DeuZert® Deutsche Zertifizierung in Bildung und Wirtschaft GmbH

Hochschulring 2

15745 Wildau

Verfahren zur Zertifizierung nach IT-Sicherheitskatalog gem. § 11 Abs. 1a EnWG

Dokument WP04 K - D01

Z U S A M M E N F A S S U N G

- Prüfungsordnung Zertifizierung von Managementsystemen
- Verfahrensanweisung Zertifizierung nach IT-Sicherheitskatalog gem. § 11 Abs. 1a EnWG

Inhalt:

Einführung

Das vorliegende Dokument stellt eine Zusammenfassung des Verfahrens zur Zertifizierung nach IT-Sicherheitskatalog gem. § 11 Abs.1a EnWG inklusive DIN EN ISO/IEC 27001:2017 i. V. m. EN ISO/IEC 27006:2020 der Zertifizierungsstelle DeuZert® dar – vgl. Abbildung Nr. 1.
Ziel dieses Dokuments ist es, die zu zertifizierende Organisation über die relevanten Regelungen zu informieren.
Dieses Verfahren wurde entwickelt in Übereinstimmung mit der relevanten Norm DIN EN ISO/IEC 17021:2015 i. V. m. EN ISO/IEC 27006:2020 sowie dem Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz in der jeweils aktuellsten Fassung.

Zertifizierungsantrag

Nach Eingang des Auftrages zur Zertifizierung erhält der Kunde das Antragsformular auf Zertifizierung und weitere Zertifizierungsunterlagen. Erst, wenn der Kunde den unterschriebenen Antrag auf Zertifizierung nebst den notwendigen Nachweisen (Dokumente/Unterlagen) zur Erfüllung der Zertifizierungsanforderungen der Zertifizierungsstelle übermittelt hat, sowie eine erfolgreiche Prüfung auf Vollständigkeit und Plausibilität erfolgt ist, kann das Auditverfahren begonnen werden.

Erst-Zertifizierungsaudit

Das Zertifizierungsaudit, eines Informationssicherheitsmanagementsystems (ISMS) gemäß IT-Sicherheitskatalog gem. § 11 Abs. 1a EnWG, besteht aus dem Audit Stufe 1 und dem Audit Stufe 2. Zusätzlich kann optional ein Voraudit vorgeschaltet durchgeführt werden.
Bei dem ISMS sind die Normen DIN ISO/IEC 27002 und DIN SPEC 27019 in der jeweils aktuellen Fassung zu berücksichtigen.

Vor-Audit

Die Durchführung eines Voraudits ist optional und einmalig. Ziel ist es, die Bereitschaft für das Zertifizierungsaudit der Organisation festzustellen („Zertifizierungsfähigkeit“). Es werden keine Empfehlungen, Ratschläge oder sonstigen Feststellungen getroffen, die einen Interessenskonflikt herbeiführen können. Entsprechend einem erstellten Auditplan führt ein Auditor das Voraudit durch und dokumentiert dieses kurz in einem Auditbericht. Ein Fachexperte, gem. Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz in der jeweils aktuellsten Fassung, kann hinzugezogen werden. Der für das Voraudit vorgesehene Aufwand wird nicht auf den Aufwand des Zertifizierungsaudits angerechnet und verkürzt damit auch nicht den Aufwand des Zertifizierungsaudits.

Audit Stufe 1

Während des Audits Stufe 1 werden die Managementdokumentation des Kunden sowie die Betriebsstätten-spezifischen Bedingungen auditiert. Sollten mehrere Betriebsstätten zertifiziert werden, findet das Audit Stufe 1 in der Unternehmenszentrale statt.

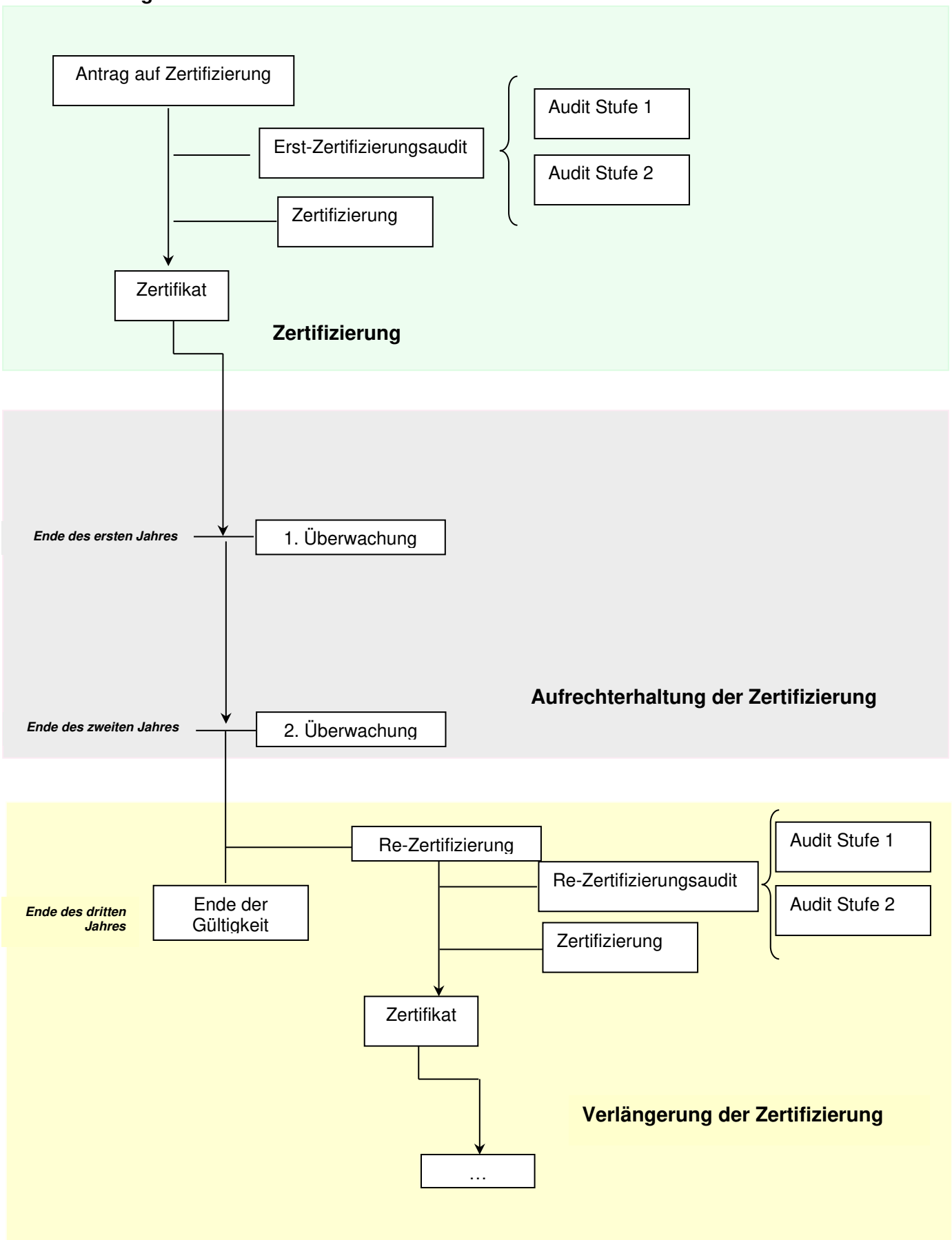
Die vom Kunden vorzulegende Managementdokumentation muss umfassen:

- Einen Netzstrukturplan mit den Technologiekategorien:
  - Leitsystem/Systembetrieb,
  - Übertragungstechnik/Kommunikation,
  - Sekundär-, Automatisierungs- und Fernwirktechnik,
- eine dokumentierte Erklärung der ISMS-Leitlinie, -Politik und der ISMS-Ziele,
- den Geltungsbereich des ISMS mit:
  - mindestens zentralen und dezentralen Anwendungen, Systeme und Komponenten, die für einen sicheren Netzbetrieb notwendig sind. Enthalten sollen demnach zumindest alle TK- und EDV-Systeme des Netzbetreibers sein, welche direkt Teil der Netzsteuerung sind, d. h. unmittelbar Einfluss nehmen auf die Netzfahrweise,
  - Daneben sollen auch TK- und EDV-Systeme im Netz berücksichtigt werden, die selbst zwar nicht direkt Teil der Netzsteuerung sind, deren Ausfall jedoch die Sicherheit des Netzbetriebs gefährden könnte. Darunter fallen z. B. Messeinrichtungen an Trafo- oder Netzkoppelstationen,
  - Solange und soweit Messsysteme nach § 21d EnWG zu netzbetrieblichen Zwecken (z. B. Ermittlung von Netzzustandsinformationen, Ermöglichung von Last- und Erzeugungsmanagement u.a.) eingesetzt werden, ist sicherzustellen, dass hinsichtlich dieses Teilbereichs Sicherheitsstandards eingehalten werden, die dem IT-Sicherheitskatalog zumindest gleichwertig sind,
- Verfahren und Maßnahmen, die das ISMS unterstützen,
- eine Beschreibung des Prozesses zur Risikoeinschätzung der Informationssicherheit,
- den Bericht der Risikoeinschätzung mit den drei Schadenskategorien:
  - „kritisch“ (die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen),
  - „hoch“ (die Schadensauswirkungen können beträchtlich sein),
  - „mäßig“ (die Schadensauswirkungen sind begrenzt und überschaubar),
- den Risikobehandlungsplan,
- dokumentierte Verfahren, die die Organisation zur Sicherstellung der wirksamen Planung, Durchführung und Kontrolle ihrer Informationssicherheitsprozesse benötigt, und die beschreiben, wie die Wirksamkeit von Maßnahmen zu messen ist,
- Ergebnisse dieser Messungen u.a. Überwachungen zur Informationssicherheit
- von der Norm geforderte Aufzeichnungen,
- die Erklärung zur Anwendbarkeit (SoA),
- die schriftliche Benennung der Ansprechpartner:in IT-Sicherheit mit den Aufgaben und Kompetenznachweisen,

- ein aktuelles Organigramm / Darstellung der Aufbauorganisation,
- eine Liste der mitgeltenden Dokumente und Formblätter,
- eine Liste der dokumentierten Verfahren,
- Verfahrensbeschreibungen zu:
  - Lenkung von Dokumenten,
  - Lenkung von Aufzeichnungen,
  - Internen Audits,
  - Korrektur- und Vorbeugungsmaßnahmen
- Nachweise über die Durchführung von internen Audits und der Managementbewertung,
- Nachweise zu festgestellten Abweichungen und abgeleiteten Korrketurmaßnahmen.

Die einzureichende Dokumentation sollte vom Kunden sicher / verschlüsselt an die Zertifizierungsstelle übertragen werden. Der Auditor sammelt im Audit notwendige Informationen bezüglich des Geltungsbereichs des ISMS, der Prozesse der Betriebsstätten des Kunden sowie zugehörige gesetzliche und behördliche Aspekte und deren Einhaltung sowie der damit verbundenen Risiken und ihre Bewertung. Dabei wird ggf. ein Fachexperte gem. Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz in der jeweils aktuellsten Fassung hinzugezogen.
Ziel ist es zu bewerten, in wie weit die Anforderungen des IT-Sicherheitskataloges gem. § 11 Abs. 1a EnWG inklusive DIN EN ISO/IEC 27001:2017 i. V. m. EN ISO/IEC 27006:2020 für die Durchführung des Audits Stufe 2 vom Kunden erfüllt werden. Bei einer Nichterfüllung der Anforderungen, wird dem Kunden eine Frist zur Nachbesserung gegeben. Erst wenn der Kunde innerhalb dieser Frist die Nachbesserungen durchgeführt hat, kann das Audit Stufe 2 stattfinden. Im Einzelfall kann eine Wiederholung des Audits Stufe 1 notwendig sein. Hier ist zu beachten, dass der Abstand zwischen dem Audit Stufe 1 und dem Audit Stufe 2 nicht länger als 3 Monate betragen darf. Der Mindestabstand zwischen Audit Stufe 1 und Stufe 2 beträgt eine Woche für den Fall, wenn Schwachstellen jeglicher Art (also auch Verbesserungspotentiale) im Audit Stufe 1 identifiziert werden. Über das Ergebnis des Audits Stufe 1 erstellt der Auditor einen Bericht, der von der Zertifizierungsstelle freizugeben ist.

Abbildung Nr. 1



Audit Stufe 2

Während des Audits Stufe 2 wird die Umsetzung und Wirksamkeit des ISMS des Kunden beurteilt. Es wird geprüft, ob das, was festgelegt und / oder dokumentiert wurde, tatsächlich umgesetzt wird.
Der Auditor führt entsprechend einem Auditplan, der dem Kunden im Vorfeld zur Verfügung gestellt wird, das Audit durch. Das Audit schließt eine Befragung von Mitarbeitern am Arbeitsplatz sowie die Einsichtnahme in mitgeltenden Unterlagen, Aufzeichnungen oder ähnliche Dokumente und die Begehung von relevanten Bereichen ein. Dabei wird ggf. ein Fachexperte gem. Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz in der jeweils aktuellsten Fassung hinzugezogen.
Teilnehmer an dem Audit werden in der Anlage des Auditplans mit Unterschrift festgehalten. Der Auditor erstellt im Ergebnis des Audits Stufe 2 einen Auditbericht inklusive aller Feststellungen aus dem Audit Stufe 2 – evtl. Nichtkonformitäten können auch separat in einem Bericht dokumentiert werden. Der Kunde und der Leitende Auditor unterschreiben zwei Exemplare der Berichte. Ein Exemplar wird zum Ende des Audits dem Kunden überlassen, vorbehaltlich der Freigabe durch DeuZert®. Das zweite Exemplar wird DeuZert® zur Freigabe vorgelegt und anschließend in der Kundenakte abgelegt. Die Berichte bleiben Eigentum von DeuZert®.
Im einen Abschlussgespräch teilt der Auditor dem Kunden das Ergebnis des Audits mit. Bei festgestellten Nichtkonformitäten werden die weiteren Maßnahmen festgelegt. Die weitere Bearbeitung der festgestellten Nichtkonformitäten verursacht in jedem Fall zusätzlichen Aufwand, der dem Kunden zusätzlich in Rechnung gestellt werden muss.

Zertifizierung

Die Entscheidung über die Erteilung einer Zertifizierung trifft der Zertifizierungsausschuss. Mitglieder des Zertifizierungsausschusses sind die fachliche Leitung der Zertifizierungsstelle oder ein vertretungsberechtigter Mitarbeiter sowie ein am Zertifizierungsverfahren nicht beteiligter und berufener Auditor.
Die Entscheidung im Zertifizierungsausschuss wird auf Grundlage der zu beurteilenden Verfahrensunterlagen, der Überprüfung der Empfehlung des Auditors sowie auf der Grundlage von weiteren relevanten Informationen (z. B. öffentliche Informationen, Stellungnahme des Kunden zum Auditbericht) getroffen.
Basierend auf dem von der Organisation ausgefüllten und unterschriebenen Formular zur Bestellung von Zertifikaten und mit Datum der Zertifizierungsentscheidung, erstellt DeuZert® das Zertifikat. Durch die Vergabe der Registriernummer wird das Zertifikat offiziell registriert. Das Zertifikat ist ab Datum der Zertifizierungsentscheidung 3 Jahre gültig.
Im Leistungsumfang ist die Erstellung und Registrierung von maximal 2 Originalzertifikaten (Haupt- und Unterzertifikaten) ohne Firmenlogoeindruck im Format DIN A4 oder A3 in den Sprachen Deutsch und Englisch sowie im PDF-Format enthalten. Für weitere Wünsche ist die Preisliste von DeuZert® in der aktuell gültigen Version zu beachten.

Gemäß Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz in der jeweils aktuellsten Fassung, übermittelt DeuZert® jeweils zum 30. Juni und 31. Dezember eines Jahres folgende Daten des zertifizierten Unternehmens an die Bundesnetzagentur:

- Netzbetreibernummer,
- Zertifikat-Nummer,
- Unternehmensbezeichnung,
- Gegenstand der Zertifizierung (Strom- und/ oder Gasnetz),
- Ausstellungsdatum des Zertifikats,
- Ablaufdatum des Zertifikats.

Aufrechterhaltung und Verlängerung der Gültigkeit

Überwachungsaudit

Während der Gültigkeit des Zertifikats werden jährliche Überwachungsaudits bei zertifizierten Unternehmen durchgeführt. In den Überwachungsaudits wird geprüft, ob Änderungen im Informationssicherheits-Managementsystems (ISMS) des Unternehmens vorgenommen wurden und ob das Unternehmen weiterhin die alle für die Zertifizierung relevanten Forderungen erfüllt.
Vor der Planung der jährlichen Überwachungsaudits aktualisiert DeuZert® die vorhandenen Kundeninformationen - insbesondere die Anzahl der Mitarbeiter und Betriebsstätten. Festgestellte Änderungen können zu einer Justierung/Änderung in der ursprünglichen ermittelten Auditdauer führen. Sollte das der Fall sein, hat DeuZert® die Auditdauer und/oder den Auditinhalt neu zu bestimmen.
Überwachungsaudits umfassen u. a. folgende Punkte:

- Prüfung ob interne Audits und Managementbewertungen durchgeführt und dokumentiert worden sind,
- Bewertung der Wirksamkeit ergriffener Maßnahmen zu Feststellungen aus dem vorhergehenden Audit,
- Prüfung der Behandlung von Beschwerden gegen das Managementsystem und von Sicherheitsproblemen,
- Prüfung der Wirksamkeit des Managementsystems im Hinblick auf das Erreichen der Ziele,
- Prüfung ob Fortschritt bei geplanten Tätigkeiten, die auf eine ständige Verbesserung zielen, gegeben ist,
- Prüfung ob anhaltende Betriebssteuerung/-lenkung gegeben sind,
- Bewertung von Unternehmensdaten wie Anzahl der Mitarbeiter, Anzahl von Betriebsstätten, usw.,
- Nutzung von Zertifizierungszeichen.

Der Solltermin für das jährliche Überwachungsaudit, das dem Zertifizierungsaudit folgt, darf nicht mehr als 12/24 Monate nach dem letzten Tag des Audits Stufe 2 liegen.
Überwachungsaudits dürfen frühestens 3 Monate vor dem Solltermin stattfinden. Vier Monate vor dem Solltermin informiert DeuZert® den Kunden über den Solltermin des kommenden Audits und vereinbart mit ihm Zeitspanne von 2 Wochen, innerhalb derer das Überwachungsaudit durchgeführt werden soll. Der Auditor vereinbart mit dem Kunden den konkreten Termin.

Der Auditor führt die Überwachungsaudits analog zum Audit Stufe 2 durch und dokumentiert dieses in einem Auditbericht– evtl. Nichtkonformitäten können auch separat in einem Bericht dokumentiert werden.
Die Entscheidung im Zertifizierungsausschuss über die Aufrechterhaltung der Zertifizierung wird auf Grundlage der zu beurteilenden Verfahrensunterlagen, der Überprüfung der Empfehlung des Auditors sowie auf der Grundlage von weiteren relevanten Informationen (z. B. öffentliche Informationen, Stellungnahme des Kunden) getroffen.
Bei Aussetzung/Entzug der Zertifizierung übermittelt DeuZert® dies der Bundesnetzagentur unverzüglich gemäß Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz in der jeweils aktuellsten Fassung.

Re-Zertifizierung

Eine Zertifizierung kann durch ein Re-Zertifizierungsaudit für weitere 3 Jahre verlängert werden, wenn das Re-Zertifizierungsaudit, einschließlich der Prüfung von Maßnahmen zur Korrektur von Nichtkonformitäten und der Empfehlung des Auditors zur Zertifikatserteilung, noch vor Ablauf der Gültigkeit des Zertifikats abgeschlossen sind.
Der Sollzeitraum für das Re-Zertifizierungsaudit ist das Datum des Ablaufs des Zertifikats minus 3 Monate.
Mindestens 4 Monate vor Ablauf der Gültigkeit des Zertifikats nimmt DeuZert® Kontakt mit dem Kunden auf und sendet ihm den Anfragebogen auf Re-Zertifizierung. Der Kunde beantragt ca. 3 Monate vor Ablauf der Gültigkeit des Zertifikats das Re-Zertifizierungsverfahren.
Tätigkeiten zu Re-Zertifizierungsaudits können ein Audit Stufe 1 erfordern, wenn es signifikante Änderungen im ISMS, beim Unternehmen oder im Zusammenhang mit der Arbeitsweise des ISMS gibt. In diesem Fall erfolgt das Audit Stufe 1 wie bereits oben beschrieben.
Die Re-Zertifizierung umfasst ein Audit Stufe 2, das wie oben beschrieben wurde, durchgeführt und dokumentiert wird.
Analog zur Zertifizierung wird die Entscheidung über die Verlängerung des Zertifikats getroffen.

Im Folgenden werden weitere Regelungen aufgelistet:

Weitere Regelungen

- Der Kunden kann gegen die Benennung eines jeden Auditors bzw. Fachexperten Einspruch einlegen. Angaben zu Namen und wenn erwünscht, Hintergrundinformationen zu jedem Mitglied des Auditteams werden nach Anfrage zur Verfügung gestellt. Dabei finden die aktuellen Regelungen zum gesetzlichen Datenschutz Beachtung.
- Einsprüche gegen die Zertifizierungsentscheidung sowie Beschwerden sind möglich. Sie führen nicht zu einer Benachteiligung des Einspruchsführers bzw. des Beschwerdeführers. Der Einspruchsführer hat binnen 4 Wochen ab Kenntnisnahme der Zertifizierungsentscheidung bei DeuZert® den Einspruch schriftlich einzulegen. Schriftliche Beschwerden können jederzeit bei DeuZert® eingereicht werden.
- DeuZert® informiert den Kunden rechtszeitig über Änderungen in den Anforderungen an die Zertifizierung. Der Kunde verpflichtet sich, aus den Änderungsmitteilungen eventuell daraus resultierende Anpassungen vorzunehmen.
- Die Verwendung des DeuZert® - Logos wird vertraglich geregelt. Diese Regelungen sind aus der Prüfungsordnung WP04 D001: Zertifizierung von Managementsystemen zu entnehmen.
- DeuZert® führt ein Verzeichnis über die gültigen Zertifizierungen gemäß den Anforderungen aus dem Konformitätsbewertungsprogramm zur Akkreditierung von Zertifizierungsstellen für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz, Stand 13.04.2016, ergänzt um den Geltungsbereich der Zertifizierung und die zertifizierten Standorte. DeuZert® kann dieses Verzeichnis nach Anfrage offenlegen.
- DeuZert® hat das Recht, nach Anfrage einer interessierten Seite diese über den Status einer Zertifizierung zu informieren. Weitere Informationen über Kunden werden mit höchster Priorität vertraulich behandelt und dürfen an Dritte nur dann offengelegt werden, wenn der Kunde dazu eine schriftliche Zustimmung abgegeben hat. Wenn DeuZert® gesetzlich verpflichtet ist, vertrauliche Informationen gegenüber Dritten offen zu legen, so wird der betreffende Kunde über diese Information vorab unterrichtet.
- Das Unternehmen gewährt DeuZert® die Durchführung von Witness-Audits seitens der Akkreditierungsstelle. Zusätzliche Kosten entstehen dem Kunden dadurch nicht.
- Das Unternehmen hat der DeuZert® ohne Verzögerung über Angelegenheiten zu informieren, die die Fähigkeit des Managementsystems des Kunden beeinträchtigen könnten. Diese Angelegenheiten sind zum Beispiel Änderungen bezüglich:
  - der Rechts- oder Organisationsform, den wirtschaftlichen oder den Besitzverhältnissen,
  - Organisation und Management (z. B. Schlüsselpersonal in leitender Stellung, Entscheidungs- oder Fachpersonal),
  - Kontaktadressen und Betriebsstätten,
  - des vom zertifizierten ISMS erfassten Tätigkeitsfeldes,
  - wesentlicher Veränderungen des ISMS und der Prozesse,
  - jegliche sonstigen Ereignisse, welche zur Folge haben können, dass Zertifizierungsvoraussetzungen vorübergehend oder dauerhaft nicht mehr vorliegen.