DICIS® Zertifizierungsstandards

Informationen für Kunden des
Digital Institute for Certification of International Standards

Dokumentenhistorie

Revision	Datum	Inhalt	Änderungen durch
23-01	23.05.15	Erstellung des Dokuments	Dr. Jens-Uwe Meyer
23-10	23.05.17	Prüfung und Freigabe	QMB + Vorstand
24-11	01.10.24	Hinzufügen der Anforderungen ISO 14001 + ISO 27001 (Anforderungen ISO 27006)	Dr. Jens-Uwe Meyer
25-10	15.01.25	Prüfung und Freigabe - Veröffentlichung	QMB + Vorstand

Einleitung

Diese Kundeninformation beschreibt das Zertifizierungsverfahren des DICIS Instituts und dient als transparente Orientierung für Unternehmen, die eine Zertifizierung anstreben bzw. als Prozessbeschreibung für deren Kunden. Ziel ist es, die einzelnen Schritte des Verfahrens nachvollziehbar darzustellen und ein klares Verständnis für die zugrunde liegenden Anforderungen zu schaffen.

Das Zertifizierungsverfahren des DICIS Instituts basiert auf den international anerkannten Normen ISO 19011, ISO/IEC 17021 sowie ISO/IEC 27006. Diese Standards legen die Grundlagen für die Auditierung von Managementsystemen, die Kompetenzanforderungen an Zertifizierungsstellen sowie die speziellen Anforderungen für Zertifizierungen im Bereich der Informationssicherheit fest.

Dieses Dokument erläutert, wie diese Anforderungen im Rahmen unseres Zertifizierungsprozesses umgesetzt werden – von der Antragstellung über die Auditplanung und -durchführung bis hin zur Entscheidung über die Zertifikatserteilung und -überwachung.

1. Grundlagen der DICIS-Zertifizierung

Das DICIS-Zertifizierungsverfahren wurde speziell für kleine Dienstleistungsunternehmen mit weniger als 50 Beschäftigten entwickelt. Ziel dieses Verfahrens ist es, eine Zertifizierung zu schaffen, die den besonderen Anforderungen kleiner Organisationen gerecht wird – ohne dabei Kompromisse bei Qualität, Aussagekraft oder Normkonformität einzugehen.

Im Mittelpunkt steht ein effizient gestalteter Zertifizierungsprozess, der praxisnah und verständlich aufgebaut ist. Unternehmen erhalten damit nicht nur eine objektive Bewertung ihrer Managementsysteme, sondern auch konkrete Impulse für Verbesserungen im Unternehmensalltag.

Trotz der kompakten Ausrichtung erfüllt das Verfahren vollständig die Anforderungen der relevanten Normen, insbesondere ISO 19011, ISO/IEC 17021 und ISO/IEC 27006. Diese Normen definieren unter anderem die Anforderungen an Auditprozesse, die Kompetenz von Auditoren sowie spezifische Vorgaben für die Informationssicherheit.

Die DICIS-Zertifizierung steht damit für einen klar strukturierten, ressourcenschonenden und gleichzeitig normgerechten Weg zur Zertifizierung – ideal zugeschnitten auf die Realität kleiner Dienstleistungsunternehmen.

2. Der Zertifizierungsprozess

Der Auditprozess beginnt mit dem Ausfüllen eines Zertifizierungsantrags gem. ISO 17021, Kapitel 9.1.1. Dieser ist über einen digitalen Fragebogen auf der Website dicis.org zugänglich. In diesem Fragebogen macht das Unternehmen grundlegende Angaben zur Betriebsgröße, zum Anwendungsbereich und zur gewünschten Zertifizierung.

Der Antrag wird hinsichtlich der in ISO 17021, Kapitel 9.1.2 aufgelisteten Anforderungen geprüft, DICIS entscheidet über die Annahme des Zertifizierungsantrags. Bei Annahme wird ein Auditprogramm gem. ISO 17021, Kapitel 9.1.3, vereinbart.

Das Unternehmen erhält die Möglichkeit, seine bestehende Dokumentation strukturiert – anhand der Normanforderungen – in ein digitales Tool hochzuladen. Mit diesem digitalen Tool erfüllt DICIS seine Informationspflichten gegenüber Kunden gem. ISO 17021, Kapitel 8.5.1 (Pflicht zur Information über Norm- und Zertifizierungsanforderungen).

Das digitale Tool bietet zudem einen Zugang zum externen KI-Anbieter OpenAI, der Kunden dabei unterstützt, fehlende Dokumente zu erstellen bzw. die Rechtschreibung zu korrigieren. Für die fachliche Richtigkeit und Vollständigkeit der Inhalte bleibt das Unternehmen selbst verantwortlich.

Das **Audit der Stufe 1** wird von Auditoren des DICIS-Instituts durchgeführt – entweder im Vorfeld oder direkt im Anschluss an das Vorgespräch mit dem Management. Dabei werden die Vorgaben gemäß ISO 27006, Kapitel 9.3.2.1 eingehalten. Ziel des Stufe-1-Audits ist eine strukturierte Prüfung der eingereichten Dokumente hinsichtlich Vollständigkeit, Relevanz und normativer Anforderungen. Die Ergebnisse dieses Audits bilden die Grundlage für die Bewertung der grundsätzlichen Zertifizierungsfähigkeit.

Das **Audit der Stufe 2** erfolgt entweder remote oder vor Ort, basierend auf den Vorgaben der Norm ISO 27006 (Kapitel 9.1.1.3) sowie der Analyse des Anwendungsbereichs der Zertifizierung (Kapitel 9.1.3.6). Für das Audit wird ein digitales Audittool genutzt, das strukturierte Fragebögen entsprechend der gewählten Zertifizierungsnorm bereitstellt. Dieses Tool unterstützt eine normkonforme Durchführung des Audits und stellt sicher, dass der in Kapitel 9.3.2.2 geforderte Fokus eingehalten wird. Abweichungen und Feststellungen werden transparent dokumentiert. Über dieses Tool erfolgt auch die Auditplanung.

Die Ergebnisse werden im **Abschlussmeeting** (ISO 17021, Kapitel 9.4) vorgestellt.

Die **Zertifizierungsentscheidung** erfolgt gemäß ISO 17021, Kapitel 9.5 bzw. ISO 27006, Kapitel 9.5.2. Unmittelbar im Anschluss an das Zertifizierungsaudit werden die erforderlichen Überwachungsaktivitäten geplant.

3. Verfahren zur Kalkulation von Auditzeiten

DICIS hat ein dokumentiertes Verfahren zur Kalkulation von Auditzeiten etabliert. Dieses richtet sich nach den Vorgaben der zertifizierungsrelevanten Normen ISO 17021, Kapitel 9.1.4 und ISO 27006 (Tabelle C.1)

Bei der Kalkulation der Auditzeiten für Zertifizierungen nach ISO 27001 wenden wir die im Annex C der ISO 27006 beschriebene Verfahren an. Insbesondere berücksichtigen wir die in Abschnitt C.3.2 genannten Möglichkeiten zur Durchführung von Audits mit Remote-Methoden. Dazu zählen unter anderem interaktive webbasierte Zusammenarbeit, Webmeetings, Telefonkonferenzen sowie die elektronische Überprüfung von Nachweisen. Diese Ansätze ermöglichen eine flexible, effiziente und zugleich normkonforme Durchführung der Audits – insbesondere für kleine Dienstleistungsunternehmen mit begrenzten Ressourcen.

Kalkulation von Auditzeiten

Bei der Kalkulation der Auditzeiten nutzt DICIS die Spielräume, die ISO/IEC 27006 der Zertifizierungsstelle einräumt. Die Normen fordern, dass die in Tabelle C.1 aufgeführten Basis-Auditzeiten nicht isoliert angewendet werden dürfen. Vielmehr

müssen bei der konkreten Kalkulation anpassende Faktoren berücksichtigt werden, die den tatsächlichen Aufwand zur Auditierung eines ISMS beeinflussen.

Bei der Kalkulation der Auditzeiten berücksichtigen wir die besonderen Erfordernisse kleiner, spezialisierte Dienstleistungsunternehmen. Im Vorfeld der Zertifizierung wird geprüft, inwieweit eine oder mehrere dieser Anpassungsfaktoren in einer Weise vorliegen, die eine Reduktion der Auditzeit rechtfertigt. Folgende Faktoren rechtfertigen eine Aufwandsreduktion.

1. Geringe Komplexität des ISMS
Das Informationssicherheitsmanagementsystem ist auf wenige Prozesse und überschaubare Informationswerte ausgerichtet. Es besteht ein niedriges bis moderates Risikoniveau.

2. Standardisierte und klar abgegrenzte Geschäftstätigkeit
Die im Geltungsbereich enthaltenen Tätigkeiten sind einfach strukturiert, wiederkehrend und mit geringem sicherheitsrelevantem Risiko verbunden.

3. Hoher Vorbereitungsgrad und strukturierte Dokumentation
Die Organisation stellt vollständige und gut aufbereitete Unterlagen zur Verfügung. Bei der Erstellung wurden unterstützende Werkzeuge wie KI-basierte Vorlagen eingesetzt.

4. Begrenzte technologische Vielfalt
Es kommen nur wenige IT-Systeme oder Plattformen zum Einsatz, häufig auf Basis gängiger Cloud- oder Standardlösungen. Die IT-Landschaft ist technisch wenig komplex.

5. Geringe externe Abhängigkeiten
Es bestehen nur wenige bis keine Outsourcing-Vereinbarungen oder Integrationen von Drittanbietern, die im Rahmen des Audits berücksichtigt werden müssen.

6. Ein Standort ohne komplexe Notfallinfrastruktur
Die Organisation arbeitet an einem einzigen Standort. Es gibt keine verteilten Systeme, Backup-Rechenzentren oder Desaster-Recovery-Sites, die zusätzlich geprüft werden müssten.

Diese Kriterien werden im Rahmen der Auditplanung berücksichtigt, um eine sachgerechte, normkonforme und aufwandsgerechte Kalkulation der Auditzeit vorzunehmen. Eine Reduktion der Auditzeit erfolgt nur dann, wenn mehrere dieser Kriterien nachweislich erfüllt sind und die Komplexität des Audits dadurch objektiv reduziert wird.

4. Kompetenz eingesetzter Auditoren

DICIS setzt Auditoren auf Grundlage klar definierter Kompetenzkriterien ein, wie sie in den Normen ISO/IEC 17021-1:2015 (Abschnitt 7.1 und 7.2) sowie ISO/IEC 27006-1:2024 (Kapitel 7.1) beschrieben sind. Ziel ist es, sicherzustellen, dass alle an der Zertifizierung beteiligten Personen über die erforderlichen Fähigkeiten verfügen, um Managementsysteme kompetent, objektiv und normkonform zu bewerten. DICIS hat Auswahlkriterien für Auditoren (ISO 17021, Kapitel 9.2.2) definiert.

Das Leitungspersonal des DICIS besteht aus erfahrenen Führungspersönlichkeiten mit abgeschlossener Auditorenausbildung nach ISO 9001, ISO 14001 und ISO/IEC 27001. Alle haben erfolgreich die Prüfung nach den internationalen Anforderungen der IRCA (International Register of Certificated Auditors) abgelegt, einem weltweit anerkannten Standard für Lead Auditoren.

Auditoren, die im Auftrag von DICIS Informationssicherheitsmanagementsysteme (ISMS) auditieren, müssen nachweislich über spezifische Kenntnisse und praktische Fähigkeiten verfügen. Dazu zählen insbesondere Fachwissen in den Bereichen Informationssicherheit, Risikomanagement, technische IT-Kenntnisse, Auditprinzipien sowie ein tiefes Verständnis für die Anforderungen der ISO/IEC 27001 inklusive der Kontrollen aus Anhang A. Diese Kompetenzen müssen nicht nur theoretisch vorhanden sein, sondern im Rahmen von Audits praktisch angewendet werden können. Die Überprüfung und Sicherstellung dieser Kompetenz ist eine durchgehende Verpflichtung des DICIS.

5. Qualitätskriterien

DICIS ist Mitglied im Bundesverband unabhängiger Zertifizierungsstellen (BVUZ) und verpflichtet sich zur Einhaltung der vom Verband festgelegten Qualitätskriterien. Diese Kriterien stellen sicher, dass die Zertifizierungstätigkeit unabhängig, qualitätsgesichert und vertrauenswürdig durchgeführt wird. Auf der Unternehmenswebsite und in den Verträgen wird auf die Qualitätskriterien des BVUZ sowie auf das Beschwerderecht bei Nichteinhaltung hingewiesen.

Als Marke der Innolytics AG ist DICIS eine juristische Person, mit Kunden werden Zertifizierungsvereinbarungen abgeschlossen, DICIS übernimmt die Verantwortung für Zertifizierungsentscheidungen. Damit werden die Vorgaben von ISO 27021, Kapitel 5.1, erfüllt.

Im Bereich Angebot und Vertrag gilt, dass keine Angebote abgegeben werden, wenn daraus eine unangemessene wirtschaftliche Abhängigkeit entstehen könnte oder wenn die Vertragserfüllung über die gesamte Laufzeit nicht sichergestellt ist.

Verträge müssen die Einhaltung aller relevanten Anforderungen über die gesamte Zertifikatslaufzeit gewährleisten und den vollständigen Geltungsbereich der Zertifizierung abdecken.

Für Evaluation, Audit und Prüfung stellt DICIS sicher, dass Entscheidungsfindung und Durchführung klar getrennt sind. Vertraulichkeit aller erlangten Informationen wird gewahrt.

Im Hinblick auf Unabhängigkeit bietet DICIS keine Beratungsleistungen an, die eine Zertifizierung vorbereiten oder begünstigen. Dabei werden die in ISO 17021, Kapitel 3.3 und 5.2, definierten Vorgaben und Kriterien berücksichtigt. Es bestehen keine Mitgliedschaften in Organisationen, die einen unangemessenen Einfluss auf die Unabhängigkeit der Zertifizierung haben könnten.

Im Bereich Kompetenz verpflichtet sich DICIS zur Festlegung von Kompetenzkriterien und stellt die Qualifikation aller beteiligten Personen sicher, die mit Evaluation, Audit, Prüfung und Entscheidungsfindung betraut sind.

Durch die konsequente Einhaltung dieser Qualitätskriterien sichert DICIS die Integrität, Transparenz und Qualität seiner Zertifizierungsverfahren.