2100

Informationstechnologie (IT)

Sachgebietseinteilung
Fachliche Bestellungsvoraussetzungen
Anlage 1: Darstellung der Sachgebietseinteilung
Anlage 2: Merkblatt zum Sachgebiet „IT – Schwerpunkt Software, insbesondere IT-Forensik

Stand: 04/2024
Revisionsnummer: 4
Erste Fassung: vor 1983

DIHK Deutsche Industrie- und Handelskammer
IfS

1 Sachgebietseinteilung und Bestellungstenor

Die Informationstechnologie (IT) hat alle Wirtschafts- und Lebensbereiche durchdrungen und besitzt eine wichtige Querschnittsfunktion.

Die Einteilung des interdisziplinären Sachgebiets beruht auf den Begrifflichkeiten eines durchschnittlichen IT-Anwendenden, der Sachverständigenleistungen nachfragt. Die Inhalte sind breit gefasst und offen formuliert, um dem schnellen technischen Fortschritt gerecht zu werden und darzustellen, welche Sachverständige in einem spezifischen Anwendungsbereich Leistungen erbringen können. Dabei wurde eine herstellerunabhängige und produktneutrale Formulierung gewählt, auch um neue Entwicklungen antizipieren zu können.

1.1 Die beiden Hauptgebiete der IT

In der IT ist es nicht möglich, in allen Bereichen gleichermaßen besonders sachkundig zu sein. Deshalb ist das Sachgebiet in die Schwerpunkte „Hardware“ und „Software“ eingeteilt. Die beiden Bestellungsgebiete lauten:

„IT - Schwerpunkt Hardware“
„IT - Schwerpunkt Software“

Dabei stehen die beiden Schwerpunkte nicht isoliert nebeneinander, sondern überschneiden sich. Oftmals wird erst im Rahmen der Begutachtung deutlich, welchem Schwerpunkt die aufgetretenen Probleme zuzuordnen sind. Um eine gutachterliche Fragestellung möglichst ganzheitlich betrachten und lösen zu können, benötigen Sachverständige daher gewisse Grundkenntnisse auch im jeweils anderen Schwerpunkt. Die Einteilung berücksichtigt somit das Bedürfnis der Nachfragenden von Sachverständigenleistungen, das fachliche Problem nicht exakt zuordnen zu können. Umgekehrt wird von Sachverständigen erwartet, dass sie über ein breites Fachwissen, viel Berufserfahrung und analytische Fähigkeiten verfügen.

1.2 Zusatzgebiete

Soweit Antragstellende besondere Kenntnisse in einem Zusatzgebiet nachweisen, kann dies - auf Antrag - im Bestellungstenor mit dem Zusatz „insbesondere...“ mit der Bezeichnung des Zusatzgebietes kenntlich gemacht werden. Derzeit bestehen folgende Zusatzgebiete, welche die oben genannten Anforderungen erfüllen und eine hinreichende Breite aufweisen:

Zusatzgebiete beim Schwerpunkt Hardware:
* Audio- und Videotechnik
* Automotive
* Netzwerke und Telekommunikation
* Rechenzentren

Zusatzgebiete beim Schwerpunkt Software:
* Enterprise Resource Planning (ERP)
* IT-Forensik
* IT-Sicherheit

Trend-Begriffe wie Web 3.0, Metaverse oder Quantencomputer sind bewusst nicht als Zusatzgebiete vorgesehen, da derzeit nicht absehbar ist, wie sich diese Bereiche entwickeln.

Beispiele für mögliche Tenorierungen mit Bezug auf die genannten Zusatzgebiete:
„IT - Schwerpunkt Hardware, insbesondere Rechenzentren“
„IT - Schwerpunkt Software, insbesondere IT-Forensik“
Eine grafische Darstellung der Sachgebietseinteilung befindet sich in Anlage 1.

1.3 Spezialgebiete

Für die Sachgebiete IT-Sicherheit (Sachgebietsnummer 2101) und IT-Forensik (Sachgebietsnummer 2102) bestehen eigene Bestellungsvoraussetzungen.

1.4 Andere Sachgebiete

Die „Informationstechnologie (IT)“ ist abzugrenzen zu folgenden Sachgebieten:
- Elektrotechnische Anlagen und Geräte
- Bestimmung der Exposition durch elektromagnetische Felder (EMF)
- Überprüfung von Geldspielgeräten
- Telekommunikation im Bereich Verbindungspreisberechnung

2 Vorbildung und praktische Tätigkeiten

2.1 Erforderlich ist entweder
ein erfolgreich abgeschlossenes Studium mit einer Regelstudienzeit von mindestens sechs Fachsemestern an einer Hochschule nach dem Hochschulrahmengesetz in den Fachrichtungen
- Informatik/Wirtschaftsinformatik
- Ingenieurwissenschaften
- Wirtschaftswissenschaften
- Wirtschaftsingenieurwissenschaften
- Physik
- Mathematik

bzw. entsprechende Kombinationen und eine mindestens fünfjährige praktische Tätigkeit, die ihrer Art nach geeignet war, die erforderlichen Kenntnisse zu vermitteln,

oder

bei Antragstellenden ohne Hochschulabschluss der Nachweis von Erfahrung, Aus- und Fortbildung sowie regelmäßig einer 10-jährigen praktischen Tätigkeit, die ihrer Art nach geeignet sind, die erforderlichen Kenntnisse zu vermitteln.

2.2 In allen Fällen haben Antragstellende nachzuweisen, dass sie in fach-verantwortlicher Stellung in der IT tätig sind und sich mit Themen wie z. B. Zeit, Kosten, Qualität, Markt, Branchenüblichkeit, Stand der Technik, auseinandergesetzt haben. Das erforderliche Erfahrungsniveau wird u. a. durch folgende Tätigkeiten gekennzeichnet:
- Umfassende Systementwicklungen auf dem entsprechenden Schwerpunktgebiet
- Erarbeitung umfangreicher Dokumentationen
- Erarbeitung umfangreicher Pflichtenhefte
- Projektmanagement für anspruchsvolle Aufgaben
- Erstellung von Gutachten oder vergleichbaren schriftlichen Ausarbeitungen.

2.3 Antragstellende sollen eine mindestens dreijährige einschlägige praktische Tätigkeit als Sachverständige/r nachweisen. Diese Tätigkeit darf - vom Zeitpunkt der Antragstellung an gerechnet - nicht länger als ein Jahr zurückliegen.

2.4 Die vorerwähnten Voraussetzungen sind durch Vorlage von mindestens fünf Gutachten nachzuweisen. Davon müssen mindestens zwei eine schuldrechtliche Fragestellung behandeln, wie sie beispielsweise häufig in einem Zivilprozess auftritt. Sofern Antragstellende ein Hauptgebiet mit einem Zusatzgebiet (z.B. „IT – Schwerpunkt Software, insbesondere …….“ oder „IT – Schwerpunkt Hardware, insbesondere …….“) beantragen, müssen sich zwei der fünf einzureichenden Gutachten auf das Zusatzgebiet beziehen.

Zum Aufbau eines Gutachtens wird auf die jeweilige Sachverständigenordnung sowie auf die „Hinweise zum Aufbau eines schriftlichen Sachverständigengutachtens” verwiesen.

3 Allgemeines

Antragstellende haben zum Nachweis der besonderen Sachkunde Kenntnisse in den jeweils angegebenen Vertiefungsgraden nachweisen:

Grundkenntnisse (G)
Vertiefte Kenntnisse (V)
Detailkenntnisse (D)

Die bei den Fachkenntnissen (Ziff. 5) und Zusatzgebieten (Ziff. 6) in Klammern angegebenen Beispiele dienen lediglich zur Erläuterung. Sie erheben keinen Anspruch auf Vollständigkeit.

4 Allgemeine Kenntnisse

4.1 Rechtsgrundlagen

Die „Allgemeinen Rechtskenntnisse Sachverständigentätigkeit“ sind Bestandteil dieser Bestellungsvoraussetzungen.

Darüber hinaus sind folgende spezielle Rechtskenntnisse nachzuweisen:

a) einschlägige versicherungsrechtliche Vorschriften (G)
b) einschlägige Vorschriften des Ordnungswidrigkeitenrechts (G)
c) einschlägige Vorschriften des Strafrechts (§§ 11 Abs. 3, 184 a-d, 202 a-c, 206, 263a, 266b, 268, 269, 270 StGB) (G)
d) weitere einschlägige Straftatbestände (UWG, UrhG, HGB, AO) (G)
e) forensisches Vorgehen bei Datensicherung und Auswertung (Umgang mit Beweismitteln, Anfertigung von Kopien, Prüfsummen, Protokollierung) (G)
f) Datenschutzgesetze (V)

4.2 Wert- und Kostenbegriffe im Sachverständigenwesen

Die für das Sachgebiet einschlägigen Wert- und Kostenbegriffe müssen bekannt sein (vgl. Glossar „Wert- und Kostenbegriffe“ https://www.muenchen.ihk.de).

5 Fachkenntnisse

Von den Sachverständigen wird erwartet, dass sie vor allem Störungs- und Ausfallmechanismen innerhalb des gesamten Spektrums ihres/seines Sachgebietes kennen und aufgrund ihres systematischen Fachwissens ermitteln und nachvollziehbar beschreiben und bewerten können.

Sachverständige müssen in ihrem Schwerpunkt über folgende Kenntnisse verfügen:

a) Allgemein anerkannte Regeln der Technik (D)
b) Stand der Technik (D)
c) marktgängige Standards (V)
d) verbreitete Produkte (V)
e) Branchenüblichkeit (V)
f) Entwicklungstendenzen (V)

5.1 Schwerpunkt Hardware

5.1.1 Grundlagenwissen (G)

a) Physik (grundlegende Begriffe und Gesetze der Elektrodynamik, Optik, Akustik, Mechanik)
b) Elektrotechnik (Ströme und Spannungen in elektrischen Netzwerken, Wechsel-stromtechnik, Filterschaltungen, Schwingkreise, elektrische und magnetische Felder)
c) Werkstoffe (physikalisch-chemische Materialeigenschaften von Metallen, Halbleitern, Isolatoren)

d) Messtechnik (elektrische Messung physikalischer Größen, Prinzip und Aufbau von Messsystemen, Systemoptimierung und Fehlerkorrektur, Standard-Messgeräte)
e) Mathematik (Logische Grundlagen (Bool'sche Algebra))
f) IT-Sicherheit (insbesondere KRITIS) (V)

5.1.2 Hardware

5.1.2.1. Bauelemente (V)

Aufbau, Wirkungsweise und Dimensionierung der wesentlichen elektrischen und elektronischen Bauelemente:

a) passive Bauelemente
b) aktive Bauelemente
c) elektromechanische Bauelemente
d) elektrochemische Bauelemente

5.1.2.2. Baugruppen/Geräte (V)

Technologie, Aufbau und wesentliche Funktionen von Baugruppen und Geräten der Informationstechnologie:

a) Rechner-/Steuereinheiten
   aa) Prozessortypen und Kennwerte
   bb) Speichersysteme
   cc) Bus-Systeme
   dd) Schnittstellen
   ee) Montage, Verkabelung
   ff) Speicherprogrammierbare Steuerung (SPS)
   gg) Mobile Endgeräte

b) Peripherie
   aa) Massenspeicher (Festplatte, Band, CD, DVD, Halbleiter)
   bb) Eingabegeräte (Lesegeräte, Scanner)
   cc) Ausgabegeräte (Drucker, Displays)
   dd) Video- und Audiogeräte

5.1.2.3. Netzwerktechnik (V)

a) Übertragungsverfahren
b) Topologien
c) Komponenten (Hub, Switch, Router)
d) Signalübertragung (physikalische und logische Ebenen)

5.1.2.4. Betrieb von Geräten und Anlagen (V)

a) Erforderliche Energieversorgung (Schutzmaßnahmen)
b) Erforderliche Umgebungsbedingungen, Kühlung
c) Schäden an Geräten/Anlagen (Überspannung, Wasser, Feuer, Staub)
d) Sanierung von Schäden an Geräten und Anlagen
e) Elektrische Störungen in Art, Entstehung, Ausbreitung und Wirkung (EMV)

5.1.3. Software (G)

a) Rechnerarchitekturen/Peripherie
b) Betriebssysteme (Embedded, Real Time Operating Systems)
c) Microcode (Firmware), Assembler
d) Datensicherheit (Zugriffsschutz, Übertragungssicherheit, Kryptographie)
e) Datensicherung (Verfahren, Lagerung, Datenrettung)

f) Netzwerke (LAN, WAN, Internet)
g) Bedrohungen (Hacking, Viren) und Schutzmechanismen (Firewall)
h) Audio, Video, Grafik
i) Datenverwaltung
j) Protokolle

5.2 Schwerpunkt Software

5.2.1 Grundlagenwissen

5.2.1.1. Informationstechnik (G)

a) Grundlagen (Berechenbarkeit, Grammatiken, Komplexitätstheorie, Informationsgehalt, Logik)
b) Modellierung (Abstraktion, Graphen, Strukturen, Prozesse)
c) Querschnittsverfahren (IT-Sicherheit, Change-Management, Datenschutz)
d) Programmierparadigmen
e) Algorithmen und Datenstrukturen

5.2.1.2. Betriebswirtschaft (G)

a) Grundbegriffe (Wirtschaftlichkeit, Aufwand und Ertrag)
b) Unternehmensaufbau und Management (Organisation, Geschäftsprozesse, Finanzen, Investitionsrechnung, internes und externes Rechnungswesen, Einkauf, Leistungserstellung, Materialwirtschaft, Vertrieb, Service und Marketing)

5.2.2 Software

5.2.2.1 Softwareengineering

a) Agile und herkömmliche Vorgehensmodelle (D)
b) Spezifikationsmethoden (D)
c) Programmiersprachen (V)
d) Technischer Systementwurf (V)
e) Arten der Dokumentation (V)
f) Datenbankentwicklung und Datenbankdesign (D)
g) Qualitätssicherung / Test (D)
h) Datenmigration (V)
i) Projektmanagement (D)
j) Schnittstellen (V)
k) Entwicklungsumgebungen (D)
l) Software-Engineering-Werkzeuge (D)
m) Systemumgebungen (V)
n) Systemarchitekturen (D)
o) Requirements Engineering (V)
p) Change Request-Verfahren (V)

5.2.2.2. Systemsoftware (V)

a) Betriebssysteme (Prozesse, Verteilte Systeme, Client-Server-Systeme, Synchronisation, Unterscheidungsmerkmale aktueller Systeme)
b) Datenbankmanagementsysteme (DBMS) (Datenbankmodelle, Abfragesprachen, Transaktionsverwaltung, Datenintegrität, Data Warehouses)
c) Middleware
d) Virtualisierungssysteme

5.2.2.3. Einsatz von Software (V)

a) Standardsoftware (branchenübergreifende Lösungen, branchenspezifische Lösungen, ERP-Systeme, Enterprise Kollaboration, E-Business-Systeme, Einführung)
b) Individualsoftware (Einführung)
c) Pflege und Wartung (Support-Organisation, Sourcing)
d) Dokumentation (organisatorisch, rechtlich)
e) Projekte (Organisation und Projektmanagement, Abnahme, Vorgehensmodelle)
f) Systemgestaltung (Usability, Gestaltungsprozesse)
g) Integration und Interoperabilität betrieblicher Anwendungssysteme
h) Auswirkungen des IT- Einsatzes (Folgen, Risiken und Gefährdungspotentiale)

5.2.3 Betrieb von Systemen (Rechenzentren, Administration) (V)

a) IT Service Management Best Practices
b) Service Level Agreements
c) Leistungs- und Abrechnungsformen
d) Fragestellungen bei Outsourcing und externer Datenspeicherung (organisatorisch, rechtlich)
e) Konfigurationsmanagement
f) Betrieb komplexer Systeme

5.2.4 Hardware (G)

a) Computer (Rechnerorganisation, Rechnerarchitektur)
b) Peripheriegeräte (Speichersysteme, Datenein- und -ausgabegeräte)
c) Datenübertragung und Vernetzung (Konzepte, Möglichkeiten und Verfahren zur Ver-bindung von Standorten, Daten- und Telekommunikation)
d) Fehlertoleranz (Verfügbarkeit, technische Möglichkeiten)
e) Energieversorgung und Elektrotechnik (im Zusammenhang mit Hardwarekomponenten und Datenübertragung)

6 Zusatzgebiete

6.1 Schwerpunkt Hardware

6.1.1 6.1.1. Audio- und Videotechnik

Audio- und Videotechnik haben sich aus ihrem klassischen Bereich der Ton- und Bildaufzeichnung hin zu komplexen Systemen entwickelt, z.B. für industrielle Qualitätssicherung, für Zutrittskontrolle oder Objektschutz. Software spielt hierbei eine zunehmende Rolle.

a) Hardware (V)
   aa) Aufnahmegeräte (Audio/Video)
   bb) Aufzeichnungsgeräte (Audio/Video)
   cc) Schnittstellen
   dd) Managementsysteme
   ee) Datenformate
   ff) Kompressionsverfahren
   gg) Übertragungsverfahren/Normen

b) Software (V)
   aa) Verschlüsselungsverfahren
   bb) Streamingverfahren
   cc) Videosensorik
   dd) Analysemodule
   ee) Biometrische Verfahren

ff) Bildbearbeitung
gg) Konferenzsysteme

c) Betrieb von Anlagen (V)
aa) Datenschutz
bb) Betrieb von Sicherheitsanlagen

6.1.2 Automotive

Im Zusatzgebiet "Automotive" geht es im Wesentlichen um die Funktion, Wirkung, Fehler und Mängel der Steuergeräte, die in Fahrzeugen eingebaut sind. Steuergeräte gibt es für die unterschiedlichsten Aufgaben und mit völlig unterschiedlicher Leistungsfähigkeit. Beispiele sind: Tastenmodule, intelligente Sensoren, Motorsteuergeräte, sicherheitsrelevante Steuergeräte und Assistenzsysteme, Navigation-, Video-Audio-Systeme.

a) Fahrzeugzustand und Verhalten der Steuergeräte (D)

b) Hardware
aa) Aufbau der Steuergeräte (Sensoren, Steckverbindungen) (D)
bb) Microcontroller (G)
cc) Bus-Technologie (V)
dd) Funktion und Schnittstellen von Sensoren und Aktoren (V)
ee) Spannungsversorgung in Fahrzeugen (D)
ff) Umwelteinflüsse auf Elektronik in Fahrzeugen (D)

c) Diagnose und Einstellmöglichkeiten von Steuergeräten (V)
aa) Diagnosegeräte
bb) Sicherheit und Manipulationsmöglichkeiten

d) Software (G)
aa) Struktur und Aufbau der Software der Steuergeräte
bb) Funktionale Sicherheit

6.1.3 Netzwerke und Telekommunikation

Netzwerke spielen im heutigen Informationsverarbeitungsprozess eine zentrale Rolle. Ihre Bedeutung und Anwendungsbreite wachsen ständig. Sachverständige müssen Kenntnisse in allen Netzwerkschichten haben. Beispiele sind die Auslegung eines Funknetzes, die Verknüpfung internationaler Unternehmensstandorte, Anforderungen bei der Nahfeld-kommunikation (NFC, RFID) und Next Generation Networks (NGN) sowie das IO Multimedia Subsystem der 3GPP.

Das Zusatzgebiet umfasst auch Telekommunikationsanlagen, die jedoch aufgrund der fortschreitenden Technik an Bedeutung verlieren.

In Anlehnung an das OSI-Schichtenmodell sind hier folgende Schwerpunkte zu nennen:

a) Kommunikationsmodelle Nachrichtenübertragungssysteme
aa) Nachricht, Signal, Störgrößen (G)
bb) OSI 7-Schichtenmodell (V)
cc) Verkehrstheorie, Dämpfung, Pegelrechnung (V)
dd) analoge/digitale Signalübertragung (V)
ee) Raum-/Zeit-/Frequenzmultiplex (V)

b) Übertragungsmedien (Schicht 1)
   aa) elektrisch (Fernkabelnetz, Teilnehmeranschlussnetz, Breitbandkabelnetz, Busverkabelungen) (D)
   bb) optisch (Multimode, Single Mode, WDM) (V)
   cc) Funk (Frequenzspektren, Modulationsverfahren) (V)

c) Sicherungsmechanismen (Schicht 2)
   aa) Übertragungsverfahren (PDH, SDH, ATM, DOCSIS, xDSL, Ethernet, MPLS) (D)
   bb) Synchronisationsverfahren, Punkt zu Punkt - / Punkt zu Mehrpunkt- Technologien, Flusssteuerung, Überlastverhalten (D)
   cc) Authentifizierungsprotokolle, Verschlüsselung (D)

d) Vermittlungssysteme (Schicht 3)
   Vermittlungsprotokolle (IPv4, IPv6, ICMP, IGMP, OSPF, BGP, SIP, ISDN, X.25) (D)

e) Transportsteuerung /-sicherung (Schicht 4)
   Protokolle der Verbindungssteuerung (TCP, UDP, RSVP, Diffserv) (D)

f) Weitere Schichten
   spezielle Funknetze (BOS) (V)

g) Bedrohungen, Forensik
   Messtechnik, Protokollanalysatoren (Cace Pilot/Riverbed, Wireshark), Werkzeuge der Netzelemente (D)

h) Telekommunikationsanlagen (G)
   aa) Telekommunikations-Endgeräte
   bb) lokal vermittelnde Anlagen und Systeme
   cc) Strukturen lokaler TK-Systeme
   dd) Sicherheitskonzepte von ITK-Systemen
   ee) Schutz gegen Überspannungseinflüsse

Neben den theoretischen Grundlagen sind auch Kenntnisse erforderlich, wie das Zusammenwirken zwischen unterschiedlichen Telekommunikationsdienstanbietern in Deutschland praktisch realisiert wird. Beispielhaft sind hier

- die Spezifikation des „Arbeitskreises Nummerierung und Netzzusammenschaltung“ (AKNN) (G) und
- die darauf aufbauende Realisierung des Netzzusammenschaltungsproduktes der Deutschen Telekom AG (siehe „Leistungsbeschreibung L2-BSA-Transport und L2-BSA-Übergabeanschluss“, verfügbar im Internet) (G)

zu nennen.

Aufgrund der zunehmenden Bedeutung der Telekommunikationsnetze für das Gemeinwohl ist aber auch die Kenntnis der gesetzlichen und regulatorischen Vorschriften zum Betrieb derartiger Infrastrukturen erforderlich. (G)
Diesbezüglich wird insbesondere auf den Katalog von Sicherheitsanforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) hingewiesen.

6.1.4 Rechenzentren

Als Rechenzentren werden sowohl Gebäude als auch Räumlichkeiten bezeichnet, in denen zentrale Informationstechnologie (Server, Storage, Netzwerk, Telekommunikationssysteme) betrieben wird. Zentraler Inhalt des Zusatzgebietes „Rechenzentren“ ist neben der Kenntnis der Funktion und Wirkungsweise der einzelnen Elemente ihre Differenzierung und das Erkennen möglicher Schwachstellen, die zu Fehlfunktionen führen können, inkl. der anzuwendenden Mess-/Nachweismethoden.

a) Energieversorgung der Rechenzentren
   - aa) Aufbau der primären und sekundären Stromversorgung der Rechenzentren (G)
     Unterbrechungsfreie Stromversorgung (USV) (V)
     Netzersatzanlagen (NEA) (V)
   - bb) Baugruppen der Stromversorgung (V)
   - cc) Bauelemente und Details der Stromversorgung (D)

b) Klimatisierung der Rechenzentren
   - aa) Grundlagen der Klimatisierung (Feuchtigkeit, Volumenstrom, Regelsysteme) (V)
   - bb) Aufbau und Funktion der Klimatisierung von Rechenzentren (G)
   - cc) Baugruppen der Klimatisierung (G)

c) Meldesysteme (Anforderungen) (G)
   - aa) Brandmeldeanlage (BMA)
   - bb) Einbruchsmeldeanlage (EMA)
   - cc) Alarmpläne

d) IT-Sicherheit (V)
   - aa) Datensicherheit
   - bb) Zutrittskontrolle (Vereinzelungsanlagen, Biometrie, Wachdienst, Kartensysteme)

e) Bauliche Anforderungen (G)
   - aa) Brandschutz
   - bb) Einbruchschutz (Perimeterschutz, Video)
   - cc) Doppelboden (Druck, Öffnungen, Lüftungsbodenplatten, Flächenlast, Punktlast)
   - dd) Löschanlagen

f) Redundanzen (G)

g) Zertifizierung und Klassifizierung (G)

6.2 Schwerpunkt Software

6.2.1 eBusiness

Dieses Zusatzgebiet konzentriert sich auf den elektronischen Geschäftsverkehr. Sachverständige müssen die fachlichen Prozesse, Anwendungen und Technologien von der digitalen Bestellung von Waren und Dienstleistungen bis hin zur Fakturierung, elektronischen Bezahlung und Buchhaltung kennen.

a) Standards
   - aa) Varianten des elektronischen Geschäftsverkehrs (D)
   - bb) Internetprotokolle (V)
   - cc) Besondere rechtliche Rahmenbedingungen des eBusiness (OSS, Absatzrichtlinien, Handelsverbote)

dd) Datenschutz (V)

b) Technologien
aa) Entwicklungs-Frameworks für Web-Anwendungen (Client- und Serverseite) (V)
bb) Optimierte Medienformate (Bild, Video, Ton) (V)
cc) Technische-Verfahren des Online-Trackings (D)

c) Prozesse und Anwendungen
aa) Online-Bestellsysteme (B2B) (V)
bb) Online-Shops / Auktionsplattformen (B2B und B2C) (D)
cc) Payment-Systeme (Technologie, Anbieter, Abwicklungsstrukturen) (D)
dd) Datenaustausch zwischen Online-Plattformen und Warenwirtschaftssysteme (V)
ee) Datenaustausch zwischen Online-Plattformen und Finanzbuchhaltung (V)
ff) Lagerwirtschaft (G)
gg) Logistik / Versand (V)
hh) CRM (G))
ii) Dokumentenmanagement (Formen von Dokumenten, Technologien, Anwendungen) (G)
jj) Remarketing (V)

d) Suchmaschinenoptimierung (SEO)/Suchmaschinenmarketing (SEM) (V)
aa) Optimierungsmethoden (On-Page/Off-Page)
bb) Relevante Suchmaschinen und Werbeplattformen
cc) Preismodelle

e) Social Media Marketing (V)
aa) Rechtliche Rahmenbedingungen
bb) Marketing-Kanäle
cc) Geschäftsmodelle

6.2.2 Enterprise Resource Planning (ERP)

Dieses Zusatzgebiet konzentriert sich auf die zahlreichen, komplexen und miteinander kommunizierenden Anwendungssystemen, die zur Unterstützung der Ressourcenplanung eines ganzen Unternehmens eingesetzt werden (ERP). Sachverständige müssen die grundsätzlichen fachlichen Prozesse der betroffenen Branchen kennen. Darüber hinaus müssen Sachverständige fundierte Kenntnisse von üblichen Lizenzmodellen, Kommunikationsmechanismen und Datenbanken sowie entsprechende Programmierkenntnisse besitzen.

a) Allgemeine Kenntnisse
aa) Einführungsstrategien für ERP-Systeme (D)
bb) Geschäftsprozessmodellierung (V)
cc) Ablauforganisation und Organisationseinheiten (G)
dd) Customizing / Parametrisierung (V)
ee) Lizenzmodelle (G)

b) Module eines ERP-Systems (V)
aa) Stammdatenverwaltung
bb) Rechnungswesen und Controlling
cc) Personalwirtschaft
dd) Warenwirtschaft
ee) Produktdatenmanagement
ff) Vertriebsprozesse(V)
gg) Produktionsplanung und -steuerung

hh) Dokumentenmanagement
ii) Archivierung

6.2.3 IT-Forensik

Die IT-Forensik bettet die Sicherung, Analyse und Präsentation digitaler Spuren in den Rahmen der klassischen forensischen Wissenschaften ein. Dazu sind Kenntnisse im forensisch korrekten Vorgehen erforderlich. Gleichzeitig werden Informatikkenntnisse benötigt, um digitale Spuren und Daten verschiedenster Art und Abstraktionsebenen erfassen und forensisch korrekt bewerten zu können. Der Umgang mit forensischen Werkzeugen wird vorausgesetzt.

a) Allgemeine Kenntnisse
- aa) Grundsätzliche Prinzipien der IT-Forensik (Grundlegende Definitionen, Chain of Custody, Nature of Evidence, Locard’sche Regel, Prozessmodelle) (D)
- bb) Verwaltung von Asservaten (V)
- cc) Kryptologie (Prinzipien, Verfahren, Anwendungen, Sicherheit) (V)
- dd) Hashfunktionen, Hashwerte (V)
- ee) Internet-Kommunikation (E-Mail, Chat, Messaging) (D)
- ff) Bild- und Videoformate (JPEG, MPEG, EXIF) (D)
- gg) Digitale Signaturen und Schlüsselverwaltungssysteme (V)
- hh) Dateisysteme (FAT, NTFS, EXT2, EXT3, HFS, ReiserFS, EXT4, XFS) (V)
- ii) Datenträger (magnetische, optische, Halbleiter) und Datenträgerverbünde (z.B. RAID, JBOD, SAN) (V)
- jj) Virtualisierungssysteme (VMWare, Virtual PC, Citrix) (V)
- kk) Cloudsysteme (Modelle, Strukturen, Zugriffs-, Sicherungs-, Analysemöglichkeiten) (V)
- ll) Datentypen und Kodierungen (INTEGER, LONG, FLOAT, DOUBLE) (V)
- mm) Netzwerk-Topologien (V)
- nn) Kommunikations- und Anwendungsprotokolle (TCP/IP, DNS, DHCP, SMTP, POP/IMAP, HTTP, SSL/TLS) (V)
- oo) P2P-Systeme (Filesharing-Netzwerke und Client-Programme) (D)
- pp) Internet-Browser (MS Edge, Chrome, Safari, Opera, Mozilla) (D)
- qq) Betriebssysteme (MS Windows, Linux, UNIX, iOS, Android, Mac OS) (V)

b) Prozess und Vorgehensweise
- aa) Planung von Sicherstellungsmaßnahmen (D)
- bb) Schreibschutzmaßnahmen (D)
- cc) Forensische Datensicherungsformate (V)
- dd) Sicherung flüchtiger Datenbestände (RAM, Cold Boot) (V)
- ee) Tools zur Datensicherung von mobilen Endgeräten und Rechnersystemen (D)
- ff) Analyse verschlüsselter Daten (Rainbow-Tables, Brute Force, Dictionary) (D)
- gg) Tools zur Auswertung (D)
- hh) Anwendungsforensik (Artefakte aus Prefetch-, Cache-, History-, Cookie-, Bookmark-, Auslagerungs-Bereichen etc.) (D)
- ii) Analyse unbekannter Anwendungen und deren Spuren (V)
- jj) Timeline (Quellen, Konsolidierung, Analysen) (D)
- kk) Auswertung von Konfigurationsdateien (Registry, INI-Files, .conf-Dateien) (D)
- ll) Auswertung von Protokoll-Dateien (Event-Logs, Sys-Logs) (D)
- mm) Rechtliche und ethische Rahmenbedingungen (V)
- nn) Datenschutz (V)
- oo) Aufbereitung der Erkenntnisse (Inhalt, Darstellungsformen, Trennung von Tatsachen und Ableitungen) (D)
- pp) Unterschiede bei der Beauftragung von Sachverständigen und bei der Art der Gutachtenerstattung im Zivilrecht und im Strafrecht, Abgrenzung zur Beauftragung als Ermittler (V)

c) Besondere rechtliche Kenntnisse (V)
   aa) Wirtschaftsstraftaten, Betrug, Untreue, Rechtsstaat gefährdende Straftaten, Sexualstraftaten (unter anderem Kinderpornographie)
   bb) Kenntnisse im Strafrecht und Strafprozessrecht (z. B. Verfahrensweisen im Ermittlungsverfahren, Auswertungsmöglichkeiten und Beweisverwertungsverbote)
   cc) Urheberrechtsstraftaten, IT-Strafrecht, Telekommunikationsgesetz und Überwachung der Telekommunikation
   dd) Täterterminologie

6.2.4 IT-Sicherheit

Die IT-Sicherheit umfasst die Sicherheit von Informationen und Systemen, die am gesamten Zyklus der Informationsverarbeitung (Erfassung, Speicherung, Verarbeitung, Kommunikation, Löschung) beteiligt sind. Entsprechend sind Kenntnisse im Bereich der Sicherheitsgrundlagen erforderlich, welche in der Breite auf die IT-Einsatzgebiete übertragen und angewendet werden müssen.

a) Allgemeine Kenntnisse
   aa) Schutzziele, Schwachstellen, Bedrohungen, Angriffe, rechtliche Rahmenbedingungen (D)
   bb) IT-Forensik (G)
   cc) Sicherheitsrichtlinien (IT-Sicherheitsgesetz), Sicherheitsinfrastruktur (V)
   dd) Governance (G)
   ee) Compliance (G)

b) Spezielle Bedrohungen (V)
   aa) Grundlagen, Angriffe, Gegenmaßnahmen zu relevanten Bedrohungen
   bb) Malware (Viren, Würmer, Trojaner)
   cc) Bot-Netze
   dd) Spam, Phishing
   ee) Denial-of-Service
   ff) Mobiler Code, Mobile Apps

c) Netzwerk- und Internet-Sicherheit
   aa) Kommunikationsgrundlagen (Klassen, Adressierungsarten, Topologien) (G)
   bb) ISO/OSI-Referenzmodell, TCP/IP-Referenzmodell (Schichten, Protokolle, Dienste) (D)
   cc) Firewall-Technologie (Paketfilter, DMZ, Proxy) (D)
   dd) OSI-Sicherheitsarchitektur (V)
   ee) Sichere Kommunikation (VPN, IPSec, SSL/TLS) (D)
   ff) Sichere Anwendungsdienste (E-Mail, Zahlungsverkehr) (D)
   gg) Web-Anwendungen (aktive Inhalte, Websockets, OWASP Top-Ten) (D)
   hh) Mobile und drahtlose Kommunikation (GSM, UMTS, LTE, WLAN, Bluetooth, RFID, NFC) (D)
   ii) Cloudsysteme (D)
   jj) Analysewerkzeuge und Systemhärtung (Überwachung, Intrusion Detection, Intrusion Prevention, Data Leakage Prevention, SIEM) (D)

d) Betriebssystem-Sicherheit
   aa) Aufgaben, Arten und Aufbau von Betriebssystemen (D)
   bb) Administration, Rechtevergabe, Zugriffskontrolle (V)
   cc) Trusted Computing, Sicheres Booten (V)
   dd) Monitoring und Logging (V)
   ee) Analysewerkzeuge und Systemhärtung (V)

e) Kryptologie, Hashfunktionen, Signaturen
   aa) Grundlagen, Prinzipien, Methoden (V)
   bb) Informationstheorie (G)
   cc) Symmetrische, asymmetrische und hybride Verfahren (Triple-DES, AES, RSA, ECC) (D)
   dd) Kryptografische Hashfunktionen (Grundlagen, Verfahren) (D)
   ee) Elektronische Signaturen (Verfahren, Standards, Signaturgesetz) (D)

f) Schlüsselmanagement, Authentifikation, Digitale Identität
   aa) Zertifizierung (Zertifikate, PKI) (D)
   bb) Schlüssel (Erzeugung, Aufbewahrung, Vernichtung, Austausch, Rückgewinnung) (D)
   cc) Authentifikation durch Wissen (Passwort-, Challenge-Response, Zero-Knowledge-Verfahren) (D)
   dd) Authentifikation durch Biometrie (Rechtsgrundlagen, Technik) (D)
   ee) Authentifikation in verteilten Systemen (Radius, Kerberos) (D)
   ff) Smartcards (Architektur, Betriebssystem) (V)
   gg) Elektronische Identifikationsausweise (D)
   hh) Second Factor Authentifizierung (D)

g) Security Engineering, Bewertungskriterien, Sicherheitsmodelle
   aa) Sicherer Entwicklungsprozess (V)
   bb) Strukturanalyse, Schutzbedarfsbestimmung, Bedrohungsanalyse, Risikoanalyse (V)
   cc) Sicherheitsarchitekturen und Betrieb (V)
   dd) Security Development Lifecycle (V)
   ee) Bewertungskriterien (TCSEC, ITSEC, Common Criteria, Zertifizierungen) (V)
   ff) Sicherheitsmodelle (Klassifikation, Zugriffskontroll-, Informationsfluss-Modelle) (D)
   gg) IT-Sicherheitsmanagement (ITSM) (D)

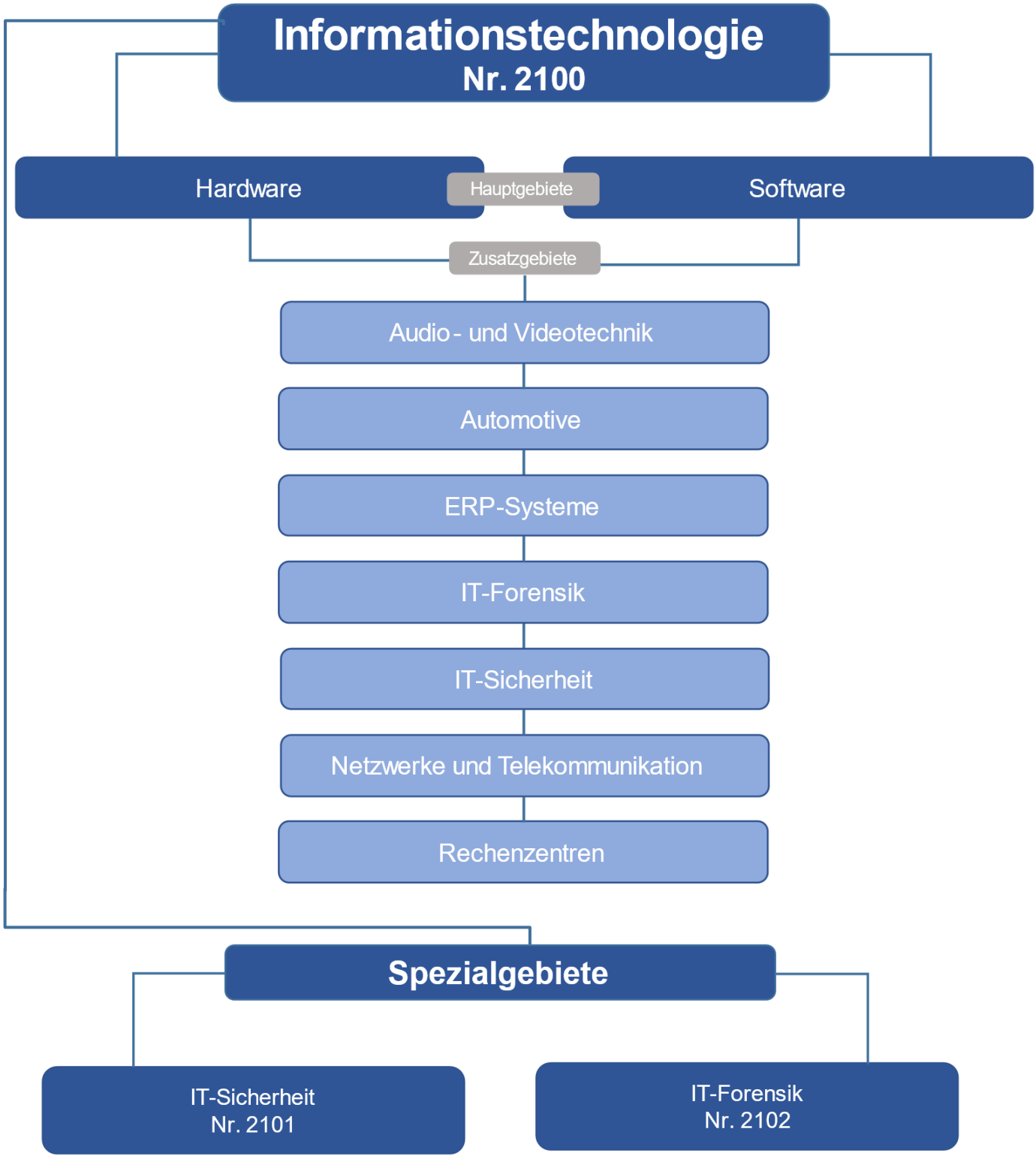
h) Datenschutz (D)
   aa) Rechtsgrundlagen (national/international)
   bb) Umsetzung (technisch/organisatorisch)
   cc) Kontrolle

7 Technische Ausstattung

Sachverständige müssen über eine angemessene IT-Ausrüstung verfügen, die es ihnen erlaubt, Programme, Komponenten, Geräte und Rechner (auch im Verbund) zu prüfen. Sie müssen mit der Bedienung und den Funktionen der Systeme auf Hard- und Software-Ebene vertraut und in der Lage sein, Systeme selbst einzurichten. Sachverständige müssen mit dieser Ausrüstung Sachverhalte zuverlässig dokumentieren können.

Zusätzlich wird für den Schwerpunkt Hardware von den Sachverständigen erwartet, dass sie mit der Handhabung und Bedienung grundlegender Messgeräte vertraut sind und mindestens Zugriff auf, besser aber Eigenbesitz an diesen Geräten haben.

Anlage 1: Darstellung der Sachgebietseinteilung



Anlage 2:
Merkblatt zum Sachgebiet „IT – Schwerpunkt Software, insbesondere IT-Forensik“

Einleitung
Staatsanwaltschaften und Kriminalpolizei beauftragen vermehrt öffentlich bestellte und vereidigte IT-Sachverständige mit der Auswertung beschlagnahmter Hardware und mit der Datenrecherche. Dabei geht es um die Aufklärung von Straftaten im Bereich der Wirtschaftskriminalität, strafbaren politischen Extremismus, Terrorismus sowie Kinderpornographie.

Besonderheiten bei der persönlichen Eignungsprüfung
Zusätzlich zur Prüfung der persönlichen Eignung durch die IHK erfolgt in einigen Bundesländern zusätzlich eine Sicherheitsüberprüfung durch die Staatsanwaltschaft oder Polizei. Davon können auch die Mitarbeitenden der/des Sachverständigen betroffen sein. Die Sicherheitsüberprüfungen werden in regelmäßigen Abständen wiederholt. Darüber hinaus kann die Beauftragung in bestimmten Deliktsbereichen von einer vorgeschalteten speziellen Beschulung durch die Staatsanwaltschaft oder Polizei abhängig gemacht werden.

Räumliche Voraussetzungen
Die Überlassung inkriminierten Materials zu Auswertungszwecken wird in einigen Bundesländern in bestimmten Deliktsbereichen von der Erfüllung sicherheitstechnischer Voraussetzungen bei den Büroräumen abhängig gemacht. Hierbei sind gesteigerte Anforderungen an die Einbruchsicherheit zu stellen, wie auch an Vorkehrungen zur Verhinderung des unbefugten Zutritts während der Bürozeiten (Zugangskontrollen, intern gesicherte Bereiche) sowie an die Sicherung von Asservaten vor unberechtigtem Zugriff. Die Sicherheitsüberprüfung erfolgt durch die Staatsanwaltschaft oder Polizei und kann in regelmäßigen Abständen wiederholt werden.