VERTRAGSDOKUMENT

1. Allgemeines

Das zu zertifizierende Unternehmen (im Nachfolgenden Kunde genannt) muss über ein implementiertes und dokumentiertes Managementsystem (z.B. QMS, UMS etc.) verfügen und dies der IFU-CERT Zertifizierungsgesellschaft für Managementsysteme mbH (im Nachfolgenden IFU-CERT genannt) nachweisen. Das jeweilige Managementsystem muss die Anforderungen der jeweils anzuwendenden Normen oder anderen normativen Dokumenten über Managementsysteme sowie der gültigen und für das Unternehmen zutreffenden rechtlichen Bestimmungen stets erfüllen.

Im vorliegenden Dokument werden die Abläufe und Regeln innerhalb des Zertifizierungs-, Überwachungs- und Re-Zertifizierungsverfahrens („Auditprogramm“) sowie die Erteilung, Erhaltung, Erneuerung, Erweiterung, Einschränkung, Aussetzung, und Annullierung des Zertifikats in Anlehnung an die gültigen internationalen anwendbaren Normen und Regeln für die akkreditierten Zertifizierungsstellen für Managementsystemen einschließlich ISO/IEC 17021-1:2015 beschrieben.

Für die Zertifizierungsverfahren der Energiemanagementsysteme nach DIN EN ISO 50001:2018 werden die zusätzlichen Anforderungen der DIN EN ISO 50003:2014 umgesetzt.

Für die Zertifizierungsverfahren der Informationssicherheitsmanagementsysteme (ISMS) nach DIN EN ISO/IEC 27001:2017 werden die zusätzlichen Regeln der ISO/IEC 27006:2015_Amd1:2020 berücksichtigt.

Für die Zertifizierungsverfahren nach IT-Sicherheitskatalog gemäß § 11 Abs. 1a und 1b Energiewirtschaftsgesetz werden die zusätzlichen Anforderungen für die Zertifizierungsstellen, gemäß ISO/IEC 27006:2015_Amd1:2020 und gemäß Konformitätsbewertungsprogramme der Bundesnetzagentur, berücksichtigt.

Für die Zertifizierungsverfahren der Managementsysteme für Sicherheit und Gesundheit bei der Arbeit **nach BS OHSAS 18001 oder nach DIN ISO 45001:2018** werden die zusätzlichen Anforderungen der IAF MD 22:2019 berücksichtigt.

2. Antrag, Antragsprüfung, Auditprogramm und Angebots-Erstellung

Vor einer Verpflichtung zur Durchführung eines Zertifizierungsverfahrens muss die Zertifizierungsstelle ausreichende Informationen über die antragstellende, zu zertifizierende Organisation einholen. Diese Informationen werden im „Erhebungsbogen“ erfasst und von einem bevollmächtigten Vertreter der antragstellenden Organisation bestätigt.

Bei Übernahme von Zertifikaten bzw. Re-Zertifizierungen werden das gültige Zertifikat sowie

die Auditberichte der letzten drei Jahre einschließlich der Nachweise aller abgeschlossenen Korrekturmaßnahmen der Zertifizierungsstelle zur Prüfung nach Anforderungen der IAF MD:2 / 2017 zur Verfügung gestellt.

Anschließend entscheidet die Zertifizierungsstelle, ob die Bereitstellung der Zertifizierung z. B. im Hinblick auf die Unparteilichkeit, der Kompetenzen etc. möglich ist. Dann wird der Auditumfang ermittelt und das Auditprogramm erstellt. Wenn die Bereitstellung der Zertifizierung nicht möglich ist, erhält der Kunde eine schriftliche Begründung.

Der Zeitaufwand für die Auditierung errechnet sich z. B. unter Berücksichtigung:

- der Anzahl der Mitarbeiter,
- der Anzahl und Größe der Standorte sowie deren geografische Lage,
- dem Reifegrad des Managementsystems,
- der Spannbreite und Komplexität der Tätigkeiten und der Unternehmensstruktur (Organisation des Unternehmens, Forschungstätigkeit, Technologie, Außenstandorte, zeitweilige Standorte, Schichtbetrieb, Teilzeittätigkeit, Produktionslinien etc.),
- der Ausgliederung von Aktivitäten, Outsourcing
- der Ergebnisse vorangegangener Audits,
- der Risiken (Qualitätsrisiken, Umweltrisiken, Arbeitsschutz-Risiken, Informationssicherheitsrisiken)
- der Energiekomplexität (bei Energiemanagementsystemen errechnet aus den Angaben von: jährlichem Energieverbrauch, Anzahl von Energiequellen – die Organisation darf keine Energiequellen ausschließen –, Anzahl der wesentlichen Energieeinsätze)
- der Einsatz von Dolmetschern und Übersetzern: dies kann ggf. eine Verlängerung des Zeitaufwandes erfordern
- der Grad der Integration bei integrierten Managementsystemen wird bei der Erstellung des Auditprogramms für ein integriertes Audit berücksichtigt.
- Die Zeiten für das Auditieren eines Integrierten Managementsystems, basierend auf dem angegebenen Integrationsgrad des Managementsystems der Organisation im Erhebungsbogen, Änderungen unterliegen können, und zwar auf Grundlage des bestätigten Integrationsgrades beim Stufe 1- Audit sowie bei nachfolgenden Audits.

Für den gesamten Zertifizierungszyklus wird ein Auditprogramm entwickelt. Das Auditprogramm für die erstmalige Zertifizierung gemäß ISO/IEC 17021-1:2015 besteht aus:

- Zweistufigem Erst-Zertifizierungsaudit

- Überwachungsaudits im ersten und zweiten Jahr nach der Zertifizierungsentscheidung. Das erste Überwachungsaudit nach der Erst-Zertifizierung muss innerhalb von 12 Monaten stattfinden
- Überwachungsaudits mindestens einmal je Kalenderjahr mit Ausnahme der Jahre, in denen ein Re-Zertifizierungsaudit durchgeführt wird
- Re-Zertifizierungsaudit im dritten Jahr; vor Ablauf der Zertifizierung (rechtzeitig, damit genügend Zeit für Korrekturmaßnahmen und Zertifizierungsentscheidung bleibt)

Der erste dreijährige Zyklus der Zertifizierung beginnt mit der Entscheidung über die Zertifizierung. Nachfolgende Zyklen beginnen mit der Re-Zertifizierungsentscheidung.

Die Festlegung von Auditprogrammen sowie alle folgenden Anpassungen berücksichtigen

- die Größe der Organisation des Kunden,
- den Geltungsbereich,
- die Komplexität des Managementsystems,
- Schichtarbeit und die Tätigkeiten, die in den Schichten ausgeführt werden,
- die Ergebnisse früherer Audits,
- das Niveau der Wirksamkeit des Managementsystems,

Zusätzliche Aspekte, die bei der Entwicklung oder Überarbeitung eines Audtiprogramms betrachtet und bei der Ermittlung des Auditumfangs berücksichtigt werden können, sind:

- Bei der Zertifizierungsstelle eingegangene Beschwerden über den Kunden
- Kombinierte/integrierte/gemeinschaftliche Audits
- Änderungen der Zertifizierungsanforderungen
- Änderungen der rechtlichen Anforderungen
- Änderungen der Akkreditierungsanforderungen
- Daten zur Leistungsfähigkeit der Organisation (z. B. Fehlerraten)
- Bedenken der relevanten interessierten Parteien

Die Kalkulation des Auditzeitaufwands und die Erstellung des Auditprogramms können jedoch später aufgrund der zusätzlich im Vorortbesuch, z. B. im Stufe 1–Audit, gewonnenen Erkenntnisse oder aufgrund der Änderungen im Unternehmen sowie jeder Zeit bei Änderungen der Akkreditierungsregeln noch Anpassungen erfahren.

Der Auditumfang und das Auditprogramm, die Zertifizierungsgebühren, die Zertifizierungsbedingungen sowie alle anderen relevanten Informationen oder Verweise darauf werden dem Kunden zusammen mit dem Angebot zur Verfügung gestellt.

3. Zertifizierungsvertrag

Ein rechtsverbindlich unterschriebener Zertifizierungsvertrag muss IFU-CERT vorliegen, bevor mit dem Zertifizierungsverfahren begonnen werden kann. Ein unterschriebener Zertifizierungsvertrag setzt Folgendes voraus:

- die Anerkennung der Allgemeinen Vertragsbedingungen
- die Anerkennung der Zertifizierungsverfahren: die Zertifizierungsanforderungen sind eindeutig festgelegt, dokumentiert und verstanden worden,
- jegliche Unterschiede in den Auffassungen zwischen dem Kunden und IFU-CERT sind ausgeräumt,
- IFU-CERT ist in der Lage, die Zertifizierungsleistung im Hinblick auf den Geltungsbereich der Zertifizierung, den (die) Standort(e) des Kunden und die zu verwendende Sprache etc. zu erbringen.

4. Vorbereitung der Auditierung

Vor der Auditierung werden gemeinsam mit dem Kunden die weitere Vorgehensweise besprochen, die Termine abgestimmt und die entsprechenden Ansprechpartner benannt.

IFU-CERT stellt ein geeignetes Auditteam zusammen. Dieses Team führt die Auditierung im Namen von IFU-CERT durch. Gegebenenfalls können auch Fachexperten aus dem zu auditierenden Fachgebiet das Auditteam beratend ergänzen. Das Auditteam wird formal benannt und mit den erforderlichen Informationen ausgestattet. Der Kunde hat das Recht, benannte Auditoren und Fachexperten im Vorfeld der Auditierung abzulehnen (siehe auch "Allgemeine Rechte und Pflichten des Zertifikatsinhabers")

5. Das Auditprogramm, Auditierung und Auditbericht

5.1 Zweistufiges Erstzertifizierungsaudit

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

5.1.1 Stufe 1

Hauptziel des Audits der Stufe 1 ist die Ermittlung der Bereitschaft für das Audit der Stufe 2. Das Audit der Stufe 1 hat folgende Einzelziele:

- die dokumentierten Informationen zum Managementsystem des Kunden zu bewerten. Diese Dokumente müssen IFU-CERT vier Wochen vor dem Audit

Stufe 1 möglichst in digitaler Form zur Verfügung stehen,

- für ISMS-Zertifizierungen und für die Zertifizierungen nach IT Sicherheitskatalog: Prüfung der internen Berichte und der sonstigen Berichte zur Informationssicherheit. Den Auditoren muss der Zugang zu den Berichten der internen Audits sowie zu den Berichten der unabhängigen Bewertungen der Informationssicherheit gewährleistet werden.
- den Standort und die standortspezifischen Bedingungen des Kunden zu beurteilen,
- Gespräche mit den Mitarbeitern der Organisation zu führen, um zu ermitteln, ob der Kunde auf das Audit Stufe 2 vorbereitet ist
- den Vorbereitungsstand sowie das Verständnis der Anforderungen der Norm zu beurteilen,
- den Integrationsgrad des Integrierten Managementsystems im Vergleich zu den Informationen im Erhebungsbogen zu überprüfen
- notwendige Informationen zu erlangen bezüglich des Anwendungsbereichs des Managementsystems, einschließlich:
  - Standorte des Kunden
  - Prozesse und eingesetzte Arbeitsmittel
  - Festgelegte Lenkungsebenen (insbesondere bei Kunden mit mehreren Standorten)
  - Anzuwendende gesetzliche und behördliche Anforderungen
- **für ISMS**-Audits: Prüfung, ob der gewünschte Geltungsbereich der ISMS – Zertifizierung mit der Erklärung zur Anwendbarkeit (Statement of Applicability) übereinstimmt. Hinweis: Die Zertifizierung von Teilbereichen, von unselbständigen, serviceorientierten Teile einer Organisation, nach ISO 27001 ist nicht möglich.
- **Für Audits nach IT-Sicherheitskatalog nach § 11 Abs. 1a und 1b Energiewirtschaftsgesetz:** Prüfung der Vollständigkeit der Erklärung zur Anwendbarkeit (Übersicht über die in der Geltungsbereich des IT-Sicherheitskatalogs betroffenen Anwendungen, Systeme und Komponenten, die für einen sicheren Netzbetrieb oder Anlagenbetrieb notwendig sind, mit den anzutreffenden Haupttechnologien und deren Verbindungen einschließlich Schnittstellen zu Teilsystemen); Prüfung ob alle verbindliche Maßnahmen gemäß Anhang A DIN EN ISO/IEC 27001:2017, erweitert nach DIN ISO/IEC 27002:2017 und nach DIN ISO 27019:2020 für die Besonderheiten im Bereich der Prozesssteue-

rung der Energieversorgung definiert worden sind.

- **für EnMS**-Audits: Prüfung und Bestätigung der Angemessenheit des Anwendungsbereichs und der Grenzen des EnMS (bei jedem Audit!); Bei der Festlegung der Grenzen darf die Organisation keine Energiequellen ausschließen; Der Geltungsbereich des Energiemanagementsystems muss nach ISO 50001 / 50003 *alle verbrauchten Energiemengen des Unternehmens umfassen;* Überprüfung der Beschreibung der Einrichtungen, Ausrüstung, Systeme und Prozesse der Organisation für den identifizierten Anwendungsbereich und die Grenzen des EnMS; Bestätigung der Anzahl des EnMS-wirksamen Personals, der Energiequellen, der wesentlichen Energieeinsätze und des tatsächlichen Energieverbrauchs, um die Auditdauer zu bestätigen; Ergebnisse des Energieplanungsprozesses; Möglichkeiten zur Verbesserung der energiebezogenen Leistung, Ziele, Aktionspläne.
- die Zuteilung der Ressourcen für Audits der Stufe 2 zu bewerten sowie die Einzelheiten der Audits der Stufe 2 mit dem Kunden abzustimmen,
- durch ausreichendes Verständnis des Managementsystems des Kunden einen Schwerpunkt für die Planung des Audits Stufe 2 zu schaffen,
- zu beurteilen, ob die internen Audits und Managementbewertungen geplant und durchgeführt worden sind. Eine Voraussetzung für die Zertifizierung ist, dass alle internen Audits und die Managementbewertung durchgeführt wurden.

Um diese Ziele zu erreichen, werden mindestens Teile des Audits der Stufe 1 auf dem Betriebsgelände des Kunden gemäß mit dem Kunden vorher abgestimmten Auditplan durchgeführt.

Die Auditfeststellungen der Stufe 1 werden dem Kunden mitgeteilt, einschließlich der identifizierten Schwachstellen, die während des Audits der Stufe 2 als Nichtkonformität eingestuft werden könnten. Die Korrekturmaßnahmen müssen nachweisbar durchgeführt sein, bevor die Auditfreigabe für das Stufe- 2- Audit erteilt wird.

Treten bedeutende Änderungen auf, die das Managementsystem beeinflussen würden, muss die Zertifizierungsstelle die Notwendigkeit in Betracht ziehen, die gesamte Stufe 1 oder Teile von Stufe 1 zu wiederholen. Der Kunde wird informiert, ob die Ergebnisse von Stufe 1 zu einer Verschiebung oder zu einer Stornierung von Stufe 2 führen können.

Bei der Ermittlung des Abstands zwischen Stufe 1 und Stufe 2 werden die Erfordernisse des Kunden berücksichtigt, um Lösungen zu den evtl. vorhandenen Schwachstellen zu finden.

5.1.2 Stufe 2

Ziel des Audits der Stufe 2 ist es, die Umsetzung einschließlich der Wirksamkeit des Managementsystems des Kunden zu beurteilen. Das Audit der Stufe 2 findet an dem/den Standort/en des Kunden statt.

Die Auditierung umfasst mindestens:

- Informationen und Nachweise über die Konformität mit allen Anforderungen
- Überwachung der Leistung, Messung, Berichterstattung und Überprüfung in Bezug auf Ziele und Vorgaben für die Schlüsselleistungen
- Die Fähigkeit und Leistungsfähigkeit des Managementsystems des Kunden im Hinblick auf die Erfüllung geltender gesetzlicher, behördlicher und vertraglicher Anforderungen
- Operative Lenkung der Prozesse des Kunden
- Internes Auditieren und Managementbewertung
- Verantwortlichkeit der Leitung für die Politiken des Kunden
- Überwachung, Messung, Analyse und Verbesserungsprozesse

Am Audittag werden im Einführungsgespräch die Vorgehensweise, die Ziele etc. erörtert. Der Geltungsbereich der Zertifizierung wird im Eröffnungsgespräch nochmals bestätigt. Eine eventuelle Änderung des Geltungsbereichs muss mit der Zertifizierungsstelle abgestimmt werden und während des Audits der Geschäftsstelle angezeigt werden, um die Auditzeiten evtl. anpassen zu können. Nach dem abgeschlossenen Audit sind keine Änderungen des Geltungsbereichs mehr möglich.

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, gesetzlichen / behördlichen und sonstigen Anforderungen entspricht. Dies erfolgt durch:

- Begehungen,
- Interviews, Befragungen,
- Beobachtung von Prozessen und Tätigkeiten,
- Auswertung von Dokumenten und Aufzeichnungen.

Für die Durchführung des Audits vor Ort stellt der Kunde einen geeigneten Besprechungsraum und er ermöglicht die zügige Begehung des Unternehmens und aller rele-

vanten Betriebsbereiche und -einrichtungen. Er stellt sicher, dass alle im Auditplan genannten Organisationseinheiten und Mitarbeiter am Tag der Begehung mit ausreichend Zeit zur Verfügung stehen und dass alle relevanten Unterlagen zur Einsichtnahme vorliegen.

Am Ende des Audits findet eine offizielle Abschlussbesprechung mit dem Management des Kunden und ggf. mit den Personen, die die Verantwortung für die zu auditierenden Funktionen oder Prozesse tragen statt.

Im Rahmen einer Zertifizierung von **Managementsystemen *für Sicherheit und Gesundheit bei der Arbeit (SGA) nach BS OHSAS 18001 oder DIN ISO 45001*** ist die Anwesenheit des rechtlich für die SGA zuständige Führungspersonals, das für die Kontrolle der Mitarbeitergesundheit zuständige Personals und die Arbeitnehmervertreter mit Zuständigkeit für die SGA gemäß IAF MD 22 ist Pflicht. Die Begründung im Fall von Abwesenheit muss dokumentiert werden.

Die Anwesenheit bei dieser Abschlussbesprechung wird aufgezeichnet. Die Ergebnisse und die aus dem Audit gezogenen Schlussfolgerungen einschließlich der Empfehlung hinsichtlich der Zertifizierung werden vorgestellt. Die Prozesse der Zertifizierungsstelle für die Behandlung von Nichtkonformitäten/Abweichungen werden mit dem Kunden erörtert und ein Zeitrahmen für die Bearbeitung vereinbart.

Das Auditteam wird den Kunden bei einer Nichtkonformität (Abweichung) darüber informieren, ob die vorzunehmenden Korrekturmaßnahmen durch Einreichung von Nachweisdokumenten oder nach Bedarf vor Ort in einem Nachaudit verifiziert werden. Der Kunde muss bei jeder wesentlichen Nichtkonformität/Abweichung eine Ursachenanalyse durchführen und die spezifischen durchgeführten Korrekturen und Korrekturmaßnahmen nachweisen.

Eine wesentliche Nichtkonformität des Energiemanagementsystems ist, wenn eine fortlaufende Verbesserung der energiebezogenen Leistung nicht erreicht wurde. Für die Erteilung der Erstzertifizierung oder für die Re-Zertifizierung ist das nachweisbare Erreichen der fortlaufenden Verbesserung des Energiemanagementsystems und der energiebezogenen Leistung erforderlich.

Zu den geringfügigen Nichtkonformitäten (geringfügigen Abweichungen) legt der Kunde Maßnahmen fest. Die Umsetzung wird im nächsten Audit verifiziert.

Zur Ergebnisdokumentation wird ein zusammenfassender Auditbericht erstellt, der die Erfüllung der Forderungen der entsprechenden Normen wiedergibt und positive Auditfeststellungen sowie zu beseitigende Nichtkonformitäten (Abweichungen) enthält.

Wenn die Nachweise zur Umsetzung der Korrekturen und Korrekturmaßnahmen jeglicher wesentlicher Nichtkonformität (Abweichung) innerhalb von 6 Monaten nach Ablauf der Zertifizierung nicht vorgelegt werden können, muss mindestens die Stufe 2-Audit

durchgeführt werden.

Nach positivem Auditergebnis und nach der Behebung aller Nichtkonformitäten (Abweichungen) im festgelegten Zeitraum empfiehlt das Auditteam die Zertifikatserteilung.

Nach Durchführung der festgelegten Verfahren der Zertifizierungsstelle zur Zertifizierungsentscheidung erfolgt die Freigabe zur Erstellung des Zertifikats. Die Zertifikate werden als Entwurf dem Kunden zur Korrektur vorgelegt. Die Zertifizierungsurkunde wird dem Kunden per Post und als PDF-Datei und das Zertifizierungszeichen (Logo) per Email zugesandt.

5.2 Überwachungstätigkeiten – Aufrechterhaltung der Zertifizierung

Das zertifizierte Unternehmen unterliegt hinsichtlich der anhaltenden Normerfüllung der Überwachungstätigkeiten durch IFU-CERT. Diese enthalten die Vor-Ort-Auditierung des Managementsystems sowie weitere Überwachungstätigkeiten wie zum Beispiel:

- Anfragen der Zertifizierungsstelle an den zertifizierten Kunden zu Aspekten der Zertifizierung
- Bewertung der Angaben des zertifizierten Kunden im Hinblick auf seine Tätigkeiten (Werbematerial, Webseiten)
- Aufforderungen an den zertifizierten Kunden zur Bereitstellung von dokumentierten Informationen
- Andere Mittel zur Überwachung der Leistungsfähigkeit des zertifizierten Kunden

Überwachungsaudits müssen mindestens einmal je Kalenderjahr durchgeführt werden, mit Ausnahme der Jahre, in denen ein Re-Zertifizierungsaudit stattfindet. Das Datum des ersten Überwachungsaudits, das der Erstzertifizierung folgt, muss innerhalb 12 Monate nach der Zertifizierungsentscheidung liegen. Der Auditumfang eines Überwachungsaudits hängt von der Komplexität des Unternehmens ab; muss aber gemäß IAF MD 5:2019 mindestens 1 Audittag vor Ort umfassen.

Die Überwachungsaudits, die jährlich stattfinden sind Vor-Ort-Audits, stellen aber nicht notwendigerweise vollständige Systemaudits dar. Sie umfassen aber mindestens die Bereiche, die genügend Nachweise über die Aufrechterhaltung und Weiterentwicklung des Managementsystems liefern:

- Interne Audits, Managementbewertung
- Maßnahmen zu den Nichtkonformitäten und zu den weiteren Feststellungen der vorhergehenden Audits
- Behandlung von Beschwerden
- Erreichen der Ziele, ständige Verbesserung (EnMS: kontinuierliche Verbesse-

rung der energiebezogenen Leistung) nachweisen

- anhaltende Betriebssteuerung/-lenkung
- Bewertung von Änderungen
- Nutzung von Zertifizierungszeichen und anderen Verweisen auf die Zertifizierung

Bei Bedarf (z.B. wegen Änderungen der Komplexität der Prozesse etc.) wird der Umfang der Überwachung neu festgelegt und dem Kunden mitgeteilt. Zu diesem Zweck erfolgt eine jährliche Abfrage der Unternehmensdaten zum Audit durch den beauftragten Auditleiter. Der Auditleiter meldet evtl. Änderungen der Zertifizierungsstelle, um den Auditaufwand evtl. anzupassen. Wenn nicht mitgeteilte Änderungen vom Auditteam vor Ort festgestellt werden, müssen diese der Zertifizierungsstelle sofort gemeldet werden. Die Auditzeiten werden entsprechend angepasst.

IFU-CERT kann jederzeit eine Überwachung anordnen, wenn dies begründet erscheint; zum Beispiel bei wesentlichen Änderungen oder Beschwerden.

Der Ablauf eines Überwachungsaudits gemäß dem abgestimmten Auditplan ist wie oben beschrieben. Der Kunde muss bei jeder wesentlichen Nichtkonformität/Abweichung eine Ursachenanalyse durchführen und die spezifischen durchgeführten Korrekturen und Korrekturmaßnahmen nachweisen. Zu den geringfügigen Abweichungen legt der Kunde Maßnahmen fest. Die Umsetzung wird im nächsten Audit verifiziert.

5.3 Audits aus besonderem Anlass gem. ISO/IEC 17021-1:2015

5.3.1 Erweiterung des Geltungsbereichs:

Als Konsequenz auf eine beantragte Erweiterung des Geltungsbereichs – Aufnahme neuer Prozesse oder Standorte – einer schon erteilten Zertifizierung muss die Zertifizierungsstelle 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.

5.3.2 Kurzfristig angekündigte Audits

Es kann für die Zertifizierungsstelle erforderlich sein, kurzfristig angekündigte Audits oder auch unangekündigte Audits bei den zertifizierten Kunden durchzuführen,

- um Beschwerden zu untersuchen, um die mögliche Aufrechterhaltung der Zertifizierung prüfen/bestätigen zu können
- als Konsequenz von Änderungen, die das Managementsystem be-

einträchtigen können, um die Aufrechterhaltung der Zertifizierung prüfen/bestätigen zu können

- gemeldete Informationssicherheitsvorfälle zu untersuchen
- wenn ein schwerer Vorfall (Unfall oder schwerer Verstoß gegen gesetzlichen Vorschriften) passiert, um zu untersuchen, ob das Sicherheits- und Gesundheitsmanagementsystem nach BS OHSAS 18001 oder DIN ISO 45001 effektiv funktioniert. Ergebnisse der Untersuchung werden dokumentiert.
- als Konsequenz auf ausgesetzte Kundenzertifizierungen, um eine Neubewertung des Managementsystems und die Rückgabe der Zertifizierung zu ermöglichen.

5.4 Re-Zertifizierungsaudits

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

Das Re-Zertifizierungsaudit muss sämtliche wesentlichen Veränderungen bei Einrichtungen, Ausrüstung, Systemen oder Prozessen mit einbeziehen.

Bei signifikanten Änderungen für das Managementsystem (z.B. gesetzliche oder betrieblichen Änderungen) kann auch bei einer Re-Zertifizierung ein Audit der Stufe 1 erforderlich werden.

Für die Ausstellung der EnMS-Re-Zertifizierung ist der Nachweis der fortlaufenden Verbesserung der energiebezogenen Leistung erforderlich.

Das Re-Zertifizierungsaudit muss vor dem Ablauf des Zertifikats stattfinden. Es soll sichergestellt werden, dass die Fristen für umzusetzende Korrekturen und Korrekturmaßnahmen zu den im Re-Zertifizierungsaudit festgestellten wesentlichen Abweichungen/Nichtkonformitäten noch vor Ablauf der Zertifizierung umgesetzt werden.

Falls eine Re-Zertifizierung nicht bis zum Ablaufdatum des Zertifikates abgeschlossen ist, können Audits, die Verifizierung der Korrekturmaßnahmen und die unabhängige Zertifizierungsentscheidung unter folgenden Bedingungen innerhalb eines Zeitraums von 6 Monaten nach dem Ablaufdatum abgeschlossen werden:

- der Angebots-, Auftrags- und Vertragsprüfungsprozess sowie die Abstimmung der Auditplanung müssen nachweislich vor dem Ablauftermin des alten Zertifikates abgeschlossen sein
- das neue Zertifikat beginnt mit dem Tag der Entscheidung zur Re-Zertifizierung und bekommt den Ablauftermin des bisherigen Zertifikatszyklus (d.h. Ablauftermin altes

Zertifikat + 3 Jahre),

- der Zeitraum zwischen Ende altes Zertifikat und Beginn neues Zertifikat in dem keine gültige Zertifizierung bestand, wird auf dem neuen Zertifikat vermerkt. Das Unternehmen darf während dieser Zeit mit der Zertifizierung nicht werben.

Falls eine Re-Zertifizierung nicht innerhalb eines Zeitraumes von 6 Monaten nach dem Ablaufdatum des Zertifikates abgeschlossen werden kann, ist der Re-Zertifizierungsprozess beendet und eine neue Zertifizierung kann nur unter den Bedingungen einer Erst-Zertifizierung erfolgen.

Die Entscheidung über die Re-Zertifizierung wird unter Berücksichtigung der Empfehlung des Auditteams, der Ergebnisse aus der Bewertung des Systems über den Zeitraum der Zertifizierung und von dem Kunden erhaltenen Beschwerden getroffen.

6. Mehrstandort-Unternehmen

Organisationen mit mehreren Standorten können in einem Zertifizierungsverfahren auditiert und zertifiziert werden, wenn sie einem gemeinsamen Managementsystem unterliegen. Im Erhebungsbogen muss die Organisation bestätigen, dass ein einziges Managementsystem in der gesamten Organisation angewendet wird, die unter der Kontrolle der definierten Zentrale liegen.

Die Zentrale ist Teil der Organisation und darf nicht an eine externe Organisation untervergeben sein. Sie muss die organisatorische Befugnis haben, das einzige Managementsystem zu definieren, einzuführen und zu warten.

Bei Erfüllung weiterer Voraussetzungen kann in diesen Fällen ein Stichprobenverfahren zum Einsatz kommen. Nach einem positiven Begutachtungsergebnis wird die Zertifizierung für die Gesamtorganisation erteilt.

Vertragspartner der Zertifizierungsstelle ist die Unternehmenszentrale, die für alle Standorten und Unternehmen im Zertifizierungsbereich Verantwortung trägt und sie mit diesen eine rechtlich durchsetzbare Vereinbarung über die Zertifizierungstätigkeiten und über die Anerkennung ihrer leitenden Funktion abschließt.

Wenn es zeitweilige Standorte („temporary sites“) gibt, die Risiken für die Erfüllung der Informationssicherheitsziele darstellen (ISMS und IT-Sicherheitskatalog) oder besondere Risiken betreffend Energieverbrauch und wesentlicher Energieeinsätze (EnMS) darstellen, werden sie in die Stichprobenverfahren miteinbezogen.

Voraussetzungen für eine stichprobenartige Auditierung der Unternehmensstandorte sind:

- Es werden sehr ähnliche Produkte hergestellt oder sehr ähnliche Dienstleistungen erbracht;

- Bei Energiemanagementsystemen werden die Tätigkeiten der Organisation bezüglich Energiequellen, Energieeinsätzen und Energieverbrauch an allen Standorten in ähnlicher Weise unter Befugnis und Lenkung der Organisation durchgeführt. Wenn **„zeitweilige Standorte“** vorhanden sind und sie ein wesentliches Element der Energieeinsätze und des Energieverbrauchs der Organisation darstellen, müssen sie im Erhebungsbogen angegeben und in die Stichprobenverfahren aufgenommen werden. Ein zentral gelenkter und verwalteter Energieplanungsprozess muss vorliegen. Die Standorte mit den energieintensivsten Prozessen werden häufiger auditiert.
- Die Organisation liefert der Zertifizierungsstelle im Anhang des Erhebungsbogens alle Informationen über die Standorte einschließlich Tätigkeiten am Standort. Nach Beginn des Zertifizierungsverfahrens darf die Liste der Standorte nicht verändert werden,
- Alle Standorte unterliegen einem gemeinsamen Managementsystem, welches von der Zentrale festgelegt und überwacht wird;
- Alle Standorte unterliegen einem zentral geführten und gesteuerten internen Auditprogramm und in Übereinstimmung mit diesem Programm vor der Zertifizierung auditiert wurden
- Alle Forderungen an die zentrale Steuerung des Managementsystems müssen von der Muttergesellschaft erfüllt werden, Leitung-, Management- und Verwaltungsprozesse können nicht in die Standorte delegiert werden;
- Stichprobenanzahl und Auswahl der Standorte obliegen IFU-CERT. Wesentliche Grundlage für die Anzahl der Stichproben ist die Anzahl der eingeschlossenen Standorte. Aspekte bei der Auswahl der Standorte richten sich nach den Ergebnissen interner Audits und der Bewertung durch die Leitung, Größe der Standorte, Komplexität der Standorte und des Managementsystems, Unterschiede in Arbeitspraktiken und Tätigkeiten, unterschiedliche Rechtsforderungen etc.; Bei Energiemanagementsystemen werden zusätzlich die Komplexität von Energiequellen, Energieeinsätzen und Energieverbrauchern berücksichtigt. Die Häufigkeit der Stichprobenprüfung wird an den Standorten erhöht, welche besondere Risiken betreffend Energieverbrauchern und wesentlicher Energieeinsätze darstellen.
- Sollten Nichtkonformitäten (Abweichungen) an einzelnen Standorten festgestellt werden, entweder während des internen Audits der Organisation oder während der Auditierung durch die Zertifizierungsstelle, muss das Unternehmen nachforschen, ob die anderen Standorte ebenfalls betroffen sein könnten. Aufzeichnungen der Überprüfung müssen aufbewahrt werden. Das Unternehmen muss prüfen, ob die Nichtkonformitäten (Abweichungen) eine allgemeine Unzulänglichkeit des Gesamtsystems darstellen. In diesem Fall müssen Korrekturmaßnahmen durchgeführt und nachgeprüft werden, und zwar sowohl in der Zentrale als auch an den einzelnen betroffenen Standorten. Sollten die Nichtkonformitäten (Abweichungen) nicht das Gesamtsystem betreffen, muss das Un-

ternehmen gegenüber der Zertifizierungsstelle nachweisen, dass eine Einschränkung ihrer Folgemaßnahmen gerechtfertigt ist.

- **Für ISMS-Audits und für die Audits nach IT-Sicherheitskatalog nach §11 Abs. 1a und 1b EnWG:** Sollten Nichtkonformitäten (Abweichungen) an einzelnen Standorten oder in der Zentrale während eines Zertifizierungsaudits festgestellt werden, müssen die Korrekturmaßnahmen an allen Standorten einschließlich Zentrale umgesetzt werden.
- Wenn ein Standort eine wesentliche Nichtkonformität zum Zeitpunkt der Zertifizierung aufweist, wird die Zertifizierung gegenüber dem gesamten Netzwerk verweigert. Problematische Standorte dürfen nicht aus dem Geltungsbereich ausgeschlossen werden.
- Für die Durchführung und Überwachung von Korrekturmaßnahmen ist die Unternehmenszentrale verantwortlich;
- Zertifizierungsdokumente: Eingeschlossene Standorte werden im Anhang des Zertifikats aufgeführt. Auf Wunsch können Zertifizierungsdokumente (Auszugszertifikate) nur für einen Standort ausgestellt werden. „Dieses Zertifizierungsdokument kann unter keinen Umständen auf den Namen des Standorts oder der Rechtsperson ausgestellt werden oder andeuten, dass dieser Standort oder die Rechtsperson zertifiziert ist (zertifiziert ist die Kundenorganisation). Darin kann auch keine Konformitätserklärung der Prozesse/Tätigkeiten des Standorts mit dem normativen Dokument enthalten sein.“ (Gemäß IAF MD 1:2018, deutsche Übersetzung durch DAkkS, *Verbindliches IAF Dokument für die Auditierung und Zertifizierung von Managementsystemen in Organisationen mit mehreren Standorten* Kap. 7.8.3) Die Auszugszertifikate gelten ausschließlich zusammen mit dem Hauptzertifikat für die Zentrale;
- Die Zentrale wird bei jeder Überwachung mit begutachtet;
- Das Zertifikat wird entzogen, wenn einer der eingeschlossenen Standorte die Bedingungen für den Zertifikatsentzug erfüllt.
- Die Aufnahme neuer Standorte muss rechtzeitig vor dem Audit beantragt bzw. angemeldet werden. Ein neuer Standort wird zusätzlich zu der festgelegten Stichprobe auditiert. Eine Gruppe neuer Standorte kann nach den Matrix-Regeln stichprobenartig auditiert werden.

Wenn keine Matrix-Zertifizierung (Stichprobenauswahl der Standorte) erfolgen kann, weil die Voraussetzungen nicht erfüllt sind (z.B. im Wesentlichen unterschiedliche Prozesse/Tätigkeiten an den Standorten durchgeführt werden) oder weitere Gründe vorliegen, richten sich die Verfahren nach den Regeln der **Organisationen mit mehreren Standorten ohne Stichprobenverfahren.** Die Anforderungen an ein zentralgeführtes Managementsystem, mit gemeinsamen internen Auditprogramm und zentralisierten Management Review für alle Standorte bleiben für dieses Verfahren unverändert. Sowohl die Zentrale als auch alle Standorte werden in Erst-zertifizierungs- und in Re-Zertifizierungsverfahren alle einzeln audi-

tiert. Die Zentrale und 30% der Standorte werden in Überwachungsaudits auditiert. Für die Festlegung der Auditzeiten ist Angabe der Prozesse / Tätigkeiten an den Standorten im Erhebungsbogen – Standortliste erforderlich.

Zwischen diesen beiden extremen Fällen gibt es viele Organisationen mit mehreren Standorten, bei denen einige Standorte ähnliche Prozesse/Tätigkeiten ausführen, wohingegen andere Standorte sehr spezifische Prozesse ausüben, die an keinen anderen Stellen der Organisation vorkommen. Das Stichprobenverfahren wird auf diejenigen Standorte beschränkt, die sehr ähnliche Prozesse/Tätigkeiten durchführen.

7. Aussetzung, Zurückziehung der Zertifikate oder Einschränkung des Geltungsbereichs der Zertifizierung

7.1 Die Einschränkung des Zertifikates

Wenn Tätigkeiten oder Standorte wegfallen, ist das Unternehmen verpflichtet, diese Änderung anzumelden und einen aktualisierten Erhebungsbogen einzureichen. Im Falle einer Einschränkung des Geltungsbereichs oder Aufgabe eines Standortes wird das Zertifikat entsprechend geändert.

Eine Einschränkung des Geltungsbereichs findet auch statt, wenn einige Teile der Anforderungen in Übereinstimmung mit der verwendeten Norm dauerhaft oder schwerwiegend nicht mehr erfüllt werden.

Bei der Einschränkung des Zertifikates hat das Unternehmen alle Werbemittel entsprechend zu ändern.

7.2 Aussetzung des Zertifikates

IFU-CERT wird Zertifikate aussetzen, wenn:

- der zertifizierte Kunde die Durchführung der planmäßigen Überwachungs- oder Re-Zertifizierungsaudits in der erforderlichen Häufigkeit nicht gestattet,
- ein zertifiziertes Managementsystem eines Kunden die Zertifizierungsanforderungen (einschließlich der Anforderungen an die Wirksamkeit des Managementsystems) dauerhaft oder schwerwiegend nicht erfüllt,
- Informationen zu Vorkommnissen wie einem schweren Unfall oder einem schwerwiegenden Verstoß gegen Vorschriften, die die Mitwirkung der zuständigen Aufsichtsbehörde erfordern, muss der Zertifizierungsstelle Gelegenheit geben, über die zu ergreifenden Maßnahmen zu entscheiden, einschließlich einer Aussetzung oder eines Entzugs der Zertifizierung nach BS OHSAS 18001 oder DIN ISO 45001, wenn nachgewiesen werden kann, dass das System die Anforderungen an die Arbeitsschutzanforderungen ernsthaft nicht erfüllt hat.

- Nichtkonformitäten (Abweichungen) nicht abgestellt werden,
- Verstöße gegen die Anzeigepflicht bei wesentlichen Änderungen vorliegen,
- Verstöße gegen IT-Recht oder gegen Meldepflichten bei wesentlichen Informationssicherheitsvorfällen vorliegen
- Verstöße gegen Regeln der Zeichennutzung und Verweise auf die Zertifizierung
- die erstellte und versandte Rechnung für die Zertifizierung bzw. für die Überwachung trotz Mahnung nicht spätestens 3 Monate nach Ausstellung der jeweiligen Rechnung beglichen wurde.
- der zertifizierte Kunde es wünscht.

Bei Aussetzung des Zertifikats ist die Zertifizierung zeitweise außer Kraft gesetzt. Das Unternehmen hat die Werbung, Verweise auf und sonstige Nutzung des Zertifikats unverzüglich einzustellen. Das Aussetzen des Zertifikates wird von der Zertifizierungsstelle öffentlich zugänglich gemacht. Das Aussetzen eines Zertifikats nach IT Sicherheitskatalog, gemäß § 11 Absatz 1a und nach IT Sicherheitskatalog, gemäß § 11 Absatz 1b Energiewirtschaftsgesetz, wird unverzüglich der Bundesnetzagentur gemeldet.

Wenn die Probleme, die zur Aussetzung geführt haben, binnen 6 Monate nicht gelöst worden sind, wird das Zertifikat zurückgezogen (annulliert). In den anderen Fällen entscheidet die Zertifizierungsstelle über den Umfang eines durchzuführenden Audits zur Neubewertung des Managementsystems. Gegebenenfalls wird der Geltungsbereich eingeschränkt, um diejenigen Teile auszuschließen, die die Anforderungen nicht erfüllen.

7.3 Zurückziehung (Annullierung) des Zertifikates

IFU-CERT kann Zertifikate entziehen/annullieren, wenn:

- Zertifikate missbräuchlich verwendet werden. Missbrauch liegt vor, wenn:
  - die Zertifikatwerbung 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,
  - 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,
- Wenn die Probleme, die zur Aussetzung geführt haben, binnen 6 Monate nicht gelöst worden sind

- Bei Missbrauch wird das Zertifikat sofort entzogen.

7.4 Informationspflicht der Zertifizierungsstelle

Bei Aussetzung oder Entzug (Annullierung) des Zertifikates wird das Unternehmen sofort benachrichtigt. Das Unternehmen wird aus der Liste der zertifizierten Unternehmen entfernt und der Entzug von der Zertifizierungsstelle öffentlich zugänglich gemacht. Das Unternehmen hat die Werbung, Verweise auf und sonstige Nutzung des Zertifikats und des Zertifizierungszeichens unverzüglich einzustellen.

Bei Aussetzung oder Entzug (Annullierung) eines Zertifikates nach **IT-Sicherheitskatalog nach § 11 Abs. 1a und Abs. 1b** EnWG wird die Bundesnetzagentur sofort informiert.