmanagement

3.5.1 Klassifizierung von Abweichungen

Wesentliche Nichtkonformität (NC 1):
- Beeinträchtigung der Managementsystemziele
- Systemversagen oder mehrere zusammenhängende untergeordnete Nichtkonformitäten

Untergeordnete Nichtkonformität (NC 2):
- Keine Beeinträchtigung der Systemziele
- Isolierte Einzelfälle

Verbesserungspotenziale können ausgewiesen werden. Sie sind für Sie nicht verpflichtend, enthalten keine Lösungsvorschläge und werden im Folgeaudit nicht verifiziert.

3.5.2 Behandlung von Abweichungen

- Mitteilung aller festgestellten Nichtkonformitäten beim Abschlussgespräch
- Fristen: Maßnahmenplan innerhalb von 30 Kalendertagen nach dem letzten Audittag; Umsetzungsnachweis für wesentliche Nichtkonformitäten innerhalb von 90 Kalendertagen (bei Re-Zertifizierung spätestens vor Ablauf des Zertifikats); bei hohem Informationssicherheitsrisiko kürzere Fristen; auf begründeten Antrag einmalige Verlängerung möglich
- Ursachenanalyse und Maßnahmenplanung durch Kunde
- Bewertung und Verifikation der Maßnahmen durch den Lead Auditor

Bei wesentlichen Nichtkonformitäten: Nachweis der erfolgreichen Umsetzung vor der Zertifizierungsentscheidung erforderlich
Bei untergeordneten Nichtkonformitäten: Bewertung und Annahme des Maßnahmenplans vor der Zertifizierungsentscheidung, Verifizierung der Umsetzung im nächsten Audit
Kann die Wirksamkeit der Maßnahmen zu wesentlichen Nichtkonformitäten nicht dokumentenbasiert nachgewiesen werden, ist ein Nachaudit erforderlich. Die Kosten trägt der Kunde.

3.6 Zertifizierungsentscheidung

3.6.1 Entscheidungsprozess

Die Zertifizierungsentscheidung (z. B. Erteilung, Ablehnung) trifft ein Zertifizierungsentscheider auf Basis vollständiger und schlüssiger Entscheidungsgrundlagen.
Es gilt das Trennungsprinzip: Der Zertifizierungsentscheider darf an dem zugrunde liegenden Audit nicht beteiligt gewesen sein.

3.6.2 Entscheidungsgrundlagen

- Vollständige Auditberichte
- Verifizierte Korrekturen und Korrekturmaßnahmen zu allen wesentlichen Nichtkonformitäten; akzeptierte Maßnahmenpläne zu allen untergeordneten Nichtkonformitäten
- Bewertung der Systemwirksamkeit
- Konformität mit allen Normanforderungen

3.6.3 Mögliche Entscheidungen

- Zertifikatserstellung bei vollständiger Konformität
- Erteilung bei untergeordneten Nichtkonformitäten, sofern der Maßnahmenplan bewertet und akzeptiert wurde; die Umsetzung wird im nächsten Audit verifiziert.
- Verweigerung der Zertifizierung bei:

- Nicht innerhalb von 6 Monaten nach dem letzten Tag des Stufe-2-Audits verifizierten Korrekturen zu wesentlichen Nichtkonformitäten; vor einer Zertifizierung ist dann eine erneute Stufe 2 erforderlich.
- Schwerwiegendem Systemversagen
- Unzureichender Systemwirksamkeit
- Mangelnder Kooperationsbereitschaft während des Audits

Bei Verweigerung:

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

3.7 Zertifikatsausstellung

3.7.1 Zertifikatsinhalte

- Organisationsname und -adresse
- Geltungsbereich der Zertifizierung
- Zugrunde liegende Norm einschließlich Ausgabestand
- Bei ISO/IEC 27001: Version der Erklärung zur Anwendbarkeit (SoA)
- Zertifikatnummer
- Ausstellungs- und Ablaufdatum
- Gültigkeitsdauer (3 Jahre)
- Standorte (bei Multi-Site-Zertifizierung im Anhang)
- Hinweis, wenn alle Tätigkeiten im Geltungsbereich ausschließlich remote erbracht werden

3.7.2 Eigentumsverhältnisse

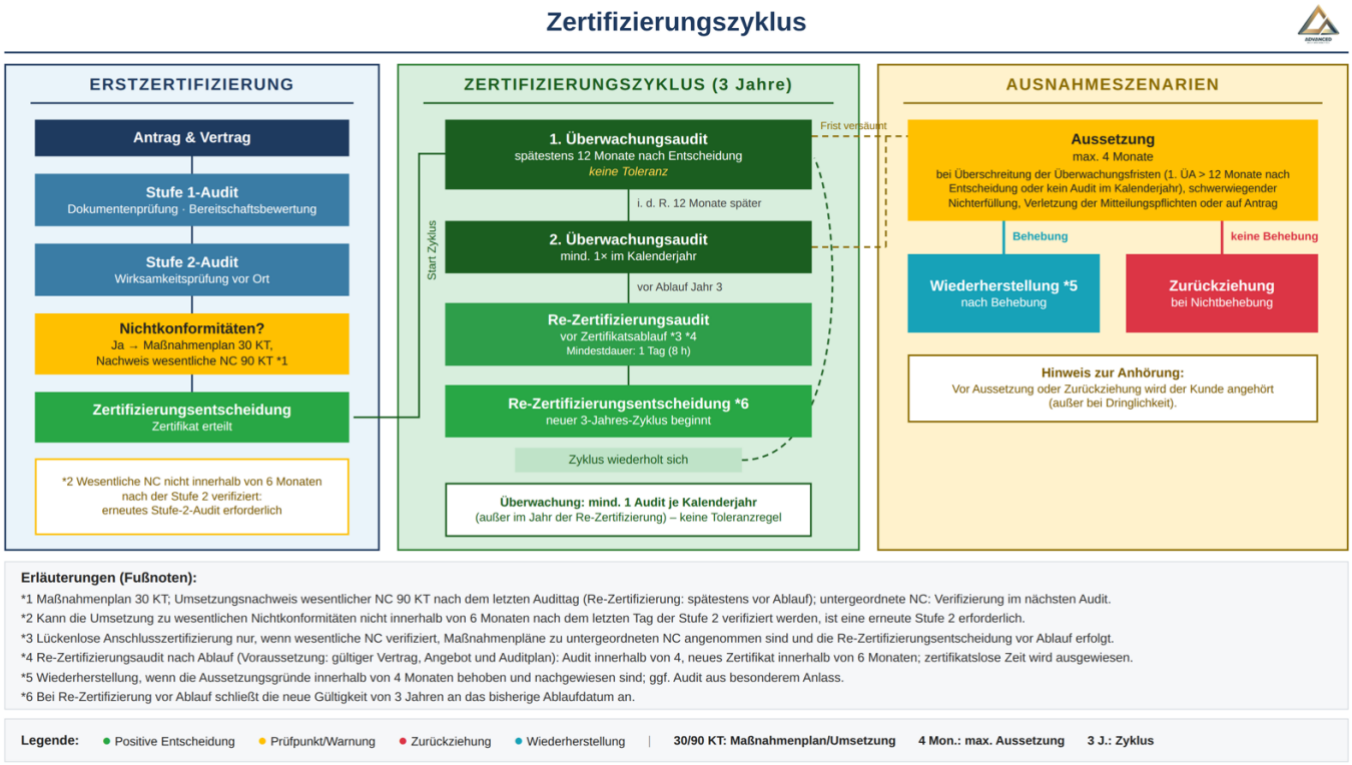
Zertifikate bleiben Eigentum der AAA.
Zertifikatskopien können auf Wunsch erstellt werden.

---

4. Der Zertifizierungszyklus

4.1 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)
Das Re-Zertifizierungsaudit muss vor Ablauf des Zertifikates mit der Re-Zertifizierungsentscheidung
abgeschlossen sein. Es beginnt ein neuer Zertifizierungszyklus mit der Planung des Auditprogramms.



4.2 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.

4.2.1 Zweck und Häufigkeit

- Erstes Überwachungsaudit: spätestens 12 Monate nach der Zertifizierungsentscheidung (ISO/IEC 17021-1:2015, 9.1.3.3) – hierfür besteht keine Toleranz
- Weitere Überwachungsaudits: mindestens einmal je Kalenderjahr (außer im Jahr der Re-Zertifizierung), in der Regel im Abstand von 12 Monaten; bei Nichteinhaltung wird die Zertifizierung ausgesetzt gemäß Kap. 4.5.1 (vgl. 3A-P2-VA_17021_Zertifizierungsprozess, Kap. 3.3.2.3)
- Aufrechterhaltung der Zertifikatsgültigkeit
- Kontinuierliche Überwachung der Systemkonformität

4.2.2 Auditumfang

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

4.3 Re-Zertifizierung

4.3.1 Zeitpunkt und Umfang

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

4.3.2 Besonderheiten

- Nahtlose Verlängerung bei rechtzeitiger Durchführung (Zertifikat ist gültig)
- Bei verspäteter Durchführung entsteht eine zertifikatslose Zeit: Das Audit muss spätestens 4 Monate, die Wiederherstellung spätestens 6 Monate nach Ablauf erfolgen; andernfalls ist eine neue Zertifizierung erforderlich.

4.4 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.

4.4.1 Anlässe

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

4.4.2 Transferaudits

Bei Übernahme von gültigen, nicht ausgesetzten oder zurückgezogenen Zertifikaten anderer Zertifizierungsstellen, die von einem IAF-MLA-Unterzeichner akkreditiert sind:

- Prüfung der Vollständigkeit aller Unterlagen
- Geltungsbereich innerhalb der Akkreditierungsbereiche beider Zertifizierungsstellen
- Verifizierung aller offenen wesentlichen Nichtkonformitäten vor der Zertifizierungsentscheidung
- Erstzertifizierung bei nicht erfüllten Voraussetzungen

Bei abgelaufenen Zertifikaten ist ein vollständiges Erstzertifizierungsaudit erforderlich.

4.5 Aussetzung, Wiederherstellung und Zurückziehung der Zertifizierung

4.5.1 Gründe für Aussetzung

- Versäumnisse der Überwachungsaudit-Fristen gemäß Kap. 4.2.1 (Überschreitung der zulässigen Frist)

- Nicht fristgerechte Schließung von wesentlichen Nichtkonformitäten
- Missbrauch des Zertifikats oder der Zeichen
- Verweigerung von Überwachungs- oder Re-Zertifizierungsaudits
- Dauerhafte oder schwerwiegende Nichterfüllung der Zertifizierungsanforderungen
- Verletzung der Mitteilungspflichten (Kap. 9.1)
- Freiwilliger Antrag des Kunden

Verfahrensweise:
Anhörung gemäß Kap. 4.5.4, schriftliche Mitteilung an den Kunden mit Begründung, Fristsetzung zur Behebung (bis innerhalb 4 Monate), Öffentliche Bekanntgabe der Aussetzung, Verbot der Zeichennutzung während der Aussetzung

4.5.2 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

4.5.3 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:
Anhörung gemäß Kap. 4.5.4, schriftliche Mitteilung mit Begründung, Öffentliche Bekanntgabe, Rückgabe aller Zertifizierungsdokumente, Sofortiges Verbot der Zeichennutzung, ggf. rechtliche Schritte bei weiterem Missbrauch

4.5.4 Anhörung

Vor einer Aussetzung oder Zurückziehung erhalten Sie Gelegenheit, innerhalb einer angemessenen Frist Stellung zu nehmen. In dringenden Fällen kann die Anhörung entfallen, insbesondere bei Missbrauch des Zertifikats oder der Zeichen oder wenn das Vertrauen in die Zertifizierung gefährdet ist. Ihre Stellungnahme können Sie dann im Rahmen des Einspruchsverfahrens (Kap. 8.2) einbringen.

5. Besondere Szenarien

5.1 Multi-Site-Zertifizierungen

5.1.1 Voraussetzungen nach IAF MD 1 und ISO/IEC 27006-1, 9.1.5.2

- Zentrale Steuerung aller Standorte

- Einheitliche Managementsysteme und Prozesse
- Interne Audits an allen Standorten
- Gemeinsame Managementbewertung

5.1.2 Stichprobenverfahren

Mindestanzahl der zu auditierenden Standorte je Audit (n = Gesamtzahl der Standorte; IAF MD 1, 6.1.3.3). Mindestens 25 % der Stichprobe werden zufällig ausgewählt (IAF MD 1, 6.1.2.2).
Erstzertifizierung: - Mindeststichprobe: $\sqrt{n}$ (aufgerundet)
Überwachungsaudits: - Mindeststichprobe: $0{,}6 \times \sqrt{n}$ (aufgerundet)
Re-Zertifizierung: - Mindeststichprobe: $\sqrt{n}$ (aufgerundet); hat sich das Managementsystem über den Zertifizierungszyklus als wirksam erwiesen, kann sie auf $0{,}8 \times \sqrt{n}$ (aufgerundet) reduziert werden

5.1.3 Besonderheiten

- Zentrale wird bei jedem Erst- und Re-Zertifizierungsaudit sowie mindestens jährlich auditiert
- Stichprobenauswahl liegt bei der AAA
- Risikobasierte Auswahl u. a. nach Audit- und NC-Ergebnissen, Größe, Komplexität und Tätigkeiten, Zeit seit dem letzten Audit sowie Beschwerden und Informationssicherheitsvorfällen
- Strukturänderungen oder neue Standorte führen zur Überprüfung der Stichprobe (IAF MD 1, 6.1.3.7, 6.1.4)
- Standorte mit signifikanten Risiken werden vor der Zertifizierung auditiert; bei erhöhtem Risiko wird die Stichprobe vergrößert.
- Liegt zum Zeitpunkt der Zertifizierungsentscheidung an einem Standort eine wesentliche Nichtkonformität vor, wird die Zertifizierung der gesamten Organisation bis zur Umsetzung angemessener Korrekturmaßnahmen verweigert; ein Ausschluss des betroffenen Standorts aus dem Geltungsbereich ist nicht zulässig (IAF MD 1, 7.7.3, 7.7.4).
- Ist ein Stichprobenverfahren nicht geeignet, werden bei Erst- und Re-Zertifizierung alle Standorte und in der Überwachung je Kalenderjahr mindestens 30 % der Standorte (aufgerundet) auditiert; die Zentrale ist bei jedem Audit einbezogen (IAF MD 1, 6.2.1).

5.1.4 Kombinierte Audits

Bei Zertifizierungsverfahren zu mehreren Managementsystemen wird zusätzlich geprüft:

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

6. Unparteilichkeit und Vertraulichkeit

6.1 Unparteilichkeitsmanagement

6.1.1 Grundsätze

Die AAA verpflichtet sich zur strikten Wahrung der Unparteilichkeit durch:

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

6.1.2 Präventive Maßnahmen

- Risikobasierte Überwachung aller Zertifizierungsprozesse
- Regelmäßige Überprüfung der Unparteilichkeit
- Verhaltenskodex für alle Mitarbeiter und Auditoren
- Beschwerdemechanismen für Interessenskonflikte

6.2 Vertraulichkeit und Datenschutz

6.2.1 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

6.2.2 Informationsmanagement

10-jährige Archivierung aller Zertifizierungsunterlagen

- Sichere Datenübertragung und -speicherung
- Regelmäßige Löschung nicht mehr benötigter Daten

7. Zeichennutzung

Nach erfolgreicher Zertifizierung dürfen Sie das AAA-Zertifizierungszeichen verwenden und auf Ihre Zertifizierung hinweisen. Voraussetzungen, Art und Umfang der Nutzung, Einschränkungen sowie Ihre Pflichten bei Aussetzung, Einschränkung, Zurückziehung oder Ablauf der Zertifizierung regelt die Zeichennutzungsregelung (FO-3A-P2_Zeichennutzungsregelung) in der jeweils gültigen Fassung.

8. Beschwerden und Einsprüche

Beschwerden und Einsprüche können über das Formular auf www.aaa-cert.org oder per E-Mail an beschwerde@aaa.ms bzw. einspruch@aaa.ms eingereicht werden.

8.1 Beschwerdemanagement

8.1.1 Definition

Eine Beschwerde ist ein Ausdruck der Unzufriedenheit einer Person oder Organisation (kein Einspruch) gegenüber:
- Einer zertifizierten Organisation
- Dem Vorgehen der AAA
- Dem Verhalten von Auditoren

8.1.2 Beschwerdeverfahren

- Entgegennahme und Bestätigung der Beschwerde in Textform (soweit möglich, z. B. nicht bei anonymen Beschwerden)
- Bewertung durch unabhängige Personen
- Untersuchung des Sachverhalts
- Begründete Beschwerden über eine zertifizierte Organisation werden dieser zeitnah mitgeteilt; ggf. erfolgt ein Audit aus besonderem Anlass
- Maßnahmenentwicklung und -umsetzung
- Fortschrittsberichte und förmliche Abschlussmitteilung an den Beschwerdeführer
- Dokumentation und Trend-Analyse

8.2 Einspruchsverfahren

8.2.1 Definition

Ein Einspruch ist ein formaler Widerspruch gegen:
- Eine Zertifizierungsentscheidung
- Andere Entscheidungen der AAA

Meinungsverschiedenheiten zu Auditfeststellungen werden im Abschlussgespräch erörtert; ungelöste Punkte können Sie in Textform an die Zertifizierungsstelle richten.

8.2.2 Einspruchsverfahren

- Entgegennahme und Bestätigung des Einspruchs in Textform
- Prüfung durch Personen, die weder am Audit noch an der Zertifizierungsentscheidung beteiligt waren
- Bewertung aller relevanten Informationen
- Entscheidung über den Einspruch
- Fortschrittsberichte und Mitteilung des Ergebnisses
- Umsetzung eventueller Korrekturmaßnahmen
- Förmliche Mitteilung über den Abschluss des Verfahrens

8.2.3 Fristen

- Einspruchsfrist: 30 Tage nach Bekanntgabe der Entscheidung
- Bearbeitungszeit: Angemessen je nach Komplexität
- Mitteilungszeit: Unverzüglich nach Entscheidung

9. Änderungsmanagement

9.1 Mitteilungspflichten des Kunden

Sie sind verpflichtet, uns unverzüglich zu informieren über:

9.1.1 Organisatorische Änderungen

- Änderung der Firmierung, Rechtsform oder Eigentümerschaft
- Veränderung von Schlüsselpositionen oder Fachpersonal
- Änderung von Kontaktadressen oder Standorten

9.1.2 System-bezogene Änderungen

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

9.1.3 Besondere Ereignisse

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

9.2 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

9.3 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
E-Mail: support@aaa-cert.org
Website: www.aaa-cert.org
Geschäftsführung: Larissa Vogt

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