Kompetenzmatrix
Zertifizierung zum IT-Sachverständigen/-Analysten nach DEKRA Standard

Darstellung der im Zertifizierungsverfahren nachzuweisenden Fachkompetenzen für die Zertifizierungsstufen

- **IT-Sachverständiger (Systeme und Anwendungen oder Systeme und Technik)**
- **Sachverständiger IT-Forensic (lokale und mobile Systeme)**
- **Sachverständiger IT-Security (Netzwerk und Internet)**

sowie

- **IT-Forensic-Analysten**
- **IT-Security-Analysten**

Aus Gründen der besseren Lesbarkeit wird in diesem Dokument davon abgesehen, die weibliche und männliche Form auszuführen. Es versteht sich von selbst, dass alle Bezeichnungen sowohl in der weiblichen als auch in der männlichen Form verwendet werden.

Darstellung der Profile im Fachbereich IT

Die Zertifizierungseingrenzung berücksichtigt, dass kein Sachverständiger/Analyst auf dem gesamten Fachgebiet der Informationstechnologie (IT) gleichermaßen besonders sachkundig sein kann. Es erfolgt daher die Einteilung in folgende Zertifizierungsschwerpunkte:

- IT-Sachverständiger (Systeme und Anwendungen) – kurz SuA
- IT-Sachverständiger (Systeme und Technik) – kurz SuT

Die Bereiche SuA und SuT können hierbei nicht immer klar voneinander abgrenzt werden und es gibt zahlreiche Überschneidungen. Bei der gutachterlichen Beauftragung und Fragestellung muss daher jeder Sachverständiger/Analyst eine gewisse Grundkenntnis auch im jeweils anderen Schwerpunkt besitzen.

Das DEKRA-Zertifizierungsprogramm konzentriert sich auf den Bereich Systeme und Anwendungen und zusätzlich auf die Fachgebiete IT-Forensic und IT-Security.

- IT-Sachverständiger Systeme + Anwendungen nach DEKRA Standard
- IT-Sachverständiger Systeme + Technik nach DEKRA Standard
- Sachverständiger IT-Forensic nach DEKRA Standard
- Sachverständiger IT-Security nach DEKRA Standard
- IT-Forensic-Analyst (Windows Betriebssysteme) nach DEKRA Standard
- IT-Forensic-Analyst (Mobile Device) nach DEKRA Standard
- IT-Security-Analyst (Netzwerk und Internet) nach DEKRA Standard

Der Antragsteller für ein Zertifizierungsverfahren gemäß den o.g. Zertifizierungsprogrammen muss den Nachweis der besonderen Sachkunde in den jeweiligen Vertiefungsgraden nachweisen:

- Grundkenntnisse (**1**)
- Vertiefende Kenntnisse (**2**)
- Detailkenntnisse (**3**)

DEKRA Standard	**Kompetenzen** **IT (allgemein) mit/ohne Vertiefung**	Vertiefungsgrad
Rechtsgrundlagen		
Einschlägige Versicherungsrechtliche Vorschriften		1
Einschlägige Vorschriften des Strafrechts §§ 11, 184 a-d, 202 a-c, 206, 263a, 266b, 268, 269, 270 StGB		1
Weitere einschlägige Straftatbestände (UWB, UrhG, HGB, AO)		1
Betriebswirtschaft		
Grundbegriffe der Betriebswirtschaft Wirtschaftlichkeit, Aufwand und Ertrag		1
Unternehmensaufbau und Management Organisation, Geschäftsprozesse, Finanzen, Investitionsrechnung, internes und externes Rechnungswesen, Einkauf, Leistungserstellung, Materialwirtschaft, Vertrieb, Service und Marketing		1
Datenschutzgesetze		2
Normen und Regeln der Technik		
Entwicklungstendenzen		2
Marktgängige Standards		2
Verbreitete Produkte		2
Branchenüblichkeit		2
Allgemein anerkannte Regeln der Technik		3
Stand der Technik		3

DEKRA Standard	**Kompetenzen** **IT-Sachverständiger**	
Computer		
Rechnerorganisationen		1
Rechnerarchitektur		1
Peripheriegeräte		
Speichersysteme		1
Dateien- und Ausgabegeräte		1
Datenübertragung und Vernetzung Konzepte, Möglichkeit und Verfahren zur Einbindung von Standorten, Daten- und Telekommunikation		1
Fehlertoleranz		
Verfügbarkeit		1
Technische Möglichkeiten		1
Einsatz von Software		
Standardsoftware Einführung von branchenüblichen und branchenspezifischen Lösungen, ERP-Systeme, E-Commerce-Lösungen		2
Individualsoftware		
Dokumentation		2
Projekte Organisation und Projektmanagement, Abnahme, Vorgehensmodelle		2
Unternehmensübergreifende Software CRM, SCM, EDI, EDIFACT		2

DEKRA Standard	**Kompetenzen IT-Sachverständiger**	
Betrieb von Systemen		
IT-Service-Management		2
Service-Level-Agreements		2
Leistungs- und Abrechnungsformen		2
Fragestellung bei Outsourcing und externer Datenspeicherung		2
Betrieb komplexer Systeme		2
Wert- und Kostenbegriffe		
Wertbegriffe Anschaffungswert, Beleihungswert, Bestandswert, Fair Value, Fortführungswert, Gebrauchswert, Gemeiner Wert, Installationswert, Liquidationswert, Marktwert, Minderwert, Merkantiler Minderwert, Technischer Minderwert, Neuwert, Nutzungswert, Restwert, Rumpfwert, Schrottwert, Taxwert, Verkehrswert, Vergleichswert, Versicherungswert, Wiederbeschaffungswert, technischer Zeitwert, Zerschlagungswert		3
Kostenbegriffe Anschaffungskosten, Abschreibungen, Betriebskosten, Gemeinkosten, Herstellungskosten, Sonstige Kosten, Transaktionskosten, Wartungskosten.		3

DEKRA Standard	**Kompetenzen Sachverständiger IT-Forensic bzw. IT-Forensic-Analyst**	
Forensisches Vorgehen bei Datensicherung und Auswertung		
Umgang mit Beweismitteln		1
Anfertigung von Kopien		1
Prüfsummen		1
Protokollierung		1
Verwaltung von Asservaten		2
Kryptologie		
Prinzipien		2
Verfahren		2
Anwendungen		2
Sicherheit		2
Hashwerte		
SHA1, ED2K, MD5		2
Cloudsysteme		
Modelle, Strukturen, Zugriffs-, sicherungs-, Auswertemöglichkeiten		2
Betriebssysteme		
Windows, Linux, Unix, MacOS, iOS, Android		2
Forensische Datensicherungsformate		2
Sicherung flüchtiger Datenbestände		
RAM		2
Cold Boot		2

DEKRA Standard	**Kompetenzen** **Sachverständiger IT-Forensic bzw. IT-Forensic-Analyst**	
Rechtliche und Ethische Rahmenbedingungen		2
Datenschutz		2
Unterschiede bei der Beauftragung von Sachverständigen und bei der Art der Gutachtenerstattung		
Zivilrecht		2
Strafrecht		2
Abgrenzung zur Beauftragung als Ermittler		2
Rechtliche Kenntnisse		
Wirtschaftsstraftaten		2
Betrug		2
Untreue		2
Rechtsstaat		2
Gefährdende Straftaten		2
Sexualstraftaten (u.a. Kinderpornografie)		2
Kenntnisse im Strafrecht und Strafprozessrecht Verfahrensweise im Ermittlungsverfahren, Auswertemöglichkeiten, Beweissicherungsverbote		2
Urheberrechtstraftaten Raubkopien, EDV-Strafrecht, Telekommunikationsgesetz, Überwachung der Telekommunikation		2
Täterterminologie		2
Grundsätzliche Prinzipien der IT-Forensic		
Grundlegende Definitionen		3
Chain of Custody		3
Nature of Evidence		3
Locard'sche Regel		3
Prozessmodelle		3
Bild- und Videoformate		
JPEG		3
MPEG		3
EXIF		3
Internetkommunikation		
E-Mail		3
Chat		3
Messaging		3
Digitale Signaturen und Schlüsselverwaltungssysteme		3
Dateisysteme		3
FAT		3
NTFS		3
EXT2		3
EXT3		3
HFS		3
ReiserFS		3
EXT4		3
XFS		3
Lux		3

DEKRA Standard	**Kompetenzen** **Sachverständiger IT-Forensic bzw. IT-Forensic-Analyst**	
Storage Systeme		
SATA		3
DIE		3
SCSI		3
SAN		3
Raid 0-6		3
ReFS		3
Datenträger Magnetische und optische Datenträger, Flashspeicher		3
Virtualisierungssoftware		
VMware		3
VirtualPC		3
Citrix		3
Planung von Sicherstellungsmaßnahmen		3
Schreibschutzmaßnahmen		3
Tools zur Auswertung von mobilen Endgeräten und Rechnersystemen		3
Tools zur Auswertung		3
Anwendungsforensik		
Artefakte aus Prefetch		3
Cache		3
History		3
Cockie		3
Bookmark		3
Auslagerungs-Bereiche		3
Timeline		
Quellen, Konsolidierung und Analysen		3
Auswertung von Konfigurationsdateien		
Registry		3
INI-Files		3
conf.-Dateien		3
Auswertung von Protokoll-Dateien		
Eventlogs		3
Syslogs		3
Aufbereitung der Erkenntnisse		
Inhalt		3
Darstellungsformen		3
Trennung von Tatsachen und Ableitungen		3
IT-Forensic		1

DEKRA Standard	**Kompetenzen** **Sachverständiger IT-Forensic bzw. IT-Forensic-Analyst**	
Kommunikationsgrundlagen		
Klassen		1
Adressierungsarten		1
Topologien		1
ISO/OSI-Referenzmodell		1
TCP/IP-Referenzmodell		
Schichten		1
Protokolle		1
Dienste		
Kryptologie, Hashfunktionen, Signaturen		
Grundlagen		1
Prinzipien		1
Methoden		1
Elektronische Signaturen Verfahren, Standards, Methoden		1
Datenschutz		
Datenschutzrecht		1
Datenschutzumsetzung		1
Datenschutzkontrolle		1
Governance		1
Compliance		1
Sicherheitsrichtlinien		
IT-Sicherheitsgesetz		2
Sicherheitsinfrastruktur		2
Spezielle Bedrohungen		
Grundlagen		2
Angriffe		2
Gegenmaßnahmen zu relevanten Bedrohungen		2
Malware Viren, Würmer, Trojaner		2
Botnetze		2
Spam, Phishing		2
Denial-of-Service		2
Firewall-Technologien		
Paketfilter		2
DMZ		2
Proxy		2
OSI-Sicherheitsarchitektur		2

DEKRA Standard	**Kompetenzen** **Sachverständiger IT-Forensic bzw. IT-Forensic-Analyst**	
Verwaltung von Betriebssystemen		
Administrationen		2
Rechtevergabe		2
Zugriffskontrolle		2
Security-Engineering		
Bewertungskriterien		2
Sicherheitsmodelle		2
Entwicklungsprozess		2
Strukturanalyse		2
Schutzbedarfsbestimmung		2
Bedrohungsanalyse		2
Risikoanalyse		2
Security Development Lifecycle		2
Allgemeine Kenntnisse		
Schutzziele		3
Schwachstellen		3
Bedrohungen		3
Angriffe		3
Rechtliche Rahmenbedingungen		3
Sichere Kommunikation		
VPN		3
IPSec		3
SSL/TLS		3
Web-Anwendungen		
Aktive Inhalte		3
Websockets		3
OWASP Top 10		3
Analysewerkzeuge und Systemhärtung		
Überwachung		3
IDS		3
IDP		3
Contentfilter		3
Betriebssystem-Sicherheit		
Aufgaben		3
Arten und Aufbau von Betriebssystemen		3
Schlüsselmanagement		
Zertifizierung Zertifikate, PKI		3
Schlüssel Erzeugung, Aufbewahrung, Vernichtung, Austausch, Rückgewinnung		3

Stand: 08/2019