Fragebogen zur Angebotserstellung

FAX: +49 6151 600336 / E-Mail: proficert@tuevhessen.de

Dieser Fragebogen dient zur Sammlung von Informationen durch die Zertifizierungsstelle im Rahmen der Angebotserstellung und –prüfung zur Vorbereitung auf den Zertifizierungs- und Auditprozess und ist Bestandteil der Verfahrensdokumentation (gemäß ISO/IEC 17021-1:2015, 9.1.1/2 u. ISO/IEC 27006:2015, 9.1.1.1, 9.1.4).

Gewünschtes Regelwerk

☐ **ISO/IEC 27001:2013**

☐ **ISO/IEC 27001:2013 mit den zusätzlichen Anforderungen des IT-Sicherheitskatalogs gemäß § 11 Absatz 1a Energiewirtschaftsgesetz (EnWG)[1]**

☐ **DIN EN ISO 9001:2015 und ISO/IEC 27001:2013 kombiniert**

☐

Ansprechpartner TÜV Hessen

(wenn bekannt, tragen Sie bitte Ihren Ansprechpartner beim TÜV Hessen ein)

Name: _____

Unternehmensdaten Zentrale / Hauptstandort

(bitte auf Homepage-Impressum verweisen oder Firmenbroschüre beilegen, wenn vorhanden)

Eingetragener Name: _____

Adresse (Hauptstandort): _____

Telefon: _____ Fax: _____

Internetadresse/Domain: _____

Produkte / Produktgruppen / Dienstleistungen

_____

_____

_____

Anwendungsbereich des ISMS InformationsSicherheitsManagementSystems[2]

(wenn bereits festgelegt, bitte als Anlage anfügen)

Marktumfeld (Branche, Kunden): _____

Interne Organisationseinheiten: _____

Gesetzliche, behördliche, vertragliche Anforderungen: _____

Interessierte Parteien: _____

Scope / Anwendungsbereich des ISMS (Prozesse, geografisch, fachlich): _____

[1] wenn zutreffend, bitte unbedingt auch Anlage (2) *Liste aller Standorte/Niederlassungen im Anwendungsbereich des ISMS* mit Angabe aller besetzten Betriebsstätten und aller nicht dauerhaft besetzten Betriebsstätten (Gruppenbildung) ausfüllen (s. hierzu auch Seite 6/Anlagen und Seite 7/Mustervorlage dieses Fragebogens)

[2] ISMS … InformationsSicherheitsManagementSystem nach ISO/IEC 27001:2013

Das Angebot soll umfassen:

☐ **nur Zentrale / Hauptstandort (Einzelverfahren)**

☐ **mehrere/alle Standorte (Multi-Site-Verfahren)**
(bitte geben Sie die Standorte/Niederlassungen mit vollständigen Adressen nachfolgend unter „Angaben zu den Mitarbeitern" an, wenn erforderlich, auf einem separaten Blatt als Anlage zu diesen Fragebogen.)

die folgenden Kriterien zur Anwendung des Multi-Site-Verfahrens (Stichprobenverfahrens) werden bestätigt ja ☐ nein ☐
(gemäß ISO/IEC 27006:2015, 9.1.5 und DAkkS 71 SD 6 013, Rev. 1.1)

(1) Alle Standorte arbeiten unter dem gleichen ISMS, das zentral verwaltet und auditiert wird und einer zentralen Managementbewertung unterliegt.
(2) Alle Standorte sind in das interne ISMS-Auditprogramm eingebunden.
(3) Alle Standorte sind in das Programm zur ISMS-Managementbewertung eingebunden.
(4) Die Zentrale hat das Durchgriffsrecht auf jeden Standort, z.B. bei Korrekturmaßnahmen.

Angaben zu den Mitarbeitern

*(bei Multi-Site-Verfahren bitte **alle** Standorte/Niederlassungen im Anwendungsbereich des ISMS angeben)*

*Bei mehr als 3 Standorten bitte separate, eigene **Anlage** verwenden*	**Zentrale / Hauptstandort**	Standort 2:	Standort 3:
Vollständige Adresse (Strasse, PLZ, Ort)			
Gesamtanzahl aller Mitarbeiter (inkl. Auszubildende, Teilzeitbeschäftigte und Sonstige [Leiharbeitnehmer, Externe, Freiberufler etc.]) ggf. in Umrechnung FTE (Full Time Equivalent):			
Anzahl der Mitarbeiter im Scope / Anwendungsbereich des ISMS:			
Reduzierende Faktoren:			
Anzahl der Mitarbeiter, die gleiche / ähnliche Tätigkeiten ausüben:			
Anzahl der Mitarbeiter im Schichtbetrieb:			
Anzahl der Schichten:			

Geschäftsführung / Leitung

Name: _____ E-Mail: _____

Telefon: _____ Fax: _____

Managementbeauftragte(r)

Name: _____ E-Mail: _____

Telefon: _____ Fax: _____

Externe Beratung zum Managementsystem durch:

Name: _____

Bestehende Zertifizierungen

Norm:	Zertifikat gültig bis:	Zertifizierer:	Letzter Audittag WA/ZA
	Datum		Datum
	Datum		Datum

Bitte stufen Sie Ihre Organisation durch einfaches Ankreuzen folgender ISMS-relevanter Themenbereiche ein:

Geschäftsprozesse und Betriebsorganisation

(gemäß ISO/IEC 27006:2015, Tabelle C.2 in Verbindung mit Tabelle C.1)

Art(en) der geschäftlichen und regulatorischen Anforderungen

☐ (1) Die Organisation arbeitet in nicht-kritischen Geschäftsfeldern und nicht-regulierten Sektoren.

☐ (2) Die Organisation hat Kunden in kritischen Geschäftsfeldern[3].

☐ (3) Die Organisation arbeitet in kritischen Geschäftsfeldern und/oder regulierten Sektoren[4].

Prozesse und Aufgaben

☐ (1) Der Zertifizierungsumfang umfasst einen Hauptgeschäftsprozess mit wenigen Schnittstellen und wenigen Geschäftseinheiten.
- Die Geschäftsprozesse sind Standardprozesse mit sich wiederholenden Aufgaben.
- Viele Personen führen unter Aufsicht der Organisation die gleichen Aufgaben aus.
- Das Leistungsangebot umfasst wenige Produkte und/oder Dienstleistungen.

☐ (2) Der Zertifizierungsumfang umfasst zwei bis drei Geschäftsprozesse mit einigen wenigen Schnittstellen und einigen wenigen Geschäftseinheiten.
- Die Geschäftsprozesse sind Standardprozesse mit sich nicht-wiederholenden Aufgaben.
- Das Leistungsangebot umfasst viele Produkte und/oder Dienstleistungen.

[3] **Kritische Geschäftsfelder** sind solche, in denen Unternehmen bei Störung oder Funktionsausfall gegen Normen und Standards verstoßen könnten.

[4] **Kritische Infrastrukturen** sind Organisationen, Einrichtungen und Dienstleistungen, bei deren Störung oder Funktionsausfall die Versorgungssicherheit der Gesellschaft mit wichtigen Gütern und Dienstleistungen nachhaltig beeinträchtigt würde. In Deutschland werden folgende **Sektoren** (und Branchen) den Kritischen Infrastrukturen zugeordnet: Transport und Verkehr, Energie (Elektrizität, Mineralöl, Gas), ITK Informationstechnik und Telekommunikation, Finanz- und Versicherungswesen, Staat und Verwaltung, Ernährung (Ernährungswirtschaft, Lebensmittelhandel), Öffentliche Wasserver- und -entsorgung, Gesundheit, Medien und Kultur (Rundfunk, gedruckte und elektronische Presse).
Mit dem **Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17.07.2015** sollen die Betreiber dieser Kritischen Infrastrukturen verpflichtet werden, Ihre Netze zu schützen.

☐ (3) Der Zertifizierungsumfang umfasst mehr als zwei komplexe Geschäftsprozesse mit vielen Schnittstellen und Geschäftseinheiten.
- Die Geschäftsprozesse sind vielschichtig und komplex.
- Das Leistungsangebot umfasst eine hohe Anzahl an Produkten und/oder Dienstleistungen.
- Im Anwendungsbereich des ISMS sind zahlreiche Geschäftseinheiten miteinbezogen, d.h. das ISMS umfasst hochkomplexe Prozesse oder eine relativ hohe Zahl an Aktivitäten oder an Sonderfällen.

Umsetzungsgrad des ISMS

☐ (1) Das ISMS ist vollständig umgesetzt und hat bereits mehrere (interne) Audit- und Verbesserungszyklen durchlaufen, was in Aufzeichnungen über interne Audits, Managementbewertungen und ein wirksames ständiges Verbesserungssystem dokumentiert ist.
- Das ISMS ist zertifizierungsreif etabliert und/oder andere (zertifizierte) Managementsysteme sind vorhanden.

☐ (2) Das ISMS ist teilweise umgesetzt, d.h. einige Instrumente eines Managementsystems stehen zur Verfügung und sind umgesetzt, ständige Verbesserungsprozesse sind vorhanden, aber nur teilweise dokumentiert.
- Das ISMS ist noch nicht bis zur Zertifizierungsreife umgesetzt und/oder einige Elemente von anderen Managementsystemen sind implementiert.

☐ (3) Das ISMS ist neu und noch nicht vollständig aufgebaut
(z.B. keine Managementsystem spezifischen Kontrollmechanismen, fehlender Reifegrad des ständigen Verbesserungsprozesses, Ad-hoc-Prozessausführung).
- Bisher wurde überhaupt kein anderes Managementsystem umgesetzt.

IT-Umfeld

(gemäß ISO/IEC 27006:2015, Tabelle C.3 in Verbindung mit Tabelle C.1)

Komplexität der IT-Infrastruktur

☐ (1) Die IT Landschaft ist einheitlich und/oder hoch standardisiert mit wenigen IT-Plattformen, Servern, Betriebssystemen, Datenbanken und getrennten Netzwerken etc.

☐ (2) Die IT Landschaft ist standardisiert mit mehreren verschiedenen IT-Plattformen, Servern, Betriebssystemen, Datenbanken, Netzwerken etc.

☐ (3) Die IT Landschaft ist komplex und vielfältig mit vielen verschiedenen IT-Plattformen, Servern, Betriebssystemen, Datenbanken, Netzwerken etc.

Abhängigkeit von Outsourcing, externen Anbietern/Lieferanten (inkl. Cloud-Services)

☐ (1) Es besteht keine oder eine geringe Abhängigkeit von Outsourcing und von externen Anbietern/Lieferanten **oder**
- die Outsourcing-Vereinbarungen sind klar definiert, gelenkt und überwacht,
- der Outsourcer unterhält ein zertifiziertes ISMS und
- einschlägige, unabhängige Prüfberichte über die Outsourcer Anbieter sind verfügbar.

☐ (2) Die Abhängigkeit von Outsourcing oder von externen Anbietern/Lieferanten in Verbindung mit einigen, aber nicht allen wichtigen Geschäftsaktivitäten ist mäßig.
- Es bestehen mehrere, z.T. gelenkte Outsourcing-Vereinbarungen.

☐ (3) Die Abhängigkeit von Outsourcing oder von externen Anbietern/Lieferanten ist hoch mit erheblichem Einfluss auf wichtige Geschäftsaktivitäten.
- Umfang und Ausmaß von Outsourcing sind unbekannt oder
- es bestehen mehrere ungelenkte Outsourcing-Vereinbarungen.

Informationssystementwicklung

☐ (1) Die Organisation betreibt keine oder eine sehr begrenzte Inhouse-System-/Anwendungsentwicklung.
- In der Organisation sind standardisierte Software-Plattformen im Einsatz.

☐ (2) Die Organisation betreibt keine eine mäßige Inhouse-System-/Anwendungsentwicklung für einige wichtige Geschäftszwecke statt.
- In der Organisation sind standardisierte Software-Plattformen mit komplexer Konfiguration/Parametrierung im Einsatz bzw.
- wird (sehr) organisationsspezifisch angepasste Software eingesetzt.
- Es finden einige Entwicklungsaktivitäten (Inhouse/Outsourcing) statt.

☐ (3) Die Organisation betreibt eine umfangreiche Inhouse-System-/Anwendungsentwicklung für wichtige Geschäftszwecke.
- Es bestehen umfangreiche interne Software-Entwicklungsaktivitäten mit mehreren laufenden Projekten für wichtige geschäftliche Zwecke.

Sonstige ISMS-relevante Informationen zur Organisation

In welchen (Haupt-)Geschäftsprozessen werden Informations- und Kommunikationstechniken eingesetzt: _____

Anzahl Nutzer:

Anzahl DV-Arbeitsplätze (Workstations + PCs + Laptops):

Anzahl der Server:

Anzahl Beschäftigte für Anwendungsentwicklung/Wartung:

Bestehen Hochverfügbarkeitsanforderungen, z.B. 24/7-Services? ja ☐ nein ☐

Gibt es mehrere Rechenzentren und/oder separate Standorte zur Notfallwiederherstellung? ja ☐ nein ☐

Gibt es einen Prozess zur Informationssicherheitsrisikobeurteilung? ja ☐ nein ☐

Gibt es einen Prozess zur Informationssicherheitsrisikobehandlung? ja ☐ nein ☐

Existiert bereits eine „Erklärung zur Anwendbarkeit“ (SoA / Statement of Applicability) gemäß ISO/IEC 27001:2013, 6.1.3 d)? ja ☐ nein ☐
(Wenn ja, bitte als Anlage anfügen)

Art und Dokumentation des ISMS-Systems

(Zutreffendes bitte ankreuzen)

Datum der Einführung: Datum

☐ Das ISMS-System ist ein eigenständiges Managementsystem und in einem separaten ISMS-Handbuch und zugehörigen Anweisungen dokumentiert.

☐ Es existiert ein integriertes Managementsystem mit Schnittstellen zum Qualitäts-managementsystem und/oder anderen Managementsystemen. Es gibt ein gemeinsames (integriertes) Managementsystem-Handbuch

Ablauf und Terminsituation

Sind Fristen[5] für die Vorlage unseres Angebotes zu beachten, wenn ja bis Datum

Als Termine sind geplant

- für das Audit Stufe 1 (Bereitschaftsbewertung): Datum

- für das Audit Stufe 2 (Zertifizierungsaudit): Datum

Datum

Datum	Ort	Unterschrift / Firmenstempel

Angefügte Anlagen (soweit vorhanden bzw. erforderlich):

☐ (1) Anwendungsbereich des ISMS gemäß ISO/IEC 27001:2013, 4.3

☐ (2) Liste aller Standorte/Niederlassungen im Anwendungsbereich des ISMS[6]

☐ (3) Erklärung zur Anwendbarkeit gemäß ISO/IEC 27001:2013, 6.1.3 d)

[5] In der Regel sind wir bemüht, Angebote umgehend zu erstellen, allerdings kann es durch eingeschränkte Verfügbarkeit der involvierten Mitarbeiter zu geringfügigen Verzögerungen kommen.

[6] Wenn zusätzliche Anforderungen des IT-Sicherheitskatalogs gemäß § 11 Absatz 1a Energiewirtschaftsgesetz (EnWG) zutreffend sind, kann als mögliche Vorlage für Anlage (2) *Liste aller Standorte/Niederlassungen im Anwendungsbereich des ISMS* mit Angabe aller besetzten Betriebsstätten und aller nicht dauerhaft besetzten Betriebsstätten (Gruppenbildung) gemäß Konformitätsbewertungsprg. zur Akkreditierung von Zert.-stellen für den IT-Sicherheitskatalog die tabellarische Struktur der nachfolgenden Seite 7 übernommen werden.

Vorlage (beispielhaftes Muster) für
Anlage (2) *Liste aller Standorte/Niederlassungen im Anwendungsbereich des ISMS*

Standortbezeichnung			…
Vollständige Adresse (Strasse, PLZ, Ort)			…
Gesamtanzahl Mitarbeiter - davon Auszubildende - davon Teilzeitbeschäftigte - davon Mitarbeiter, die gleiche / ähnliche Tätigkeiten ausüben - davon Sonstige [Leiharbeitnehmer, Externe, Freiberufler etc.]			…
Anzahl der Mitarbeiter im Scope / Anwendungsbereich des ISMS			…
Anzahl der Mitarbeiter mit unmittelbarer Relevanz (GF, ISMS-Verantwortliche, IT-Personal, unterstützende Funktionen) für die Informationssicherheit			…
Anzahl der Mitarbeiter im Schichtbetrieb:			…
Anzahl der Schichten:			

Nicht dauerhaft besetzte Betriebsstätten[7] (im Scope / Anwendungsbereich des ISMS)

Art der nicht dauerhaft besetzten Betriebsstätte	**Anzahl**
Notleitstelle	
Ferngewirkte Umspannwerke/Schaltstellen (Strom)	
Ferngewirkte Umspannpunkte/Schaltpunkte (Strom)	
Fernwirktechnik in Fremdanlagen	
Ferngewirkte Verdichterstation (Gas)	
Ferngewirkte Anladestation (Gas)	
.....(ggf. ergänzen)	

[7] *„Zusätzlich sind im Rahmen der Audits von jeder Gruppe der nicht dauerhaft besetzten Betriebsstätten, die Teil des Scopes sind, je Zertifizierungszyklus mindestens zwei Betriebsstätten auf die Umsetzung der zutreffenden Maßnahmen der DIN ISO/IEC TR 27019:2015-03; DIN SPEC 27019:2015-03 zu auditieren.*“
(Vorgabe gemäß Abschnitt 5 des Konformitätsbewertungsprg. zur Akkreditierung von Zert.-stellen für den IT-Sicherheitskatalog)