Inhaltsverzeichnis

1. Geltungsbereich

Diese Prüfungs- und Zertifizierungsordnung (PZO) gilt für das Zertifizierungsverfahren für IT-Security entsprechend dem Programm zur Zertifizierung von Personen der DEKRA Certification GmbH (DCG) und auf der Grundlage der DIN EN ISO 17024 in der jeweils gültigen Fassung und für die folgenden Abschlüsse:

- IT-Security-Analyst (Netzwerke und Internet) (ITSA)
- Sachverständige:r IT-Security (Netzwerke und Internet) (SVITS)

Zusätzlich gelten die Allgemeinen Geschäftsbedingungen (AGB) (D-030-18) und die Allgemeinen Zertifizierungsbedingungen (AZB) (D-030-19) der DCG.

Die Dienstleistungen der Zertifizierungsstelle stehen allen interessierten Personen offen und die DCG garantiert die Gleichbehandlung aller Antragsteller:innen durch die Festlegung objektiver Kriterien für die Zulassung, die Prüfung und die Zertifizierung.

2. Anmeldung und Zulassung zur Prüfung

Die Anmeldung zu einer Prüfung und Zertifizierung erfolgt schriftlich anhand des Antrags zur Zertifizierung zum Standard IT-Security (F-03S-60) und Bestätigung der PZO, AZB und AGB der DCG. Die Antragstellung muss spätestens 10 Werktage vor dem geplanten Prüfungstermin erfolgen.

Die Teilnahme an den unter **Punkt 1** genannten Prüfungen unterliegt den in **Anlage 1** entsprechend genannten Zulassungsvoraussetzungen.

Die in der **Anlage 1** geforderten Nachweise sind dem Antrag zur Zertifizierung beizufügen. Die Nachweispflicht liegt bei der zu prüfenden Person.

Bei nicht erfüllten Zulassungsvoraussetzungen wird die zu prüfende Person von der Prüfung ausgeschlossen oder nimmt an der Prüfung teil und reicht die fehlenden Nachweise innerhalb von 10 Werktagen nach. Sollten die Zulassungsvoraussetzungen nicht innerhalb von 10 Werktagen nach dem Prüfungstermin erfüllt worden sein, wird eine durchgeführte Prüfung ohne weiteres als nicht bestanden gewertet und der Prüfungspreis ist in voller Höhe zu entrichten. Bei Unklarheiten ist die Zertifizierungsstelle berechtigt, weitere Nachweise anzufordern.

Alle Nachweise müssen in deutscher Sprache verfasst sein. Ausländische Nachweise müssen über eine:n öffentlich bestellte:n und allgemein beeidigte:n Übersetzer:in durch den/die Antragsteller:in übersetzt sein.

Die Zertifizierungsstelle prüft die Vollständigkeit und formale Richtigkeit der Anmeldeunterlagen und entscheidet über die Zulassung zur Prüfung.

3. Durchführung der Prüfung

Die Prüfungsaufgaben sind von der Zertifizierungsstelle erstellt und aus dem aktuellen Prüfungsfragenpool ausgewählt. Die Prüfung erfolgt grundsätzlich in deutscher Sprache und schriftlich. Teil 1 der Prüfung besteht aus Multiple-Choice-Fragen (MCF). Teil 2 der Prüfung besteht aus einer selbstständig zu erstellenden Heimarbeit. Die Prüfungsfragen und - aufgaben spiegeln hierbei repräsentativ die vermittelten Lerninhalte wider.

Die Organisation der Prüfung liegt in der Verantwortung der Zertifizierungsstelle. Präsenz-Prüfungen führen zugelassene und von der DCG für diese Durchführung beauftragte Prüfer:innen oder eine Prüfungsaufsicht durch. Die Durchführung der Prüfung vor Ort obliegt dem/der eingesetzten Prüfer:in / Prüfungsaufsicht.
Remote-Prüfungen werden über das von der DCG bereitgestellte Prüfungstool durchgeführt.

3.1. Durchführung der Prüfung IT-Security-Analyst (ITSA)

Teil 1 der Prüfung erfolgt schriftlich und besteht aus 30 MCF. Die Dauer der Prüfung beträgt 45 Minuten. Die mögliche Höchstpunktzahl beträgt 30 Punkte.
Es sind keine Hilfsmittel zugelassen.

Teil 2 der Prüfung besteht aus einem in Heimarbeit zu erarbeitenden Bericht einer Sicherheitsanalyse (Anlage 2). Die Aufgabenstellung wird im Anschluss an Teil 1 der Prüfung versendet. Zur Bearbeitung stehen 2 Wochen zur Verfügung. Später eingereichte Berichte werden nicht mehr akzeptiert.

3.2. Durchführung der Prüfung Sachverständige:r IT-Security (SVITS)

Teil 1 der Prüfung erfolgt schriftlich und besteht aus 50 MCF. Die Dauer der Prüfung beträgt 70 Minuten. Die mögliche Höchstpunktzahl beträgt 50 Punkte. Als Hilfsmittel ist ein Taschenrechner zugelassen.

Teil 2 der Prüfung besteht aus einem in Heimarbeit zu erarbeitenden Gutachten (Anlage 3). Die Aufgabenstellung wird im Anschluss an Teil 1 der Prüfung versendet. Zur Bearbeitung stehen 8 Wochen zur Verfügung. Später eingereichte Berichte werden nicht mehr akzeptiert.

4. Bewertung

Die Auswertung der Prüfung erfolgt durch den/die beauftragte:n und zugelassene:n Prüfer:in.

Die Prüfung gilt als bestanden, wenn mindestens 66 % der möglichen Höchstpunktzahl in jedem Prüfungsteil erreicht wird. Bei weniger als 66 % gilt die Prüfung als nicht bestanden.

Bei jeder MCF werden vier Antwortmöglichkeiten vorgegeben, wobei immer eine oder zwei oder drei Antworten richtig sind, jedoch nie alle vier Antworten. Jede vollständig richtig beantwortete MCF wird mit einem Punkt gewertet.
Das Gutachten/der Bericht wird entsprechend der in Anlage 2 und 3 genannten Kriterien entsprechend dem Erfüllungsgrad der Aufgabe gewertet. Wird ein KO-Kriterium (Anlage 4) festgestellt, gilt der Prüfungsteil als nicht bestanden.

Das Prüfungsergebnis und die Prüfungsunterlagen werden der Zertifizierungsstelle übermittelt und gegengeprüft.

5. Wiederholung der Prüfung

Eine nicht bestandene Prüfung kann zweimal wiederholt werden. Die Anmeldung zu einer Wiederholungsprüfung erfolgt schriftlich anhand des Antrags zur Wiederholungsprüfung (F-03S-09) und Bestätigung der PZO, AZB und AGB der DCG.

Die Wiederholungsprüfung muss im Regelfall innerhalb von 60 Tagen nach der Zertifizierungsentscheidung (Datum des Informationsscheibens) beantragt werden. Der Termin der Wiederholungsprüfung wird von der DCG festgelegt.

6. Zertifizierungsentscheidung

Das Zertifizierungsgremium trifft die Zertifizierungsentscheidung innerhalb von ca. 3 Wochen nach dem Prüfungstermin. Weicht das Zertifizierungsgremium vom Votum des Prüfers oder der Prüferin ab, ist dies schriftlich zu begründen.

Bei bestandener Prüfung und erfolgreicher Zertifizierung wird das DEKRA Zertifikat in deutscher Sprache für die Laufzeit von max. 3 Jahren erteilt. Das Zertifikat beinhaltet die folgenden Angaben: vollständiger Name, Geburtsdatum und Titel (falls vorhanden) der zertifizierten Person, die erworbene Qualifikationsstufe, der Hinweis auf das Zertifizierungsprogramm, nachgewiesene Kenntnisse und Kompetenzen, DEKRA Logo, DEKRA Zeichen, Angaben zur Zertifizierungsstelle, Prüfungsdatum, Prüfungsort, Ausstellungsdatum, Ausstellungsort, Ablaufdatum des Zertifikates, eindeutige Zertifikatsnummer sowie die Unterschrift der verantwortlichen Person.

Die Zertifikatsinhaber:innen werden in das zur Veröffentlichung für berechtigte Personen bestimmte Verzeichnis der zertifizierten Personen der DCG aufgenommen. Das Zertifikat sowie das Siegel bleiben das Eigentum der DCG. Die Nutzungsbedingungen für das Zertifikat und das Siegel sind in den AZB geregelt.

7. Überwachung

Die zertifizierte Person hat eigenverantwortlich ihren Kompetenzerhalt sicherzustellen. Die DCG überwacht die Einhaltung der Nutzungsbedingungen für das Zertifikat und das Siegel. Dazu gehören – sofern im Gültigkeitszeitraum des Zertifikats eintretend – die Auswertung von Informationen von Aufsichtsbehörden, die Bewertung von Beschwerden und Informationen von interessierten Kreisen sowie von eingeleiteten rechtlichen Schritten in Bezug auf die zertifizierte Person.

8. Rezertifizierung

Eine Rezertifizierung kann von Zertifikatsinhaber:innen spätestens bis zu 3 Monaten nach dem Ablauf der Gültigkeit des aktuellen Zertifikates unter Verwendung des Antrags zur Rezertifizierung (F-03S-17) schriftlich bei DCG beantragt werden.

Dabei sind die in der **Anlage 1** folgenden geforderten Nachweise mit einzureichen.

Später eingereichte Anträge werden nicht akzeptiert. Alle Anforderungen für die Rezertifizierung müssen im Zeitraum der Zertifikatsgültigkeit erfüllt worden sein.

Voraussetzung für eine Rezertifizierung sind ein vollständiger und korrekter Antrag und die positive Bewertung der eingereichten Nachweise. Das Ergebnis der Dokumentenprüfung wird dem/der Antragsteller:in mitgeteilt. Bei erfolgreicher Dokumentenprüfung wird ein neues Zertifikat für weitere max. 3 Jahre ausgestellt. Das bisherige Zertifikat verliert seine Gültigkeit.

9. Prüfungsunterlagen

Alle Unterlagen zur Prüfung werden von der Zertifizierungsstelle elektronisch archiviert. Die Aufbewahrungsfrist beträgt 10 Jahre.

10. Kosten

Erstprüfung (inkl. Zertifizierung)	**Preis zzgl. MwSt.**	**Preis inkl. MwSt.**
IT-Security-Analyst (Netzwerke und Internet) (ITSA)	350,00 EUR	416,50 EUR
Sachverständige:r IT-Security (Netzwerke und Internet)	715,00 EUR (650,00 EUR bei bestehendem Zertifikat IT-Security Analyst)	850,85 EUR (773,50 EUR bei bestehendem Zertifikat IT-Security Analyst)
Wiederholungsprüfung		
Teil 1: schriftliche Prüfung (alle Produkte)	195,00 EUR	232,05 EUR
Teil 2: Bericht ((ITSA)	245,00 EUR	291,55 EUR
Teil 2: Gutachten (SVITS)	295,00	351,05 EUR
Rezertifizierung	**Preis zzgl. MwSt.**	**Preis inkl. MwSt.**
IT-Security-Analyst (Netzwerke und Internet) (ITSA)	245,00 EUR	291,55 EUR
Sachverständige:r IT-Security (Netzwerke und Internet)	475,00 EUR	565,25 EUR

11. Änderungsdienst

Der/Die Teilnehmende bzw. die zertifizierte Person hat sich laufend eigenverantwortlich über Änderungen an den für den Zertifizierungsprozess relevanten Verfahren, Beschreibungen, Dokumenten und Formularen zu informieren. Die aktuellen Unterlagen sind auf der Website der DCG erhältlich.

Anlage 1 - Formale Zulassungsvoraussetzungen zur Teilnahme an der Prüfung und Zertifizierung

Erstzertifizierung		
	IT-Security-Analyst (Netzwerke und Internet) (ITSA)	Sachverständige:r IT-Security (Netzwerke und Internet) (SVITS)
Option 1 Master-Studium mit zertifikatsrelevantem Schwerpunkt	3 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 5 Jahre	5 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 8 Jahre
Option 2 Bacherlor-Studium mit zertifikatsrelevantem Schwerpunkt	5 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 8 Jahre	8 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 12 Jahre
Option 3 Berufsausbildung mit zertifikatsrelevantem Schwerpunkt	5 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 8 Jahre	8 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 12 Jahre
Option 4 Ohne einschlägige Berufsausbildung	8 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 12 Jahre **UND** Fachgespräch	12 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 15 Jahre **UND** Fachgespräch
sowie	Erfolgreiche Teilnahme am Lehrgang „IT-Security-Analyst“ bei einem von der DCG anerkannten Bildungspartner oder gleichwertiger Nachweis.	Erfolgreiche Teilnahme am Lehrgang „IT-Security-Analyst“ bei einem von der DCG anerkannten Bildungspartner oder gleichwertiger Nachweis.
Rezertifizierung		
	2 unterschiedliche Berichte über IT-Sicherheitsanalysen, die im Laufe der Zertifikatsgültigkeit ausgearbeitet und erstellt wurden.	2 unterschiedliche Gutachten, die im Laufe der Zertifikatsgültigkeit ausgearbeitet und erstellt wurden.
sowie	Nachweis über mindestens 16 Lehreinheiten (1 LE = 45 Minuten) Auffrischungsschulung im zertifizierten Bereich.	Nachweis über mindestens 24 Lehreinheiten (1 LE = 45 Minuten) Auffrischungsschulung im zertifizierten Bereich.

Bitte beachten Sie unbedingt die folgenden Hinweise:

- Die Nachweise müssen vollständig und lesbar sein. Sollten die Nachweise aus mehreren Seiten bestehen, sind alle Seiten des Nachweises einzureichen.
- Die Nachweise sind in Kopie bzw. elektronisch einzureichen.
- Die Berufserfahrung orientiert sich an einer Vollzeitstelle von mindestens 35 Wochenstunden.
- Das Fachgespräch hat einen Umfang von ca. 20 Minuten.
- Der Lehrgangsanbieter für die Auffrischungsschulung ist frei wählbar.

Anlage 2 – Mindestanforderungen an die Erstellung eines IT-Security-Berichts

1. Bericht einer IT-Security Analyse

- Allgemeine Angaben
  - Deckblatt (Angaben zur/zum Verfasser:in, Untersuchungszeitraum, Auftraggeber:in usw.)
- Inhaltsverzeichnis
- Zusammenfassung
- Auftrag und Zweck
- Vorgehensweise
  - Beschreibung der Vorgehensweise
  - Beschreibung der Untersuchungsausrüstung
  - Beschreibung des Untersuchungsgegenstands
- Ergebnis der Schwachstellenanalyse
- Schlussbemerkung
  - Verschwiegenheitserklärung und Verbleib von Aufzeichnungen
- Literatur und Anlagen

Der Umfang des Berichts sollte zwischen 15 und 25 Seiten liegen. Bitte achten Sie auf Grammatik und Rechtschreibung sowie an ansprechendes und übersichtliches Layout.

Das Gutachten muss Ihre (digitale) Unterschrift enthalten.

Anlage 3 – Mindestanforderungen an die Erstellung eines Gutachtens der IT-Security

1. Formale Anforderungen an das Gutachten

1.1. Allgemeine Anforderungen an Gutachten

Ein Gutachten muss verständlich und nachvollziehbar sein. Maßstab hierfür ist ein:e fachlich unvorbereitete:r Dritte:r. Diese:r muss in der Lage sein dem roten Faden, der sich durch das Gutachten zieht, folgen zu können.

1.2 Lesbarkeit und Verständlichkeit eines Gutachtens

Gutachten sollen so erstellt werden, dass Dritte die Möglichkeit haben Notizen im Gutachten zu vermerken.

Die/der Sachverständige hat die äußerliche Gestaltung entsprechend der vom DIN für Veröffentlichungen aus Wissenschaft, Technik, Wirtschaft und Verwaltung des Normenausschusses, Bibliotheks- und Dokumentenwesen herausgegeben Normen vorzunehmen.

- Schriftart: Arial bzw. Times New Roman
- Schriftgröße: 11/12 pt
- linker Seitenrand 4 cm, rechter Seitenrand 3 cm.
- Zeilenabstand: 1,15 bis max. 1,5
- Eigenhändige Unterschrift im Gutachten
- Besiegelung des Gutachtens
- Bindung des Gutachtens, dass unerwünschte Änderungen, bzw. der Austausch oder das Entfernen einzelner Seiten oder Abschnitte nicht möglich ist

Der Vollständigkeit und Übersichtlichkeit entsprechen muss das Gutachten enthalten:

- Inhaltsverzeichnis mit Seitenzahlen
- Anlagenverzeichnis
- Kopf-/Fußzeile ab Seite 2
  - Name der/des Sachverständigen
  - Name des Auftraggebers
  - Gutachten-Nr.
  - Seitenzahl

1.3 Neutrale Sprache und Ausdrucksweise

Eine neutrale, sachorientierte und objektiv Ausdrucksweise ist zu verwenden. Dies gilt auch, in der Auseinandersetzung mit Feststellungen anderer Sachverständigen.

1.4 Angaben der Grundlagen/Quellen

Sachverständige haben die Grundlagen ihrer Tätigkeit deutlich zu machen. Dieses beinhaltet z.B. die Darstellung der rechtlichen und wirtschaftlichen Grundlagen der Gutachtenerstellung, als auch die Auseinandersetzung mit dem Stand der Wissenschaft und Technik.

Sofern die verwendeten Grundlagen auf eine Quelle zurückzuführen sind, so ist diese eindeutig anzugeben.

Die im Gutachten aufgeführten Quellen sind in einem Literaturverzeichnis anzugeben.

1.5 Angabe der angewandten Verfahren

Die angewandten Verfahren sind zu beschreiben und der Bezug zum Gutachtenauftrag ist herzustellen.

Sofern mehrere Verfahren in Betracht kommen, ist die getroffene Auswahl für ein Verfahren zu erläutern und zu begründen.

2. Gutachteninhalte und Gliederung

2.1. Das Deckblatt

Das Deckblatt eines schriftlichen Gutachtens enthält folgende Angaben:

- Name, Anschrift, Kontaktdaten der/des Sachverständigen
- Fachgebiet der/des Sachverständigen
- Bezeichnung „Gutachten“ mit zusätzlicher Spezifizierung der Gutachtenerstellung
- eindeutige Gutachtennummer
- Untersuchungszeitraum
- Erstellungsdatum des Gutachtens
- Nennung der auftraggebenden Partei
- Gesamtumfang des Gutachtens inkl. Anlagen
- Ggf. Aktenzeichen der auftraggebenden Partei oder des Gerichts
- Anzahl der Ausfertigungen / Nr. der Fertigung

2.3 Grundlegende Informationen zu Ausgangssituation und Kontext des Gutachtens

Zu einem Gutachten gehören Unterlagen, bei Gerichtsaufträgen in der Regel Gerichtsakten, die der/dem Sachverständigen ausgehändigt werden. Die Gerichtsakte wird in der Regel im Original ausgehändigt, die sonstigen Unterlagen in Kopie.

Sonstige Grundlagen des Gutachtens sind zu benennen und ggf. Auflagen zu verweisen:

- Beschreibung der Ausgangssituation
- Vollständige Nennung inkl. Anschrift des Auftraggebers/der Auftraggeberin
- Fragestellung / Beweisfragen der Auftraggeberin/des Auftraggebers
- Beschreibung des Gutachtenzwecks
- Bezeichnung aller von der auftraggebenden Partei zur Verfügung gestellten Unterlagen
- eigene Recherchen der/des Sachverständigen mit geeigneter Quellangabe
- verwendete Literatur, Normen mit Quellangaben (Titel, Autor, Verlag, Ausgabe/Auflage)

- verwendete Normen, Richtlinien
- verwendete Software
  - Produktname Software
  - bei Software-Versionsnummer (Release)
  - Kurzbeschreibung, wofür das Gerät verwendet wird bzw. wofür die Software verwendet wird

2.4 Ortsbesichtigung / Persönliche Inaugenscheinnahme

Ohne eine persönliche Inaugenscheinnahme (Ortstermin), kann in der Regel kein Auftrag ausgeführt werden. Eine Ausnahme ist dann gegeben, wenn z. B. die zu begutachtende Sache nicht mehr vorhanden ist (z. B. Diebstahl, Veräußerung usw.).

Die/der Sachverständige ermittelt auftragsgemäß den Zustand der zu begutachtenden Sache und beschriebt, was gesehen und vorgefunden wurde, ohne die Einflussnahme durch Dritte.

Im Gutachten führen Sachverständige aus, warum sie die Sache oder das Objekt untersucht haben, damit Prozessvertreter:innen, Parteien, Richter:innen oder Dritte verstehen, wie sie zu ihren Ergebnisem gekommen sind.

Die/der Sachverständige fast in der Beschreibung des Ortstermins seine Feststellungen zusammen. Dabei sollten folgende Angaben vorhanden sein.

- Ort und Datum des Ortstermins
- Teilnehmende Personen, sowie ggf. vor Ort eingesetzten Hilfskräfte
- Beginn und Ende des Ortstermins
- Anwesenheitszeiten der teilnehmenden Personen
- Beschreibung der vor Ort durchgeführten Maßnahmen und Feststellungen
- Nennung und Beschreibung der eingesetzten Hilfsmittel (z. B. Messgeräte usw.)

- Sollte eine Hilfskraft vor Ort eingesetzt werden, so ist deren Tätigkeit und Feststellungen zu nennen und ggf. zu beschreiben
- Nennung von Hinweisen der Beteiligten, die für Gutachtenbewertung von Relevanz sind

2.5. Beschreibung der zu begutachtenden Objekte

Einer der wichtigsten Punkte im Rahmen der Gutachtenerstellung ist die Beschreibung des zu begutachtenden Objektes. Sachverständige müssen sich in diesem Fall auf das Wesentliche beschränken und die für das Gutachten entscheidenden Tatsachen darstellen.

Bei den Gutachten im Bereich der Wertermittlung, IT-Forensic und IT-Security gelten u. a. folgende Mindestangaben.

2.5.1 Wertermittlung

Die charakteristischen Daten eines Systems sind anlagespezifisch. Sie geben Auskunft über Art und Typ des Gegenstands, seiner Leistungsfähigkeit, seiner Optionen und über seinen Hersteller bzw. Systemintegrator:in.

Sachverständige haben sicherzustellen, dass im Gutachten eine eindeutige Zuordnung möglich ist. Mindestens sollte jedoch enthalten sein:

- Typenschildangaben
  - Modell
  - Typenangabe
  - Charakteristische Leistungsmerkmale
- ggf. Betriebsanleitungen oder Handbücher
- ggf. Systemkonfigurationsunterlagen oder Dateien
- ggf. Anschaffungsbelegen
- ggf. Software
  - Betriebssystem
  - ggf. Anwendungssoftware (inkl. Versions-Nr., ggf. Service-Pack)

Im Bereich der IT-Security werden u. a. Konzepte erstellt. Art und Umfang der Konzeptionserstellung richten sich individuell nach den Vorgaben des Auftraggebers. Dabei kann es sein, dass auch nur einzelne Bereiche untersucht werden. Weiteren Unterteilungen sind jederzeit durch den Sachverständigen möglich.

Nachfolgende Bausteine geben eine Orientierung:

- Geschäftsprozesse
- IT-Systeme
- Gebäude/Räume
- Netze und Kommunikation
- Infrastruktur
- Anwendungen

2.6 Beschreibung der im Gutachten angewandten Verfahren

Aufgrund der besonderen Erfahrung in Sachgebiet, erkennen Sachverständige vorhandene Abweichungen und haben diese fachlich zu beschreiben. Insbesondere die durchgeführten Maßnahmen und Verfahren sind so zu beschreiben, dass sie für Laien verständlich sind. Die Maßnahmen wie auch die Verfahren sind nach dem jeweilig gültigen technischen Stand durchzuführen.

Sofern von den gängigen Verfahren abgewichen wird, ist dieses zu erläutern und das angewandte Verfahren so zu erklären, dass deutlich erkennbar ist, warum dieses und nicht das gängige Verfahren angewandt wird.

2.6.1 Wertermittlungsverfahren

In der Wertermittlung sind alle angewandten Verfahren zu beschreiben, die angewandten Wertermittlungsansätze und Begrifflichkeiten sind zu erläutern, z. B.

- Grundlagen der Zeitwert-, Verkehrswert-, Restwertberechnungen usw.
- Grundlagen der Zeitwert- und Gebrauchswertfaktors
- Grundlagen der Softwareberechnung
  - Standardsoftware
  - Individualsoftware
- Vorgehensmodell
- Schutzziele
- Definition des Gefährdungspotentials bzw. Risikoabstufungen

2.7 Analyse und Bewertung

Im Bereich der Bewertung und Analyse werden alle Feststellungen zu einem Ereignis formuliert. Es ist Aufgabe der/des Sachverständigen darauf hinzuweisen, ob nur dieses Ereignis eintreten kann oder ob noch Alternativen im Ergebnis möglich sind.

Im Einzelnen können Szenario Analysen zu einem wahrscheinlichen Ergebnis führen. Der Wahrscheinlichkeitsgrad soll hierfür angegeben werden.

Bei der Analyse und Bewertung soll so aufgebaut werden, dass Laien den Gedankengang der/des Sachverständigen folgen können. Die jeweiligen Bewertungskriterien sind zu nennen und zu begründen. Das Ergebnis ist zu erläutern und eine Plausibilisierung durchzuführen.

2.7.1 Zusätzlich in der Wertermittlung

- Zeitwertberechnung
  - Berechnung des Alters
  - Begründung der betriebsgewöhnlichen Nutzungsdauer
  - Berechnung und Erläuterung des Zeitwertfaktors
  - Auswahl und Begründung des Gebrauchswertfaktors
- Verkehrswertberechnung
  - Begründung für die Auswahl des Verfahrens
  - Angaben zum ermittelten Verkehrswert und Ableitung und Begründung der Vergleichswerte

Zusätzlich in der IT-Security

- Begründung und Erläuterung der Feststellungen
- Begründung und Definition der Schutzbedarfsfeststellung
- Empfehlungen zur Erhöhung des Schutzbedarfs (nach Best-Practice)

2.8 Zusammenfassung der Ergebnisse

Sachverständige haben nach dem Auftrag oder dem Beweisbeschluss seine Zusammenfassung zu formulieren und die Fragestellung zu beantworten.

Sie müssen davon ausgehen, dass immer zuerst die Zusammenfassung gelesen wird, da die auftraggebende Partei erst einmal an dem Ergebnis interessiert ist. Dies bedeutet, dass die Zusammenfassung kurz und knapp die wesentlichen und relevanten Ergebnisse des Gutachtens erläutert und zusammenfasst. Zur besseren Verständlichkeit wird die Fragestellung oder die Beweisfragen wiederholt und die dazu gehörenden Antworten daruntergeschrieben.

Inhalte einer Zusammenfassung:

- Kurze Beschreibung der Ausgangssituation und ggf. Informationen aus dem Ortstermin
- Wiederholung der Fragestellung / Beweisfragen
- Kurze, knappe und übersichtliche Antwort der Fragestellung / Beweisfragen

Erst wenn hier keine befriedigende Antwort gefunden wird, wird das Gutachten durch die Auftraggeberin/den Auftraggeber durchgearbeitet. Wobei es meist eine Partei gibt, die im Verfahren unterliegt und deren Prozessvertretung versucht, das Gutachten auszuheben. Somit sollte jedes Wort genau im Ergebnis formuliert werden.

In der Zusammenfassung dürfen keine neuen Erkenntnisse oder Ergebnisse vorhanden sein, die nicht im eigentlichen Gutachten abgehandelt worden sind.

2.9 Schlussbemerkungen

Gutachtenerstattung versichert werden.

Nach der Schlussformel wird

- das Erstellungsdatum
- die eigenhändige Unterschrift und
- Stempel

gesetzt.

2.10 Anlagen zum Gutachten

Die Anlagen des Gutachtens sollen es den Lesenden ermöglichen einen Zusammenhang zu anderen Punkten der Gutachtenerstattung zu erarbeiten.

Die/der Sachverständige hat als Anlage alle für die Bearbeitung des Sachverhalts notwendigen Unterlagen aufzuführen.

Ein:e sachverständige:r Dritte:r muss anhand der Unterlagen, das Gutachten mit den Feststellungen und dem Ergebnis nachvollziehen können.

Anlage 4. - KO-Kriterien für Beichte und Gutachten

1. Unvollständigkeit – Fehlen wesentlicher Teile des Berichts/Gutachtens

- Auftragsbeschreibung fehlt
- Darstellung der Befund- und Anknüpfungstatsachen fehlt
- Unterschrift/Stempel fehlt

1.1. Zusätzlich bei der Wertermittlung

- keine Begründung des ausgewählten Verfahrens
- keine Begründung der betriebsgewöhnlichen Nutzungsdauer
- keine Begründung des Gebrauchswertfaktors

- keine Erläuterung des angewandten Verfahrens
- keine Erläuterung der Schutzziele

2. Grundlegende Fehler in der Gutachtenerstellung

- unvollständige oder falsche Beantwortung der Fragstellung/Beweisfragen
- fehlende Begründung zur der Vorgehensmethode
- fehlende Offenlegung der Methodik (kein nachvollziehbarer und plausibler Lösungsweg)
- Rechenfehler oder falscher Rechenweg, falsche Analyseergebnisse
- wiederholte Rechenfehler, falsche Analysen
- fehlende Erläuterung der in den Verfahren herangezogenen Eingangsparameter

3. Mangelnde Sorgfaltspflichten

- mehrfach divergierende Angaben innerhalb des Gutachtens
- mangelhafte Rechtschreibung und Grammatik
- mangelhafter Stil oder Layout (z. B. keine Bindung, Pflichtangaben Gutachtendeckblatt)