DeuZert® Deutsche Zertifizierung in Bildung und Wirtschaft GmbH

Hochschulring 2

15745 Wildau

Verfahren zur Zertifizierung von Informationssicherheitsmanagementsystemen (ISMS) gemäß ISO/IEC 27001:2022

Dokument WP04 I - D01

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

- Prüfungsordnung Zertifizierung von Managementsystemen
- Verfahrensanweisung Zertifizierung von Informationssicherheitsmanagement-systemen (ISMS) gemäß ISO/IEC 27001:2022

Inhalt

Einführung

Das vorliegende Dokument stellt eine Zusammenfassung des Verfahrens zur Zertifizierung von Managementsystemen gemäß ISO/IEC 27001:2022 i. V. m. ISO/IEC 27006-1:2024 der Zertifizierungsstelle DeuZert® dar – vgl. Abbildung Nr. 1.
Ziel dieses Dokuments ist es, eine sichere, normenkonforme Zertifizierung nach ISO/IEC 27001:2022 inkl. korrekter Bestimmung der notwendigen Auditzeiten jederzeit zu gewährleisten und 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 inkl. Amd 1 i. V. m. ISO/IEC 27006-1:2024.

Zu beachten:

Wenn nachfolgend das Wort „Auditor“ benutzt wird, ist ein:e für ISO/IEC 27001:2022 qualifizierte:r Auditor:in gemeint.

Zertifizierungsantrag

Nach Eingang des Auftrages zur Zertifizierung erhält die Organisation das Antragsformular auf Zertifizierung und weitere Zertifizierungsunterlagen. Erst, wenn die Organisation 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-Zertifizierung und Bestimmung der Auditzeiten

Das Zertifizierungsaudit eines Informationssicherheitsmanagementsystems (ISMS) besteht aus dem Audit Stufe 1 und dem Audit Stufe 2. Zusätzlich kann optional ein Voraudit vorgeschaltet durchgeführt werden.

Voraudit

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 Vor-Audit durch und dokumentiert dieses kurz in einem Auditbericht. 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

Ziel des Audits Stufe 1 ist zu bewerten, inwieweit die Anforderungen gemäß ISO/IEC 27001:2022 für die Durchführung des Audits Stufe 2 von der Organisation erfüllt werden. Während des Audits Stufe 1 werden die Managementdokumentation der Organisation sowie die standortspezifischen Bedingungen auditiert. Sollten mehrere Standorte zertifiziert werden, findet das Audit Stufe 1 in der Zentrale der Organisation statt.
Die vom Kunden vorzulegende Managementdokumentation muss umfassen:

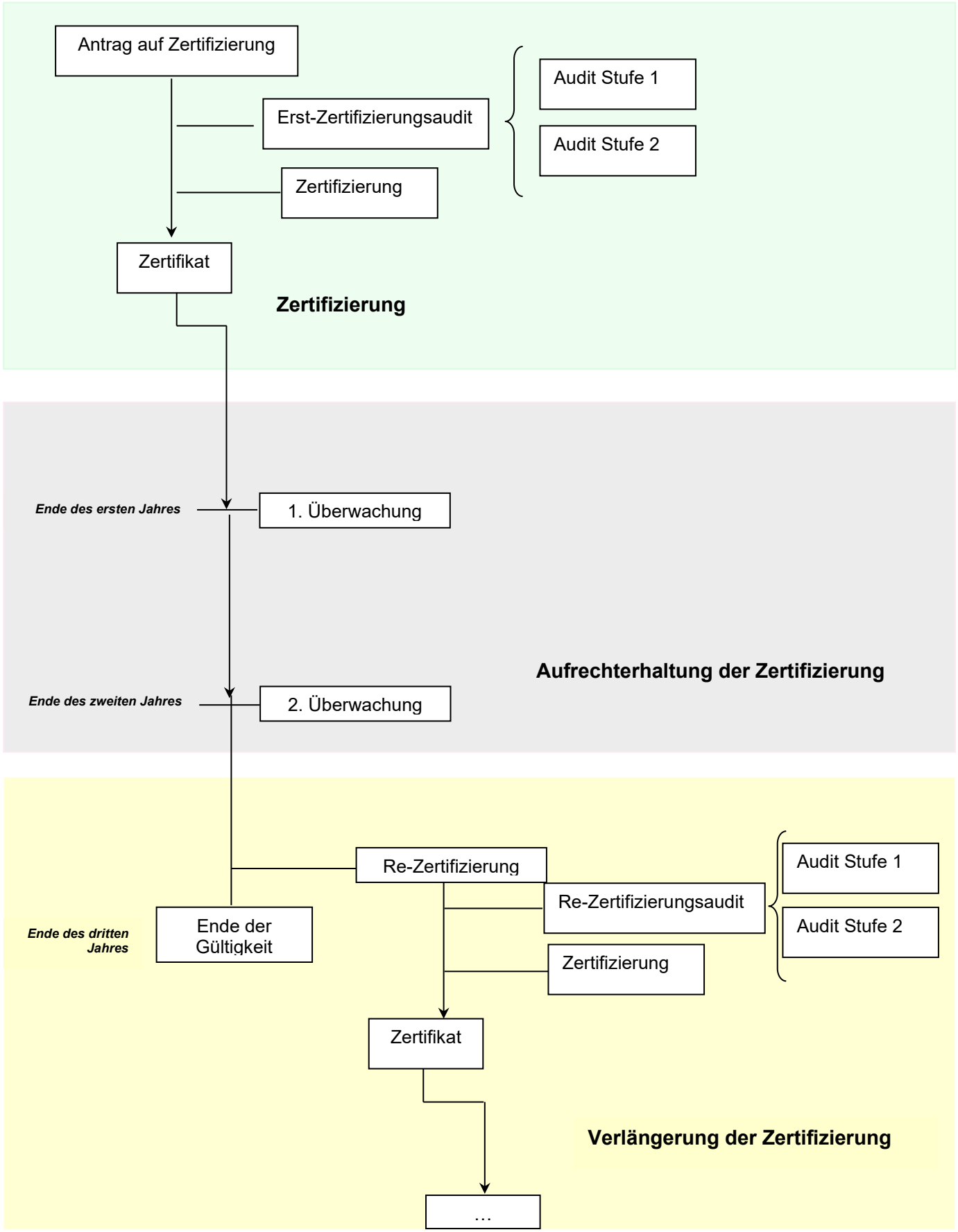
Dokumentierte Erklärung zur Informationssicherheitsleitlinie, Informationssicherheitspolitik, und den Informationssicherheitszielen
Dokumentation zum Anwendungsbereich des Informationssicherheitsmanagementsystems
Erklärung zur Anwendbarkeit (Statements of Applicability [SoA])
Verfahren und dokumentierte Maßnahmen, die das Informationssicherheitsmanagementsystem unterstützen
Beschreibung der Methode bzw. des Prozesses zur Risikoermittlung/ -behandlung
Bericht zur Risikoeinschätzung
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
Kompetenznachweise der Verantwortlichen für Informationssicherheit
Von der Norm geforderte Aufzeichnungen als Liste
Aktuelles Organigramm/ Darstellung der Aufbauorganisation
Liste der mitgeltenden Dokumente und Formblätter
Liste der dokumentierten Verfahren
Verfahrensbeschreibungen zu Lenkung dokumentierter Information, internen Audits, Korrektur- und Vorbeugungsmaßnahmen
Nachweise über die Planung und Durchführung von internen Audits und einer aktuellen Managementbewertung
Nachweise zu festgestellten Abweichungen und abgeleiteten Korrekturmaßnahmen

Die einzureichende Dokumentation sollte vom Kunden sicher/ verschlüsselt an die Zertifizierungsstelle übertragen werden. Der Auditor sammelt im Audit notwendige Informationen bezüglich des Geltungsbereichs des Informationssicherheitsmanagementsystems (ISMS), der Prozesse der Betriebsstätten des Kunden sowie zugehörige gesetzliche und behördliche Aspekte und deren Einhaltung sowie der damit verbundenen Risiken und ihre Bewertung.

Ziel ist es zu bewerten, in wie weit die Anforderungen der Norm für die Durchführung des Audits Stufe 2 vom Kunden erfüllt werden. Bei einer Nichterfüllung der Anforderungen der Norm, 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. Über das Ergebnis des Audits Stufe 1 erstellt der Auditor einen Bericht.

Das Audit Stufe 2 kann im Anschluss an das Audit Stufe 1 durchgeführt werden. In diesen Fall können aufgetretene Schwachstellen während des Audits Stufe 1 als Nichtkonformitäten im Audit Stufe 2 eingestuft werden. Es sollten aber ca. zwei Wochen Abstand zwischen Audit Stufe 1 und Stufe 2 gewählt werden.

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.
Die Auditteilnehmer werden in einer Teilnehmerliste mit Unterschrift festgehalten. Der Auditor erstellt im Ergebnis des Audits Stufe 2 einen Bericht, 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 des Auditberichts. 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. Der Auditbericht bleibt 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.

Aufrechterhaltung und Verlängerung der Gültigkeit

Überwachungsaudit

Während der Gültigkeit des Zertifikats werden jährliche Überwachungsaudits bei zertifizierten Kunden durchgeführt. In den Überwachungsaudits wird geprüft, ob Änderungen am ISMS des Kunden vorgenommen wurden und ob die Organisation weiterhin alle relevanten Normforderungen erfüllt.
Vor der Planung der jährlichen Überwachungsaudits aktualisiert DeuZert® die vorhandenen Kundeninformationen - insbesondere die Anzahl der Mitarbeiter und Standorte. 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. auch folgende Punkte:

- Prüfung ob interne Audits und Managementbewertungen durchgeführt und dokumentiert worden sind;
- Bewertung der ergriffenen Maßnahmen zu Feststellungen aus dem vorhergehenden Audit;
- Prüfung der Behandlung von Beschwerden gegen das Managementsystem und Sicherheitsprobleme;
- 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 Daten der Organisation, wie Anzahl der Mitarbeiter, Anzahl von Standorten, usw.;
- Nutzung von Zertifizierungszeichen.

Der Solltermin für das jährliche Überwachungsaudit, das dem Zertifizierungsaudit folgt, darf nicht mehr als 12 Monate nach dem Datum der Zertifizierungsentscheidung liegen. Überwachungsaudits müssen ansonsten mindestens einmal im Jahr durchgeführt werden.
Die Überwachungsaudits sollen frühestens 3 Monate vor dem Solltermin stattfinden. Ab vier Monate vor dem Solltermin informiert der DeuZert®-Kundendienst und vereinbart mit der Organisation den konkreten Termin.
Der Auditor führt die Überwachungsaudits analog zum Audit Stufe 2 durch und dokumentiert dieses in einem Bericht
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 zum Auditbericht) getroffen.

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.

Ab 4 Monate vor Ablauf der Gültigkeit des Zertifikats nimmt der DeuZert®-Kundendienst in der Regel Kontakt mit der Organisation auf und sendet ihr den Antrag auf Re-Zertifizierung. Die Organisation 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 am ISMS, bei der Organisation 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.

Übergang von DIN EN ISO/IEC 27001:2017 auf ISO/IEC 27001:2022

DeuZert® versendet gemäß Abschnitt „Weitere Regelungen“, 3. Punkt, im Mai 2023 eine dezidierte Kundeninformation zum Übergang bestehender ISMS-Zertifizierungen auf ISO/IEC 27001:2022.
Da jegliche Zertifizierungen gemäß DIN EN ISO/IEC 27001:2017 spätestens zum 31. Oktober 2025 auslaufen oder zurückgezogen werden, ist eine intensive inhaltliche Auseinandersetzung mit den Änderungen durch die Normaktualisierung für jeden Kunden angezeigt. Insbesondere (aber nicht nur) der normative Anhang A weist signifikante Änderungen auf (z. B. statt 114 Controls jetzt nur noch 93 Controls, davon 11 neu). Daher ist kundenseitig eine GAP-Analyse notwendig, um ggf. notwendige Änderungen am ISMS zu planen und umzusetzen. Dies könnte u. a. auch Auswirkungen auf die Erklärung zur Anwendbarkeit (SoA), den Risikoermittlungs- und -behandlungsplan haben. Auch ist das kundenseitige Personal für die Aufrechterhaltung des ISMS auf die Anforderungen der ISO/IEC 27001:2022 zu schulen. Für den Übergang gelten folgende weitere Regelungen:

- Der Übergang auf die ISO/IEC 27001:2022 muss formal als Änderung beantragt werden.
- Es ist in jedem Fall ein Übergangsaudit notwendig.
- Dieses Übergangsaudit kann in ein reguläres Überwachungs- oder Re-Zertifizierungsaudit integriert oder separat durchgeführt werden.
- Der Zusatzaufwand für das Übergangsaudit ergibt sich aus den entsprechenden normativen Dokumenten (z.B. IAF MD 26) und beträgt mindestens 0,50 Personentage.
- Eine ausschließliche Dokumentenprüfung zum Übergang ist ausgeschlossen. Ggf. sind teilweise Remote-Verfahren im Übergangsaudit möglich, sofern die Ziele des Übergangsaudits erreicht werden können.
- Das Übergangsaudit beinhaltet die Prüfung der GAP-Analyse zur ISO/IEC 27001:2022 und die Notwendigkeit von Änderungen am ISMS, ggf. Aktualisierung der SoA, ggf. Aktualisierung des Risikoermittlungs- und -behandlungsplan, Umsetzung und Wirksamkeit der neuen/ geänderten Normanforderungen und Controls, sofern anwendbar.
- Spätestens ab 1. November 2023 wird DeuZert® die Audits auf Basis der ISO/IEC 27001:2022 anbieten. Allerdings werden reguläre Überwachungsaudits auf Basis der DIN EN ISO/IEC 27001:2017 noch bis spätestens 31. Juli 2025 von DeuZert® durchgeführt.
- Zertifizierungsurkunden gemäß ISO/IEC 27001:2022 werden nur nach nachgewiesener Erfüllung der Anforderungen aus ISO/IEC 27001:2022 ausgestellt.
- Ein bestehender Zertifizierungszyklus von drei Jahren wird von dem Übergang auf ISO/IEC 27001:2022 a priori nicht berührt.
- Gemäß Abschnitt „Weitere Regelungen“, 5. Punkt, führt DeuZert® ein Verzeichnis über die gültigen Zertifizierungen. In diesem Verzeichnis wird auch der zutreffende Zertifizierungsstandard eingetragen. Dies ist jetzt DIN EN ISO/IEC 27001:2017 und nach Übergangsaudit und positiver Zertifizierungsentscheidung ISO/IEC 27001:2022 – die Listung erfolgt also klar getrennt.

Weitere Regelungen

- Die Organisation kann gegen die Benennung eines jeden Auditors 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. Im Verzeichnis werden der Name der zertifizierten Organisationen, der zutreffenden Zertifizierungsstandard, der Geltungsbereich der Zertifizierung, die zertifizierten Standorte und die Gültigkeit des Zertifikats eingetragen. 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, soweit nicht gesetzliche/ behördliche Regelungen dagegenstehen.
- Die Organisation gewährt DeuZert® die Teilnahme von Trainees sowie die Durchführung von Witness-Audits seitens der Akkreditierungsstelle. Zusätzliche Kosten entstehen dem Kunden dadurch nicht.
- Die Organisation hat DeuZert® ohne Verzögerung über Angelegenheiten zu informieren, die die Fähigkeit des ISMS 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 Standorten,
  - des vom zertifizierten ISMS erfassten Tätigkeitsfeldes und
  - wesentlicher Veränderungen des ISMS und der Prozesse und
  - jegliche sonstigen Ereignisse, welche zur Folge haben können, dass Zertifizierungsvoraussetzungen vorübergehend oder dauerhaft nicht mehr vorliegen.