

## Kriterienkatalog zur Aufnahme in IHK- Datenbank von IT-Sicherheitsdienstleister

### 1. Anbieterinformationen

1.1	Name des Anbieters	
1.2	Rechtsform	
1.3	Straße	
1.4	Postleitzahl	
1.5	Ort	
1.6	Ansprechpartner	
1.7	Telefonnummer	
1.8	E-Mail-Adresse	
1.9	Startseite der Webpräsenz (URL)	
1.10	Jahr der Unternehmensgründung	
1.11	Anzahl der Mitarbeiter	
1.12	Art der Muttergesellschaft(*)	
1.13	Land der Muttergesellschaft(*)	
1.14	Land der Zentrale(*)	

\* falls zutreffend

### 2. Informationen zum Angebot

*Bitte kreuzen Sie an, welche Produkte in den Unterkategorien angeboten werden.*

	Hauptkategorie	Unterkategorie	Leistungsportfolio
2.1		Beratung Informationssicherheit, IT-Sicherheit, Cybersicherheit	
2.2		Beratung Business Continuity Management (BCM)	
2.3		Einführung eines Informations-Sicherheits-Management-Systems	
2.4		externer Informationssicherheitsbeauftragter	
2.5		Datenschutz-Beratung (Einführung Datenschutzmanagement)	
2.6		Externer Datenschutzbeauftragter	
2.7		Beratung/ Unterstützung situativ inkl. Forensik (Red Team)	

2.8	Organisatorische Angebote, inkl. Beratung, externe Dienstleistung	IT-Sicherheitscheck (inkl. Penetrationstest oder Schwachstellentest)	
2.9		Network Operations Center (Beratung zu Aufbau oder externe Dienstleistung)	
2.10		Security Operations Center (Beratung zu Aufbau oder externe Dienstleistung)	
2.11		Incident Analyse/ Auswertung von Log-Dateien (Beauftragung eines Dienstleisters)	
2.12		Awareness/ Sensibilisierung von Mitarbeitern (Aufbau eines eigenen Mitarbeiter-Schulungsservice oder Beauftragung eines Dienstleisters)	
2.13		Regeln der IT-Sicherheit und Technische und Organisatorische Maßnahmen a) Beratung und Einführung	
2.14		Regeln der IT-Sicherheit und Technische und Organisatorische Maßnahmen b) Audits	
2.15		Hinweise und Angebote zur Beschaffung zertifizierter Komponenten	
2.16		Full-Service 24/7 IT-Sicherheitsdienstleister	
2.17		Cyberversicherung	
2.18	Technisches Angebot	Präventive IT-Sicherheitsmaßnahmen (Firewalls, Anti-Viren-Programm, Angriffserkennung, etc.)	
2.19		Verfahren und Technologien zum Schutz des Unternehmensnetzwerks (NAC, MDM, SOC, etc.)	
2.20		Technologien zu Business Continuity Management (BCM)	
2.21		Technologien zur Analyse/ Bekämpfung akuter Sicherheitsvorfälle (IT-Forensik o.ä.)	
2.22		Verfahren und Technologien zur Erkennung von Innentätern (IT-Forensik o.ä.)	
2.23		End Point Protection	
2.24	Sonstiges		

### 3. Unternehmenskriterien

*Bitte füllen Sie die Kriterien nach aktuellem Stand aus. Nachweise können als Anhang beigefügt werden.*

	Kriterium	Anmerkung	Vorhanden
3.0	Das Unternehmen hat seinen Standort in Thüringen	Musskriterium für Punkt 2.1 - 2.24	

3.1	Es liegt eine ISO27001 oder BSI Zertifizierung "Praktiker" für im Unternehmen beschäftigte Berater und/ oder Techniker vor	Musskriterium für Punkt 2.1 - 2.4	
3.2	Es liegt eine ISO27001 oder BSI Zertifizierung "Auditor" für im Unternehmen beschäftigte Berater und/ oder Techniker vor	Musskriterium für "Audits" unter 2.14	
3.3	Es liegt eine Zertifizierung zum (externen) Datenschutzbeauftragten vor	Musskriterium für 2.5 - 2.6	
3.4	Es liegt eine Zertifizierung im Bereich BCM/ Notfallmanagement vor	Musskriterium für "BCM" unter 2.2	
3.5	Bitte nennen Sie entsprechende Referenzen (können als separaten Anhang beigelegt werden)	Musskriterium für Punkt 2.1 - 2.24	
3.6	Technische Produkte sind nach ISO27001, BSI oder einer anderen vertrauenswürdigen Stelle zertifiziert	Musskriterium für 2.18 - 2.24	
3.7	Technische Produkte wurden durch andere vertrauenswürdige Stellen ausgezeichnet		
3.8	Es liegen weitere Zertifizierungen im Bereich Informationssicherheit, IT-Sicherheit, Cybersecurity vor (CHFI, OSCP, CEH, ePPT, o.ä.)		