UIMCert® GmbH

Ablauf einer Zertifizierung gemäß ISO 27001

Die rechts dargestellten Schritte stellen den Auditierungs-/Zertifizierungsablauf dar. Dieser besteht, neben den formalen Voraussetzungen, aus drei Teilen: Im Stufe-1-Audit findet eine grundsätzliche Betrachtung des Managementsystems auf Basis der Dokumentation als Vorbereitung auf das Stufe-2-Audit dar. Zusätzlich muss zur Bewertung der grundsätzlichen Zertifizierungsfähigkeit des Informationssicherheitsmanagementsystems eine Vor-Ort-Begehung erfolgen. Die Norm sieht vor, dass nach Stufe 1 ein Abbruch des Audits möglich ist, sollte die Dokumentation und/oder andere individuelle Bedingungen dies nahelegen. Auditfeststellungen aus der Stufe 1 werden dokumentiert und Ihnen mitgeteilt, einschließlich der Hinweise zu identifizierten Schwachstellen, die während des Audits der Stufe 2 als Nichtkonformität eingestuft werden könnten.

Die **Stufe 2** beinhaltet das eigentliche Audit in Form eines Vor-Ort-Audits. Hierbei wird die Umsetzung einschließlich der Wirksamkeit des Managementsystems des Kunden unter Berücksichtigung der verschiedenen Standorte bewertet. Auf Basis des abschließenden Prüfberichts wird dann durch die Zertifizierungsstellenleitung die Entscheidung über die Erteilung bzw. Verlängerung des Zertifikats getroffen.

mit Prototypenschutz möglich

Stufe 1	» Dokumentationsprüfung » Grundlegende Feststellung der Zertifizierungsfähigkeit » Durchsprache von evtl. Audit-Findings
Stufe 2	» Überprüfung der Umsetzung der dokumentierten Prozesse » Auditierung der Wirksamkeit des ISMS vor Ort » Durchsprache der Auditergebnisse
Bericht	» Berichtserstellung » ggf. Abstellung von (Haupt-) Abweichungen durch den Auditee
Zertifikat	» Entscheidung über Zertifikatserteilung durch die Leitung der Zertifizierungsstelle
Überwachung	» ggf. Überwachung der Behebung von (Neben-)Abweichungen » Jährliche reguläre Überwachungsaudits

Erstzertifizierungs-Audit
Voraussetzungen

Grundlage eines jeden Audits ist ein eingereichter Antrag auf Zertifizierung sowie ein unterschriebener Vertrag über Zertifizierungsdienstleistungen. Dieser stellt das rechtliche Rahmenwerk für die Erbringung von Zertifizierungsdienstleistungen dar. Darüber hinaus gibt es konkrete inhaltliche Anforderungen.

Die UIMCert darf kein ISMS zertifizieren bevor der Auditee nicht mindestens ein Management Review und ein internes Audit durchgeführt hat. Der Auditee muss ein zertifizierungsnormkonformes, dokumentiertes und implementiertes ISMS betreiben. Die UIMCert darf keine bestimmte Art der Dokumentation des ISMS voraussetzen. Das Erstzertifizierungsaudit setzt sich aus zwei Stufen zusammen.

Stufe 1

In der ersten Auditstufe werden folgende Themen begutachtet:
» Auditierung der Managementsystem-Dokumentation
» Beurteilung der standortspezifischen Bedingungen
» Ermittlung der Bereitschaft für ein Stufe-2-Audit
» Bewertung des Status im Hinblick auf das Verständnis der Normanforderungen, die Identifizierung von Schlüsselleistungen und das Betreiben des ISMS
» Sammlung von Informationen bzgl. des Geltungsbereichs, der Standorte und der zugehörigen gesetzlichen und regulatorischen Aspekte und deren Einhaltung
» Bewertung der Zuteilung der Ressourcen für das Stufe-2- Audit
» Bestimmung der Schwerpunkte für das Stufe-2-Audit
» Beurteilung, ob interne Audits und Managementbewertungen geplant und durchgeführt werden

Dabei geht es in erster Linie darum sich einen Eindruck über die Zertifizierungsreife der jeweiligen Organisation zu verschaffen und aus diesen gewonnenen Informationen nähere Einzelheiten für den zweiten Schritt des Audits zu ermitteln, so dass sich die zweite Phase des Audits und die eingesetzten Ressourcen planen lassen.

Weiterhin werden die Ergebnisse dem Auditee in Form eines schriftlichen Berichts zur Verfügung gestellt und dienen ihm zur Umsetzung der zur Normerfüllung notwendigen Änderungen im Unternehmen. Dabei wird der Auditee auf Findings hingewiesen, die innerhalb des Stufe-2-Audits als Nichtkonformitäten gewertet werden könnten.

Je nach Art und Umfang der im Stufe-1-Audit aufgedeckten Sachverhalte und ggfs. erkannten Findings wird entschieden, ob der Auditee für das Audit der Stufe 2 bereit ist und ob das Stufe-2-Audit sinnvoll durchgeführt werden kann. In Abhängigkeit dieser Ergebnisse wird ein Termin für das Stufe-2-Audit vereinbart.

Stufe 2

Im zweiten Schritt wird die Umsetzung der Normforderungen vor Ort begutachtet und bewertet. Zum Abschluss der beiden Phasen des Audits wird vom Auditteam ein Auditbericht erstellt, welcher später als Grundlage für die Zertifizierungsentscheidung dient.

Folgende Informationen müssen die Auditoren der Leitung der Zertifizierungsstelle zur Verfügung stellen, damit diese eine Entscheidung über die Zertifizierung treffen kann:
» Auditberichte,
» Anmerkungen zu den Nichtkonformitäten und, wo zutreffend, zu Korrekturen und Korrekturmaßnahmen, die von der auditierten Organisation getroffen wurden,
» Bestätigung der an die Zertifizierungsstelle gelieferten Informationen, die in der Antragsprüfung verwendet wurden und
» Empfehlung, ob die Zertifizierung gewährt werden soll (zusammen mit Bedingungen bzw. Beobachtungen).

Überwachungsaudits (periodische Audits)

Zur Überprüfung der Normkonformität finden Überwachungsaudits bei den zertifizierten Organisationen statt. Die Audits sollen mit Ausnahme des Rezertifizierungsaudits je innerhalb eines Kalenderjahres stattfinden; das erste Überwachungsaudit jedoch innerhalb der ersten 12 Monate nach dem Zertifizierungsaudit. Das Überwachungsaudit stellt ein Vor-Ort-Audit dar, bei dem
» die zur Beseitigung der Schwachstellen ergriffenen Maßnahmen bewertet werden.
» eventuelle Beschwerden behandelt werden.
» die Wirksamkeit des Managementsystems überprüft wird.
» festgestellt wird, ob die Fortschritte geplanter Tätigkeiten auf eine ständige Verbesserung abzielen.
» Änderungen, die dem ISMS unterliegen, Änderungen des SoA oder die umgesetzten Maßnahmen bewertet werden.
» die Implementierung, Aufrechterhaltung und Effektivität von Maßnahmen geprüft werden.
» die ordnungsgemäße Nutzung von Zeichen und Zertifizierungsverweisen geprüft wird.
» die Risikobetrachtung überwacht wird.
» interne Audits, die Managementbewertung und korrektive Maßnahmen überwacht werden.

mehr Informationen unter www.uimcert.de

UIMCert® GmbH

Wie kann uns die UIMCert unterstützen?

Als akkreditiertes Unternehmen können wir Ihnen folgende Unterstützung anbieten:

- » Auditierung der Managementsystem-Dokumentation
- » Beurteilung der standortspezifischen Bedingungen
- » Ermittlung der Bereitschaft für Zertifizierungsaudit
- » Begutachtung der Umsetzung der Normforderungen vor Ort
- » Begutachtung der Umsetzung der dokumentierten Verfahren
- » Überprüfung der Leistungsfähigkeit des ISMS

Wenn die Institution nicht weiß, wo Sie qualitativ steht, hat die UIMCert ein Konzept entwickelt, um den Status quo der Institution zu evaluieren. Die UIMCert kann:

- » Prüfung des Fortschritts der Implementierung eines ISMS
- » Ermittlung des Grades der Erfüllung anwendbarer Anforderungen an das ISMS
- » Prüfung der Anwendung und Wirksamkeit des ISMS
- » Identifikation von Sicherheitsschwachstellen
- » Feststellung von Verbesserungspotential

Zu Beginn kann auch gerne zunächst ein Workshop durchgeführt werden, durch den das Projekt, die ausgewählten Normen und die Ziele definiert werden können.

Warum sollte uns gerade die UIMCert unterstützen?

Die UIMCert besitzt als DAkkS akkreditiertes Unternehmen umfangreiche fachliche Kompetenz im Umfeld der Informationssicherheit. Durch unsere qualifizierten ISO 27001 Lead-Auditoren, Auditteamleiter und Datenschutzexperten, die sowohl mit Zertifizierungen und Gütesiegelungen als auch mit Normen und deren Eigenheiten bestens vertraut sind und damit ausführliche Fach- und Methodenkompetenz besitzen, können wir Ihnen praxisgerechte Auditierungen bieten und Sie auf dem Weg zur Zertifizierung unterstützen.

Die UIMCert kennt die Informationssicherheitsmanagementprozesse in Institutionen unterschiedlicher Branchen sehr genau und kennt daher auch die Fallstricke bei den jeweiligen Prozessen und kann gezielt auf die individuelle Situation der Auditees eingehen.

Durch die jahrelange Tätigkeit in diesem Normumfeld und durch Festlegung der genauen Arbeitsschritte können wir mit Ihnen gemeinsam ein klar strukturiertes und transparentes Verfahren durchführen und helfen Ihnen somit, Zeit und damit auch Kosten zu sparen. Die Ergebnisse der Begutachtung werden von uns in einem Bericht zusammengefasst, mit welchem Sie durch die Dokumentation der eventuellen Auditfindings auch gleichzeitig eine Möglichkeit zur Optimierung Ihres ISMS erhalten.

Wer ist die UIMCert?

Die UIMCert GmbH ist ein führendes Unternehmen in den Bereichen Informationssicherheits- und Datenschutzzertifizierung. Wir haben einen unabhängigen Ausschuss, der die Geschäftsführung in wichtigen Fragen im Bereich IT-Management, Informationssicherheit und Datenschutz sowie Zertifizierung berät.

Wir verfügen über qualifiziertes und erfahrenes Personal für die Auditierung und Zertifizierung in den genannten Bereichen. Wir sind bei der „Deutschen Akkreditierungsstelle GmbH“ [DAkkS] für den Standard ISO 27001 (inkl. Prototypenschutz) und für den IT-Sicherheitskatalog gemäß § 11 Absatz 1a Energiewirtschaftsgesetz auf der Grundlage des Konformitätsbewertungsprogramms der Bundesnetzagentur akkreditiert. Auch haben wir beim BSI-lizenzierte Auditoren (BSI Grundschutz) sowie Prüfer für Nachweise gemäß § 8a (3) BSIG [KRITIS] in unseren Reihen.

Wir haben darüber hinaus eigene Prüfsysteme für Informationssicherheit und Datenschutz (datenverarbeitende Stellen und Produkte) aufgebaut, innerhalb derer wir nach erfolgreicher Auditierung gemäß prüfbaren standardisierten Normen ein **eingetragenes Gütesiegel** verleihen.

Welchen Nutzen bringt eine Unterstützung durch die UIMCert?

- » Fach- und Methodenkompetenz im Fachgebiet und in der Ordnungsmäßigkeitsprüfung
- » unabhängige, schnelle und routinierte Prüfung von Verfahren und Konzepten
- » Nutzung eines etablierten Tools zur Effizienz- und Effektivitätssteigerung
- » langjährige Erfahrungen in der Auditierung und Zertifizierung
- » Rückgriff auf Best-Practice-Lösungen und -Vorgehensweisen
- » hohe Qualität durch langfährig festangestellte, eigene Auditoren

Fragen?
Interesse?

Dann zögern Sie nicht
und sprechen uns an:
(0202) 946 7726 300
certification@uimcert.de

UIMCert® GmbH

Unternehmens- und Informations-Management Certification

UIMCert GmbH + Otto-Hausmann-Ring 113 + 42115 Wuppertal + Tel: (0202) 946 7726 300 + Mail: certification@uimcert.de + Internet: www.UIMCert.de

Zertifizierung nach ISO 27001
Informationssicherheits-Managementsystem

inkl. Prototypenschutz möglich

Nutzen einer Zertifizierung

Verbesserung der Informationssicherheit

Erhöhung des Imagewertes in Sachen Sicherheit
bei den Mitarbeitern und bei externen Bezugsgruppen

Publicity-wirksames Zeugnis über die Qualität
in der Informationssicherheit

Erlös- und Gewinnzuwächse durch Vertrauenserhöhung
bei umsatzrelevanten Bezugsgruppen

Vermeidung/Reduzierung von Kunden-Audits

akkreditiert bei
DAkkS Deutsche Akkreditierungsstelle D-ZM-17294-01-01