

# Antrag auf eine Zertifizierung

Dieses Formblatt dient dem Einholen von Informationen und relevanten Kennzahlen über das zu zertifizierende Unternehmen. Diese Datenerhebung ist wichtig für das Zertifizierungsinstitut für Informationssicherheit Dr. Scharff GmbH (ZIS), um eine Bewertung durchführen zu können, inwiefern eine Zertifizierung für den angegebenen Geltungsbereich realisierbar ist. Des Weiteren dienen die Informationen zur Erstellung eines kostenfreien und unverbindlichen Angebotes. Mit der Einreichung dieses Antrages entsteht somit kein rechtsverbindliches Vertragsverhältnis.

## 1 Datenschutz und Vertraulichkeit

Alle Informationen und Aufzeichnungen, die wir vom Antragsteller erhalten, werden von uns vertraulich behandelt. Für Daten und Informationen, die dem Datenschutz unterliegen (personenbezogene oder –beziehbare Daten bzw. Informationen), werden unsererseits die Vorgaben des Gesetzgebers zum Datenschutz, insbesondere die Europäische Datenschutz-Grundverordnung (DS-GVO), das Bundesdatenschutzgesetz (BDSG) und die Datenschutzgesetze der Länder (LDSG) beachtet.

ZIS ist daneben verpflichtet, keine Informationen offenzulegen oder an Dritte weiterzuleiten ohne schriftliches Einverständnis der antragstellenden Organisation.

Auskünfte über den Status Ihrer laufenden Zertifizierung bekommen Sie gerne, kontaktieren Sie uns dazu jederzeit.

## 2 Offenlegung von Informationen

ZIS wird durch die Deutsche Akkreditierungsstelle GmbH (DAkkS, nationale Akkreditierungsbehörde) überwacht. Somit können Begutachtungen der vertraulichen Dokumentation der Zertifizierung (z.B. Auditpläne, Zertifizierungsverträge) seitens dieser genannten Behörde vorgenommen werden. Der zu zertifizierende Kunde wird von ZIS über diese Offenlegung unterrichtet, sofern kein gesetzliches Verbot dagegen spricht.

ZIS ist außerdem gemäß DIN EN ISO/IEC 17021, Kap. 8.1.2 verpflichtet, folgende Informationen des Antragstellers auf Anfrage zur Verfügung zu stellen:

- Informationen zum Status einer erteilten Zertifizierung
- Informationen zum Namen des Unternehmens, einschlägigen normativen Dokumenten, dem Geltungsbereich und dem Standort (Stadt, Land) eines zertifizierten Kunden

In Ausnahmefällen kann auf Kundenwunsch der Zugang zu bestimmten Informationen beschränkt werden.

Mit Bezug auf DIN EN ISO/IEC 17021, Kap. 8.4 wird ZIS den Antragsteller benachrichtigen, bevor Informationen frei zugänglich gemacht werden.

### 3 Informationen über das zu zertifizierende Unternehmen

Die mit \* gekennzeichneten Felder sind Pflichtfelder und müssen ausgefüllt werden. Das zu zertifizierende Unternehmen bestätigt mit diesem Antrag, dass das Unternehmen über ein dokumentiertes und implementiertes ISMS verfügt, welches ISO/IEC 27001 und andere für die Zertifizierung erforderlichen Dokumente erfüllt.

Den Antrag muss von einem bevollmächtigten Vertreter der antragsstellenden Organisation ausgefüllt werden.

#### 3.1 Allgemeine Angaben

##### 3.1.1 Firmensitz / Geographischer Ort des Hauptsitzes der Organisation

Firmenbezeichnung*	
Straße *	
PLZ und Ort *	
Land *	
Branche * (z.B. Energieversorger...)	
Name der Geschäftsführung	
E-Mail-Adresse *	
Telefonnummer*	
Webauftritt	

##### 3.1.2 Hauptansprechpartner Zertifizierung / ISB

Anrede *	<input type="checkbox"/> Frau <input type="checkbox"/> Herr
Titel	
Vorname	
Name *	
Position *	
E-Mail-Adresse *	
Telefonnummer *	

##### 3.1.3 Terminwunsch (Datum bzw. KW der Auditierung) \*:

--

## 3.2 Basisangaben zum Managementsystem

### 3.2.1 Angestrebte Zertifizierung \*

☐ ISO/IEC 27001:2022

Weitere zu berücksichtigende normative Dokumente, Richtlinien, Regeln, Vorschriften, vertragliche Regelungen, etc. (DSGVO, IT-Sicherheitsgesetz, Energiewirtschaftsgesetz, ...):

Ist das Unternehmen bereits nach der angestrebten Norm zertifiziert? \*

☐ **Ja**, bis (Gültigkeitsdatum): \_\_\_\_\_

Hiermit wird beantragt (zutreffendes ankreuzen):

☐ Überwachungsaudit

☐ Re-Zertifizierung

☐ Erweiterung des Geltungsbereichs

☐ Übernahme einer bestehenden Zertifizierung

☐ **Nein**, das Unternehmen beantragt eine Erstzertifizierung nach o.g. angestrebter Zertifizierung

**Bitte führen Sie im Anhang hinten alle Standorte auf, die bereits nach der angestrebten Norm zertifiziert sind.**

### 3.2.2 Kurzfassung: Gewünschter Geltungsbereich des Zertifikats\*

Bitte geben Sie hier den eindeutigen und unmissverständlichen Geltungsbereich der Zertifizierung im Hinblick auf Tätigkeiten, Produkte und Dienstleistungen an. **Dieser Text wird ins Zertifikat übernommen und muss eine Kurzbeschreibung der Unternehmenstätigkeit und der Prozesse sein.**

### 3.2.3 Anzahl der Standorte im Geltungsbereich nach DIN EN ISO/IEC 27001 \*

Bitte nur die für die Zertifizierung relevanten Standorte aufführen, d.h. die, die für den Geltungsbereich der Zertifizierung relevant sind.

Multi-Site-Zertifizierung:

ZIS entwickelt ein Auditprogramm gemäß den Vorgaben des IAF MD 1 zur Stichprobenprüfung, damit eine ordnungsgemäße Überprüfung des Managementsystems sicherstellt ist.

Im Anschluss prüft und dokumentiert ZIS im Stufe-1 Audit, ob und inwiefern die Voraussetzungen für ein Multisite-Verfahren gemäß IAF MD1 eingehalten sind. Die Zertifizierungsdokumente müssen daher alle Standorte im Geltungsbereich des Unternehmens ausweisen.

Zentrale (Name und Ort)	
Gesamtanzahl Standorte	
<b>Falls mehr als 1 Standort:</b>	
<b>Bitte führen Sie hinten im Anhang auf: Bezeichnung und Adressen aller Standorte innerhalb des Geltungsbereichs mit Angabe der Prozesse, Tätigkeiten, Anwendungen und Systeme</b>	
<u>Falls mehr als ein Standort:</u> Führen die Standorte sehr ähnliche Prozesse oder Tätigkeiten aus?	<input type="checkbox"/> Ja <input type="checkbox"/> Nein <input type="checkbox"/> Ja, allerdings nur an den Standorten:
<u>Falls mehr als ein Standort:</u> Davon dauerhaft besetzte Standorte	
<u>Falls mehr als ein Standort:</u> Davon nicht dauerhaft besetzte Standorte ( <i>diese Standorte werden nicht auf dem Zertifikat gelistet</i> )	

### 3.2.4 Anzahl der Mitarbeiter im Geltungsbereich \*

Gesamtanzahl Mitarbeitende inkl. Geschäftsführung, wichtig: bitte Zahl der Mitarbeitenden in FTE (=Vollzeitäquivalenten) angeben:

\_\_\_\_\_ FTE

Davon die Vollzeitäquivalente, die effektiv am ISMS mitwirken: \_\_\_\_\_ **FTE**

*Hier sind die Mitarbeitenden in FTE gemeint, die im ISMS-Prozess mitwirken oder ISMS-tätig sind bzw. in dem Bereich Rollen besitzen: CISO/ ISB, GF, IT-Leiter, ...*

*Diese Mitarbeitenden wirken aktiv beim Aufbau und auch bei der Umsetzung (z.B. in der IT) eines wirksamen ISMS mit (wie das ISMS-Team zusammen mit dem IT-Team).*

*Nicht dazu gehören Personen, die zwar im Geltungsbereich (also zur gesamt-FTE zählen) liegen, die aber keine „aktive“ Rolle haben (wie Poststelle, Consulting, Produktion, ....).*

**Besonderheiten:**

*z.B. Anzahl aller Schichtarbeiter in wieviel Schichten (bitte auch die Zeiten der Schichten angeben)*

*Fahrpersonal, Anzahl Mitarbeiter im Außendienst, Anzahl Hilfskräfte, Anzahl Zeitarbeitskräfte, Anzahl Mitarbeiter in geringfügiger Beschäftigung, Anzahl nicht fest angestellter Mitarbeiter (z.B. Vertragspartner)*

**Falls mehr als 1 Standort im Geltungsbereich liegt:**

Verteilung der Vollzeitäquivalente (FTE) an den jeweiligen Standorten:

Standortbezeichnung	FTE


### 3.2.5 Inanspruchnahme von Beratungsleistungen bzgl. des zu zertifizierenden Managementsystems \*

Werden oder wurden Sie beim Aufbau des zu zertifizierenden Managementsystems extern beraten?

*(Diese Angabe ist notwendig für eine unabhängige/unparteiliche Durchführung der Zertifizierung, z.B. darf der Beratende nicht als Auditor eingesetzt werden.)*

☐ **Ja**

Name der Beratungsgesellschaft:

Name des/der Berater(s):

☐ **Nein**

## 3.3 Detailangaben zum Managementsystem

*Die nachfolgenden Angaben dienen einer möglichst realistischen und genauen Abschätzung des notwendigen Auditzeitaufwands. Je detaillierter die Angaben erfasst werden, desto genauer lässt sich der Aufwand bestimmen. Keine oder unrichtige Angaben erhöhen demzufolge ebenso das Risiko einer Fehleinschätzung des benötigten Aufwands.*

### 3.3.1 Bestehende Zertifizierung anderer betriebener Managementsysteme \*

☐ **Ja**

Auflistung der zertifizierten Managementsysteme (inkl. Norm); bitte Zertifikate anfügen:

☐ **Nein**

3.3.2 Auflistung aller ausgegliederten Aktivitäten (Prozesse, Dienstleistungen, ...) innerhalb des Geltungsbereichs, falls vorhanden \*

3.3.3 Sind Ausschlüsse vorhanden? Bitte listen Sie diese auf:

### 3.3.4 Geschäftskomplexität: Mit dem Geschäft und der Organisation zusammenhängende Faktoren (ohne IT) \*

Bitte setzen Sie nur 1 Kreuz in jeder Kategorie. Kreuzen Sie das Kästchen an, das die höchste zutreffende Relevanz für Ihr Unternehmen hat.

Kategorie	Einteilung
Art(en) der Geschäfte und behördliche Anforderungen	<input type="checkbox"/> Die Organisation arbeitet in nicht kritischen Geschäftsfeldern und unregulierten Branchen. <input type="checkbox"/> Die Organisation hat Kunden in kritischen Geschäftsfeldern. <input type="checkbox"/> Die Organisation arbeitet in kritischen Geschäftsfeldern.  <i>Diese Frage zielt nicht darauf ab, ob das Unternehmen zu den KRITIS-Unternehmen im Sinne der IT-Sicherheitsgesetzgebung (IT-SiG 2.0) und der BSI KRITIS-Verordnung (BSI-KritisV) zählt. Hier ist der Schutzbedarf von Informationen und Systemen einzubeziehen.</i>  <i>Bsp: Bei Dienstleistungen mit hohem Schutzbedarf hinsichtlich der Vertraulichkeit, Integrität und /oder der Verfügbarkeit ist davon auszugehen, dass es sich dabei um Services mit hoher Kritikalität handelt. Daher muss das Kreuz gesetzt werden bei „Die Organisation arbeitet in kritischen Geschäftsfeldern“.</i>
Prozesse und Aufgaben	<input type="checkbox"/> Standardprozesse mit genormten und sich wiederholenden Aufgaben; viele im Auftrag der Organisation tätige Personen, die dieselbe Aufgabe ausführen; wenige Produkte oder Dienstleistungen <input type="checkbox"/> Standardprozesse, die sich nicht wiederholen mit einer hohen Anzahl von Produkten oder Dienstleistungen <input type="checkbox"/> Komplexe Prozesse, hohe Anzahl von Produkten und Dienstleistungen, viele Geschäftseinheiten im Geltungsbereich der Zertifizierung (das ISMS deckt sehr komplexe Prozesse oder eine hohe Anzahl von Tätigkeiten oder einzigartige Tätigkeiten ab)
Grad der Etablierung des Managementsystems	<input type="checkbox"/> Das ISMS ist bereits gut etabliert und/oder es stehen andere Managementsysteme bereit. <input type="checkbox"/> Einige Elemente anderer Managementsysteme wurden implementiert, andere nicht. <input type="checkbox"/> Kein anderes Managementsystem wurde implementiert, das ISMS ist neu und nicht etabliert.



### 3.3.5 IT-Komplexität: Mit der IT-Umgebung zusammenhängende Faktoren \*

Bitte setzen Sie nur 1 Kreuz in jeder Kategorie. Kreuzen Sie das Kästchen an, das die höchste zutreffende Relevanz für Ihr Unternehmen hat.

Kategorie	Einteilung
Komplexität der IT-Infrastruktur	<input type="checkbox"/> Wenige oder stark genormte IT-Plattformen, Server, Betriebssysteme, Datenbanken, Netzwerke usw. <input type="checkbox"/> Mehrere unterschiedliche IT-Plattformen, Server, Betriebssysteme, Datenbanken, Netzwerke <input type="checkbox"/> Viele verschiedene IT-Plattformen, Server, Betriebssysteme, Datenbanken, Netzwerke
Abhängigkeit von Ausgliederung und Lieferanten, einschließlich Cloud-Dienstleistungen	<input type="checkbox"/> Geringe oder keine Abhängigkeit von Ausgliederung oder Lieferanten <input type="checkbox"/> Einige Abhängigkeit von Ausgliederung oder Lieferanten, mit einigen, aber nicht allen wichtigen Geschäftstätigkeiten zusammenhängend <input type="checkbox"/> Hohe Abhängigkeit von Ausgliederung oder Lieferanten, erhebliche Auswirkungen auf wichtige Geschäftstätigkeiten
Informationssystementwicklung	<input type="checkbox"/> Keine oder sehr eingeschränkte interne System-/Anwendungsentwicklung <input type="checkbox"/> Einige interne oder ausgegliederte System-/Anwendungsentwicklung für einige wichtige Geschäftszwecke <input type="checkbox"/> Umfassende interne oder ausgegliederte System-/Anwendungsentwicklung für einige wichtige Geschäftszwecke

3.4 Gibt es Bereiche (ISMS-Aufzeichnungen, etc.), die nicht auditert werden können, da sie vertrauliche oder sensible Informationen enthalten?

Bitte fügen Sie diesem Antrag die folgenden beiden Anlagen als dokumentierte Informationen bei\*:

- ✓ Den ausführlichen Geltungsbereich des Informationssicherheitsmanagementsystems
- ✓ Die Anwendbarkeitserklärung (SoA).

☐ falls zutreffend: Ausgefüllter Anhang ist beigelegt (siehe Kap. 3.2.1 und 3.2.3)

3.5 Dieser Antrag wurde ausgefüllt von:

\_\_\_\_\_  
Name, Vorname der/des Bevollmächtigten:

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Unterschrift

## Anhang

Zu Kapitel 3.2.1:

### **Angestrebte Zertifizierung**

*Bitte führen Sie alle Standorte auf, die bereits nach der angestrebten Norm zertifiziert sind. Bitte Zertifikat beilegen.*

Zu Kapitel 3.2.3:

### **Anzahl der Standorte im Geltungsbereich nach DIN EN ISO/IEC 27001**

*Bezeichnung und Adressen aller Standorte innerhalb des Geltungsbereichs mit Angabe der Prozesse, Tätigkeiten, Anwendungen und Systeme*

Bezeichnung Standort	Adresse	Prozesse, Tätigkeiten, Anwendungen und Systeme

[illegible]