DIN EN ISO/IEC 27001:2017

Anfrage

Per E-Mail an: kundendienst@deuzert.de oder per Fax an: +49 3375 217459-19

DeuZert® Deutsche Zertifizierung in Bildung und Wirtschaft GmbH

Hochschulring 2, 15745 Wildau

Art der Anfrage		
Anfrage auf Erst-Zertifizierung		
Firmensitz / Hauptzentrale der Organisation		
Organisation:		
Anschrift:		
Geschäftsführung:	Vorname, Name:	
Telefon / Fax:		
Internet:		
Rechnungsanschrift (wenn Anschrift von oben abweichend)		
Organisation:		
Anschrift:		
HauptansprechpartnerIn		
Vorname, Name:		
Funktion:		
Anschrift:		
Telefon / Fax:		
E-Mail:		

Informationen über die Organisation		
Welche Produkte und/oder Dienstleistungen bietet die Organisation an?		
In welchen Bereichen sind die Kunden vertreten (z. B. Datenverarbeitung, Automobilindustrie, usw...)?		
Hat die Organisation bei der Entwicklung des Informationssicherheitsmanagementsystems (ISMS) gemäß DIN EN ISO/IEC 27001:2017 die Unterstützung eines externen Beraters/Beratungsunternehmens in Anspruch genommen?		
☐ Ja	Name des Beraters **und** der Beratungsgesellschaft	
☐ Nein		
Werden nicht zutreffende Anforderungen/ Ausschlüsse zur DIN EN ISO/IEC 27001:2017 geltend gemacht?		
☐ Ja	Welche? Bitte Risikoakzeptanzkriterien angeben.	
☐ Nein		
Gibt es ISMS-relevante Bereiche in Ihrem Unternehmen, die dem Auditteam aus Geheimhaltungsgründen nicht zugänglich gemacht werden können?		
☐ Ja	Welche? Bitte angeben.	
☐ Nein		

Grunddaten des Informationssicherheitsmanagementsystems (ISMS)		
Werden die Geschäftsprozesse der Organisation rechnergestützt abgewickelt?	☐ Ja	☐ Nein
Unterliegt die Organisation verstärkten Forderungen bzgl. des Datenschutzes (Geheimhaltung, Verwaltung personenbezogener Daten)?	☐ Ja	☐ Nein
Betreibt die Organisation aus Gründen der Datensicherheit „getrennte“ (dedizierte) Systeme?	☐ Ja	☐ Nein
Verwaltet die Organisation externe Daten?	☐ Ja	☐ Nein

Informationssicherheitsanforderungen (Vertraulichkeit, Integrität, Verfügbarkeit):	☐ Viele sensitive/ vertrauliche Informationen; hohes Anforderungsniveau.	☐ Eine Reihe von sensitiven/ vertraulichen Informationen; mittleres Anforderungsniveau.	☐ Wenig sensitive/ vertrauliche Informationen; geringes Anforderungsniveau.
Anzahl kritischer Vermögenswerte bzgl. Vertraulichkeit, Integrität, Verfügbarkeit:	☐ Viele kritische Vermögenswerte.	☐ Eine Reihe von kritischen Vermögenswerten.	☐ Wenige kritische Vermögenswerte.

Informationen über die Organisation			
Anzahl Prozesse und Services:	☐ Mehr als 2 komplexe Geschäftsprozesse mit vielen Schnittstellen und einbezogenen Geschäftseinheiten.	☐ Bis 3 einfache Geschäftsprozesse mit wenigen Schnittstellen und einbezogenen Geschäftseinheiten.	☐ Ein Hauptgeschäftsprozess mit wenigen Schnittstellen und einbezogenen Geschäftseinheiten.
Geschäftsrisiko innerhalb des Anwendungsbereiches des ISMS:	☐ Hohes Geschäftsrisiko.	☐ Mittleres Geschäftsrisiko mit höheren regulatorischen Anforderungen.	☐ Niedriges Geschäftsrisiko ohne regulatorische Anforderungen.
Umfang und Vielfalt von genutzter IT-Technologie und -Umgebung:	☐ Hohe Vielfalt oder Komplexität der IT-Umgebung.	☐ Standardisierte IT-Umgebung mit vielfältigen IT-Plattformen, Servern, Betriebssystemen, Datenbanken & Netzwerken.	☐ Hoch standardisierte IT-Umgebung mit wenig Vielfalt.
Umfang des Outsourcing an externe Dienstleister innerhalb des Anwendungsbereiches des ISMS:	☐ Hohe Abhängigkeit von Outsourcing <u>oder</u> Lieferanten mit hohem Einfluss auf wichtige Geschäftsaktivitäten.	☐ Teilweises Outsourcing.	☐ Kein Outsourcing und geringe Abhängigkeit von Lieferanten <u>oder</u> gut etabliertes bzw. überwachtes Outsourcing mit zertifizierten ISMS beim Lieferanten.
Umfang der Systementwicklung:	☐ Umfangreiche interne Software-Entwicklung in verschiedenen laufenden Projekten für wichtige Geschäftsanwendungen.	☐ Systementwicklung unter Nutzung standardisierter Software-Plattformen mit komplexer Konfiguration; kundenspezifische Softwarelösungen.	☐ Keine Inhouse-Systementwicklung mit Nutzung standardisierter Software-Plattformen.
Anzahl der Notfallwiederherstellungsstandorte (Disaster recovery sites):	☐ Hohe Anforderung (24/7) mit verschiedenen Notfallwiederherstellungs standorten und Datencentern.	☐ Mittlere Anforderung und max. 1 Notfallwiederherstellungsstandort.	☐ Keine Anforderung und max. 1 Notfallwiederherstellungsstandort.
Anzahl aller Mitarbeitenden (Vollzeitäquivalent) im Anwendungsbereich des Informationssicherheitsmanagementsystems:			
Anzahl aller zu berücksichtigenden Mitarbeitenden, mit denen sonstige vertraglichen Vereinbarungen bestehen (z. B. Honorarbeschäftigte):			
Anzahl der Mitarbeitenden:	☐ ≥ 1.000	☐ ≥ 200	☐ < 200
Anzahl der Mitarbeitenden, die die IT-Systeme pflegen/ administrieren:	☐ ≥ 100	☐ ≥ 20	☐ < 20
Anzahl der Standorte:	☐ ≥ 5	☐ 2 bis 4	☐ 1

DIN EN ISO/IEC 27001:2017

Anfrage

Wie viele **Standorte**[1] sollen insgesamt zertifiziert werden? *Bitte pro Standort unser Formular „Anfrage / Angaben zum Standort“ (WP04 I F01a) ausfüllen.*	

Eine **Verbundzertifizierung**[2] ist nur möglich, wenn folgende Punkte zutreffen:	
☐	Die Organisation wendet ein einziges Informationssicherheitsmanagementsystem für alle Standorte an.
☐	Die Organisation weist eine Zentrale als Teil der Organisation auf (nicht notwendigerweise der Hauptsitz der Organisation; nicht unbedingt ein einzelner Standort).
☐	Die Zentrale hat die organisatorische Befugnis, das Informationssicherheitsmanagementsystem zu definieren, einzuführen und zu pflegen.
☐	Das Informationssicherheitsmanagementsystem unterliegt einer zentralen Überprüfung durch die oberste Leitung der Organisation.
☐	Alle Standorte unterliegen dem internen Auditprogramm der Organisation.
☐	Die Zentrale stellt sicher, dass Daten von allen Standorten erhoben und analysiert werden. Sie kann nachweisen, dass sie in dieser Hinsicht die Befugnis und Fähigkeit zur Einleitung organisatorischer Änderungen u.a. zu Folgendem besitzt: • Managementsystemdokumentation und dessen Veränderungen, • Managementbewertung, • Behandlung von Beschwerden, • Bewertung von Korrekturmaßnahmen, • Planung interner Audits mit Bewertung der Ergebnisse sowie • Berücksichtigung/ Einhaltung gesetzlicher/ behördlicher Anforderungen in Bezug auf DIN EN ISO/IEC 27001:2017.

Die Mitglieder des Unternehmensverbunds werden in einem Referenzauswahlverfahren auditiert. Bei der Stichprobenwahl in einer Verbundzertifizierung ist zu beachten, dass es Standorte mit ähnlichen/ vergleichbaren Prozessen/ Tätigkeiten/ Produkten gibt, aber auch Standorte mit im Wesentlichen unterschiedlichen Prozessen/ Tätigkeiten/ Produkten. Daher müssen uns je Standort die dort vorhandenen Prozesse/ Tätigkeiten zur Kenntnis gebracht werden.
Bitte pro Standort unser Formular „Antrag – Anfrage – Angaben zum Standort“ (WP04 - F01a) ausfüllen.

1 An einem festen Standort führt die Organisation fortlaufend Arbeiten oder Dienstleistungen einschließlich damit verbundener bzw. angegliederter Tätigkeiten aus. An einem virtuellen Standort führt die Organisation mit Hilfe einer Online-Umgebung Arbeiten aus oder erbringt Dienstleistungen auf der Grundlage von Prozessen von physischen Standorten. Ein virtueller Standort gilt zur Bestimmung der Auditzeit als ein einzelner Standort.

2 Die Zertifizierung einer Organisation mit einem Informationssicherheitsmanagementsystem an mehreren Standorten.

DIN EN ISO/IEC 27001:2017

Anfrage

Falls Änderung des Geltungsbereiches einer bestehenden Zertifizierung			
Zertifikat-Registrier-Nr.:		Ausstellungsdatum:	
Bitte beschreiben Sie die Änderung:			
Weitere abschließende Angaben.			
Sollen alle Standorte auf einem Zertifikat aufgeführt werden?		Ja	
Geben Sie uns bitte Ihren Vorschlag für den Zertifikatstext als Formulierung Ihres Anwendungsbereiches – nach erfolgreicher Auditierung:			
Gewünschter Audittermin (KW Jahr):			
Ort, Datum:			
Vorname, Name:			
Unterschrift für die Richtigkeit der Angaben:			

Vielen Dank für Ihre Mühe.