ISO/IEC 27001:2022

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		
Firmensitz / Hauptzentrale des Unternehmens		
Firma:		
Anschrift:		
Geschäftsführung:	Vorname, Name:	
Telefon / Fax:		/
Internet:		
Rechnungsanschrift (wenn Anschrift von oben abweichend)		
Firma:		
Anschrift:		
Hauptansprechpartner:in		
Vorname, Name:		
Funktion:		
Anschrift:		
Telefon / Fax:		/
E-Mail:		

Informationen über Ihr Unternehmen		
Welche Produkte und/oder Dienstleistungen bietet Ihr Unternehmen an?		
In welchen Bereichen sind die Kunden vertreten (z. B. Datenverarbeitung, Automobilindustrie, usw.)?		
Hat das Unternehmen bei der Entwicklung des Informationssicherheitsmanagementsystems (ISMS) gemäß ISO/IEC 27001:2022 die Unterstützung eines externen Beraters/Beratungsunternehmens in Anspruch genommen?		
☐ Ja	Name des Beraters und der Beratungsgesellschaft:	
☐ Nein		
Werden nicht zutreffende Anforderungen zur ISO/IEC 27001:2022 geltend gemacht?		
☐ Ja	Welche? Bitte Risikoakzeptanz-kriterien 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 Ihres Unternehmens rechnergestützt abgewickelt?		☐ Ja	☐ Nein
Unterliegt Ihr Unternehmen verstärkten Forderungen bzgl. des Datenschutzes (Geheimhaltung, Verwaltung personenbezogener Daten)?		☐ Ja	☐ Nein
Betreibt Ihr Unternehmen aus Gründen der Datensicherheit „getrennte“ (dedizierte) Systeme?		☐ Ja	☐ Nein
Verwaltet Ihr Unternehmen externe Daten?		☐ Ja	☐ Nein
Informationssicherheits-anforderungen (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.
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 Outsourcings an externe Dienstleister innerhalb des Anwendungsbereiches des ISMS:	☐ Hohe Abhängigkeit von Outsorcing <u>oder</u> Lieferanten mit hohem Einfluss auf wichtige Geschäftsaktivitäten.	☐ Teilweises Outsorcing.	☐ Kein Outcourcing und geringe Abhängigkeit von Lieferanten <u>oder</u> gut etabliertes bzw. überwachtes Outsorcing 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 Notfallwiederherstellungsstandorten und Datencentern.	☐ Mittlere Anforderung und max. 1 Notfallwiederherstellungsstandort.	☐ Keine Anforderung und max. 1 Notfallwiederherstellungsstandort.

Anzahl aller Mitarbeitenden (**Vollzeitäquivalent**) im Anwendungsbereich des Informationssicherheitsmanagementsystems:			
… davon Anzahl Mitarbeitende mit identischen Tätigkeiten, ...			
➔ davon Mitarbeitende mit reinem Informationslesezugriff			
➔ davon Mitarbeitende ohne Zugang zu informationsverarbeitenden Einrichtungen			
➔ davon Mitarbeitende mit einem spezifisch, nachweislich eingeschränkten Zugang zu informationsverarbeitenden Einrichtungen			
➔ davon Mitarbeitende mit strengen Beschränkungen für die Weitergabe von Informationen, z.B. und nicht ausschließlich Verbot des Mitbringens von persönlichen Gegenständen und Geräten in den Arbeitsbereich			
Anzahl aller 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

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 ISO/IEC 27001:2022.

Die Standorte des Unternehmensverbunds <u>können</u> in einem Stichprobenverfahren auditiert werden. 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.*	
☐	**Stichprobenverfahren bei der Verbundzertifizierung wird gewünscht.** [3] Gründe:

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.

3 <u>Anderenfalls werden jährlich alle Standorte des Unternehmensverbundes auditiert</u> (Regelfall).

Falls Änderung des Geltungsbereiches einer bestehenden Zertifizierung			
Zertifikat-Registrier-Nr.:		Ausstellungsdatum:	
Bitte beschreiben Sie die Änderung [4]:			
Weitere abschließende Angaben			
Sollen alle Standorte auf einem Zertifikat aufgeführt werden?			
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:			

4 Handelt es sich um eine **Erweiterung des Anwendungsbereiches**, machen Sie bitte zu folgenden Faktoren dezidiert Angaben:
a) der Art der Erweiterung;
b) der Tätigkeit(en) der aktuellen Zertifizierung in Bezug auf die Erweiterung;
c) der Anzahl der Standorte, an denen die Tätigkeit(en) verrichtet wird/werden;
d) der mit der/den Tätigkeiten(en) verbundenen Informationssicherheitsrisiken;
e) der Anzahl der für die Erweiterung relevanten Maßnahmen/ Controls aus Anhang A der ISO/IEC 27001:2022;
f) der Anzahl der Mitarbeitenden im neuen Anwendungsbereich; und
g) Ihr Zeitaufwand für die Überprüfung der Integration des erweiterten Anwendungsbereichs in das ISMS (interne Audits etc.).

Bitte füllen Sie diese Seite für jeden Standort[5] separat aus.		
Firmensitz:		
Anschrift des Standortes		
Firma:		
Anschrift.:		
Vorhandene Zertifizierungen am Standort ***(Bitte fügen Sie die aktuellen Zertifikate als Kopie bei).***		
Standard	Zertifizierungsstelle	Gültig bis
☐ ISO/IEC 27001:2022		
☐ DIN EN ISO 9001:2015		
☐ DIN ISO 21001:2021		
☐ Sonstiges:		
Anzahl aller Mitarbeitenden **(Vollzeitäquivalent[6])** an diesem Standort, im Geltungsbereich der angefragten Zertifizierung**:**		
… davon Anzahl Mitarbeitende mit identischen Tätigkeiten an diesem Standort, ...		
➔ davon Mitarbeitende mit reinem Informationslesezugriff an diesem Standort		
➔ davon Mitarbeitende ohne Zugang zu informationsverarbeitenden Einrichtungen an diesem Standort		
➔ davon Mitarbeitende mit einem spezifisch, nachweislich eingeschränkten Zugang zu informationsverarbeitenden Einrichtungen an diesem Standort		
➔ davon Mitarbeitende mit strengen Beschränkungen für die Weitergabe von Informationen an diesem Standort, z.B. und nicht ausschließlich Verbot des Mitbringens von persönlichen Gegenständen und Geräten in den Arbeitsbereich		
Gibt es Mitarbeitende im Schichtbetrieb an diesem Standort?		
☐ Ja	Anzahl der Schichten	
☐ Nein		

5 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.

6 Anzahl der Mitarbeitenden ohne Auszubildende und ohne Praktikanten angeben.
Mitarbeitende in Teilzeit sind in Vollzeitäquivalent zu berechnen.

Welche Tätigkeiten und Prozesse gibt es am Standort?	
Angaben zur vorhandenen IT-Infrastruktur am Standort	
Anzahl der PCs/ Laptops:	
Anzahl der Server:	
Anzahl der aktiven Netzwerkkomponenten:	
Anzahl der internen Netzwerke bzw. Netzwerkzweige:	
Anzahl der externen Dienstleister:	
Weitere Anmerkungen *(z. B. temporärer Standort).*	

Vielen Dank für Ihre Mühe.