Richtlinien für die Anerkennung von Beratern für Cyber-Security

Herausgeber und Verlag: VdS Schadenverhütung GmbH

Amsterdamer Str. 172-174
D-50735 Köln
Telefon: (0221) 77 66 0; Fax: (0221) 77 66 341

VdS-Richtlinien für die Informationssicherheit

Richtlinien für die Anerkennung von Beratern für Cyber-Security

Die vorliegende Publikation ist unverbindlich. Die Versicherer können im Einzelfall auch andere Sicherheitsvorkehrungen oder Installations- oder Wartungsunternehmen zu nach eigenem Ermessen festgelegten Konditionen akzeptieren, die diesen technischen Spezifikationen oder Richtlinien nicht entsprechen.

Inhalt

1 Anwendungsbereich ... 4
1.1 Allgemeines ... 4
1.2 Gültigkeit ... 4
2 Definitionen ... 4
3 Normative Verweisungen ... 4
4 VdS-Anerkennung ... 5
4.1 Anforderungen an den Auftraggeber ... 5
4.1.1 Anerkennungsverfahren ... 5
4.1.2 Anerkennungsbedingungen ... 5
4.1.3 Auftragserteilung und einzureichende Unterlagen ... 8
4.1.4 Verpflichtungen ... 8
4.2 Voraussetzungen für die Erteilung der Anerkennung ... 9
4.2.1 Prüfung der Unterlagen ... 9
4.2.2 Erteilung der Erstanerkennung ... 9
4.3 Verlängerung der Anerkennung ... 9
4.3.1 Anforderungen ... 9
4.3.2 Verlängerung der Anerkennung ... 10
4.4 Erlöschen der Anerkennung ... 10
5 Änderungen der Anerkennung ... 10
6 Widerruf ... 11
7 Werbung ... 11
8 Gebühren ... 12
9 Sonstiges ... 12
9.1 Allgemeine Geschäftsbedingungen ... 12
9.2 Nebenabreden ... 12
10 Änderungen zur Vorversion ... 12
Anhang A Auftrag ... 13
Anhang B Prüfung ... 15

1 Anwendungsbereich

1.1 Allgemeines

Für den Erfolg eines Unternehmens ist es unabdingbar, wettbewerbsfähige Produkte oder Dienstleistungen anzubieten. Ebenso ist die Nutzung moderner Informationstechnologie (IT) zur Bewältigung von betriebswirtschaftlichen, logistischen und technischen Geschäftsprozessen sowie eine ständige Vernetzung über das Internet zwingend erforderlich, um im weltweiten Wettbewerb bestehen zu können. Digitalisierung und Vernetzung bergen neben vielfältigen Vorteilen jedoch auch neue Gefahren, die Unternehmen in ihrem Risikomanagement berücksichtigen müssen. Eine gut organisierte betriebsinterne Informationssicherheit verringert die Risiken, in dem Schwachstellen entschärft und dadurch die möglichen negativen Auswirkungen auf das Unternehmen begrenzt werden.

Die Richtlinien VdS 3473 beschreiben Anforderungen an die Informationssicherheit in Unternehmen und sind dabei auf die Schutzbedürfnisse von kleinen und mittelständischen Unternehmen (KMU) abgestimmt. Sie basieren auf den Erkenntnissen des BSI-Grundschutzkatalogs, den BSI-Standards und den Normen ISO 27001 und 27002.

Beratungsleistungen durch Dienstleister im Sinne dieser Richtlinien sollten darauf ausgerichtet sein, die IT-Sicherheit von KMU zu überprüfen und es dem beratenen Unternehmen zu ermöglichen, seine IT-Sicherheit derart zu ertüchtigen, dass eine formelle VdS-Bestätigung (VdS Quick-Audit nach VdS 3474 oder die Zertifizierung der Informationssicherheit nach VdS 3475) umsetzbar ist.

Die Zertifizierungsstelle von VdS Schadenverhütung GmbH (nachstehend VdS-Zertifizierungsstelle genannt) erkennt bei entsprechender Beauftragung Dienstleister für die Beratung von Sicherheit in der Informationstechnik (Cyber-Security) an. Die Anerkennung wird – wenn alle Voraussetzungen dieser Richtlinien erfüllt sind – von der VdS-Zertifizierungsstelle ausgesprochen und ist zeitlich befristet. Die Anerkennung wird durch ein Zertifikat dokumentiert. VdS-anerkannte Berater für Cyber Security werden in einem im Internet veröffentlichten Verzeichnis geführt.

1.2 Gültigkeit

Diese Richtlinien gelten ab dem 01.12.2016. Sie ersetzten die Richtlinien mit Stand 2015-11 (03).

2 Definitionen

Es gelten die in den Richtlinien VdS 3473 genannten Definitionen.

3 Normative Verweisungen

Diese Richtlinien enthalten datierte und undatierte Verweise auf andere Regelwerke. Die Verweise erfolgen in den entsprechenden Abschnitten, die Titel werden im Folgenden aufgeführt. Änderungen oder Ergänzungen datierter Regelwerke gelten nur, wenn sie durch Änderung dieser Richtlinien bekannt gegeben werden. Von undatierten Regelwerken gilt die jeweils letzte Fassung.

DIN EN ISO/IEC 17024 Konformitätsbewertung – Allgemeine Anforderungen an Stellen, die Personen zertifizieren

VdS 3177 AGB der VdS Schadenverhütung GmbH für die Erbringung von Prüf- und Zertifizierungsdienstleistungen

VdS 3473	Informationssicherheit in kleinen und mittelständischen Unternehmen (KMU), Anforderungen
VdS 3474	VdS Quick-Audit für Cyber-Security, Verfahren
VdS 3475	Zertifizierung der Informationssicherheit in kleinen und mittelständischen Unternehmen (KMU), Verfahren
ISO/IEC 27001	Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen

4 VdS-Anerkennung

4.1 Anforderungen an den Auftraggeber

4.1.1 Anerkennungsverfahren

Aufträge zur Anerkennung werden in der Reihenfolge ihres Eingangs bearbeitet.

Erfüllt der Auftraggeber die Anerkennungsbedingungen, erhält er eine auf 4 Jahre befristete Anerkennung. Diese Anerkennung kann – bei weiterer Einhaltung der zugrunde liegenden Richtlinien – bei entsprechender Beauftragung jeweils für weitere 4 Jahre verlängert werden.

Der Auftraggeber muss alle Anerkennungsbedingungen erfüllen. Die VdS-Zertifizierungsstelle behält sich vor, die Einhaltung der Bedingungen durch geeignete Maßnahmen zu überprüfen.

Der Auftraggeber erkennt

a) die vorliegenden Richtlinien VdS 3477 als Vertragsbestandteil sowie als Basis für die VdS-Anerkennung als Berater für Cyber-Security

b.1) die Richtlinien VdS 3473 als Basis für die Beratung

b.2) die Richtlinien VdS 3474 als Basis für das Beratungsziel VdS Quick-Audit

b.3) die Richtlinien VdS 3475 als Basis für das Beratungsziel VdS-Zertifizierung der Informationssicherheit

an.

4.1.2 Anerkennungsbedingungen

Die Anerkennung als Berater für Cyber-Security setzt voraus, dass alle im Folgenden aufgeführten Anerkennungsbedingungen erfüllt und im Rahmen des Anerkennungsverfahrens durch Vorlage der entsprechenden Nachweise gegenüber der VdS-Zertifizierungsstelle bestätigt wurden.

Der Auftraggeber

a) verfügt über ein abgeschlossenes Studium der Informatik (Hoch- oder Fachhochschule).

   Nachweis: Kopie der Abschlussurkunde.

   und

a.1) besitzt mindestens 3-jährige, innerhalb der letzten 5 Jahre vor Auftragserteilung erworbene, praktische und fundierte Berufserfahrung in der Informationstechnologie (Beratungs-, Planungs-, Administrations- oder Errichtungsleistungen mit Schwerpunkt in der IT-Security).
   Die berufliche Tätigkeit deckt in dieser Zeit mindestens 50 % einer Vollzeitstelle ab.

   Nachweis: Tabellarischer Lebenslauf einschließlich detaillierter Tätigkeitsbeschreibung (Beschreibungen hinsichtlich Inhalt und Dauer der Tätigkeiten).

Alternativ – ohne abgeschlossenes Studium der Informatik (Hoch- oder Fachhochschule):

a.2) besitzt mindestens 5-jährige, innerhalb der letzten 7 Jahre vor Auftragserteilung erworbene praktische und fundierte Berufserfahrung in der Informationstechnologie (Beratungs-, Planungs-, Administrations- oder Errichtungsleistungen mit Schwerpunkt in der Cyber-Security).
   Die berufliche Tätigkeit deckt in dieser Zeit mindestens 50 % einer Vollzeitstelle ab.

   Nachweis: Tabellarischer Lebenslauf einschließlich detaillierter Tätigkeitsbeschreibung (Beschreibungen hinsichtlich Inhalt und Dauer der Tätigkeiten).

b) ist aktuell (mindestens 6 Monate innerhalb des letzten Jahres vor Auftragserteilung) als Berater für Cyber-Security tätig.
   Die berufliche Tätigkeit deckt in dieser Zeit mindestens 50 % einer Vollzeitstelle ab.

   Nachweis: Tabellarischer Lebenslauf einschließlich detaillierter Tätigkeitsbeschreibung (Beschreibungen hinsichtlich Inhalt und Dauer der Tätigkeiten).

c) besitzt ein einfaches polizeiliches Führungszeugnis ohne Einträge, das maximal 6 Monate vor Auftragserteilung ausgestellt wurde.

   Nachweis: Kopie des Führungszeugnisses.

d) versichert, sofern keine Selbstständigkeit besteht, dass er die Tätigkeit als Berater für Cyber-Security uneingeschränkt ausüben kann.

   Nachweis: Bestätigung des Arbeitgebers, dass keine inhaltlichen oder arbeitsrechtlichen Beschränkungen bestehen, Tätigkeiten als VdS-anerkannter Cyber-Berater wahrzunehmen.

   Hinweis: In jedem Fall muss eine freie und objektive Beratungsleistung nach bestem Wissen und Gewissen erfolgen können, unabhängig von einer möglichen wirtschaftlichen Abhängigkeit vom Arbeitgeber.

e) weist Kenntnisse über gängige Angriffsmethoden, Schwachstellenanalyse, Risikoanalyse, Bewertung von Sicherheitsvorfällen, IT-Sicherheitsprodukten und IT-Sicherheitssystemen nach.

   Nachweis: Zertifikate über anerkannte Ausbildungen, die entweder nicht länger als 3 Jahre vor Auftragserteilung erlangt wurden oder zu denen regelmäßige Weiterbildungsmaßnahmen nachgewiesen wurden.

Als anerkannte Bildungsmaßnahmen gelten z. B.:

- Certified Information Security Manager (CISM)
- Certified Information System Auditor (CISA)
- ITIL-Expert
- Certified Information System Security Professional (CISSP)
- Teletrust Information Security Professional (TISP)
- Ausbildung zum ISMS Auditor/Lead Auditor nach ISO/IEC 27001
- ISO 27001-Auditor auf Basis von IT-Grundschutz
- Alle IT-Professionals/Operative Professionals sowie sonstige Bildungsabschlüsse mit Schwerpunkt der IT-Sicherheit, die durch öffentlich-rechtliche Kammern mit Prüfung erworben wurden

Nachweis: Zertifikat.

Alternativ können gleichwertige Bildungsmaßnahmen anerkannt werden, die eine Mindestausbildungsdauer von 5 Tagen (40 Stunden) nicht unterschritten, Fachbereiche der folgenden Liste geschult und das Ausbildungsziel durch Abschlussprüfung bestätigt haben:

- IT-Governance und IT-Management
  - Sicherheits- und Datenschutzmanagement
  - Risiko- und Schwachstellenmanagement
  - Business Continuity Management und Emergency Response
  - Rechtliches – relevante Gesetze, Richtlinien und Standards zur IT-Security
- Hardware/Software
  - Penetration von IT-Systemen
  - Applikations- und Software-Entwicklung
  - Betriebssystemsicherheit – Windows/Unix
  - Hackerangriffe
  - Storage- und Backupmanagement
  - Kryptografie
- Netzwerk und Infrastruktur
  - Netzwerksicherheit und -konfiguration
  - PKI
  - Konfiguration und Absichern von Firewalls
  - Routing/Switching

Nachweis: Zertifikat mit Darlegung der Lehrinhalte und zeitlichem Umfang.

Darüber hinaus weist der Auftraggeber den Besitz von Kenntnissen und Erfahrungen zu den im Folgenden unter f) bis k) genannten Themengebieten gegenüber der VdS-Zertifizierungsstelle nach. Es müssen Grundkenntnisse in allen diesen Themengebieten und weitergehende Kenntnisse in mindestens drei dieser Themengebiete nachgewiesen werden.

Der Auftraggeber verfügt über

f) Erfahrung zum Schutz der IT gegen computerbasierte Angriffe, sowie über umfangreiche Kenntnisse zu IT-Sicherheitsprodukten und IT-Systemen, z. B. als Administrator

g) Erfahrung zu IT-bezogenen Business Continuity Management-Prozessen

h) Kenntnisse gängiger Angriffsmethoden und Fähigkeit, vorhandene IT-Systeme und IT-Strukturen auf mögliche Schwachstellen hin zu analysieren

i) Kenntnisse über Bewertung der sich aus der IT-Landschaft ergebenden Risiken für ein Unternehmen (KMU)

j) Kenntnisse zur Bewertung von Sicherheitsvorfällen

k) Kenntnisse über Nutzen, Wirksamkeit und Schwachstellen gängigerweise eingesetzter IT-Produkte und –Systeme und Fähigkeit zur Beurteilung solcher Systeme aus dem Blickwinkel der IT-Security

   Nachweis der Anforderungen gemäß f) bis k): Detaillierte Tätigkeitsbeschreibung durch den Auftraggeber, in Form von Arbeitszeugnissen, Bestätigung der erfolgreichen Teilnahme an einschlägigen Lehrgängen wie bspw. VdS-Lehrgang zum Informationssicherheitsbeauftragten, zur ISO/IEC 27000er-Reihe, zum BSI-Grundschutzkatalog oder gleichwertig.

Darüber hinaus weist der Auftraggeber gegenüber der VdS-Zertifizierungsstelle nach, dass er über die nachfolgend genannten Anforderungen verfügt:

l) Kenntnisse über spezifische gesetzliche Regelungen

   Nachweis: Zertifikat über erfolgreiche Schulung als Datenschutzbeauftragter oder über den VdS-Lehrgang zum Informationssicherheitsbeauftragten.

m) Kenntnisse einschlägiger VdS-Richtlinien und Sicherungsrichtlinien zur Schadenverhütung in KMU, soweit diese im Zusammenhang mit IT-Security relevant sind

n) Kenntnisse über das Richtlinienwerk zur Cyber-Security, insbesondere zu VdS 3473.

   Nachweis: Bestätigung der erfolgreichen Teilnahme am VdS-Lehrgang zu den Richtlinien VdS 3473 oder gleichwertig.

o) bestandene Prüfung gemäß Anhang B

Weiterhin bestätigt der Auftraggeber verbindlich, dass er über alle erforderlichen Normen und Richtlinien (z. B. ISO/IEC 27000-Reihe sowie die VdS-Richtlinienreihe zur Cyber-Security) stets in der aktuellen Fassung verfügt bzw. sich kurzfristig Zugriff beschaffen kann.

4.1.3 Auftragserteilung und einzureichende Unterlagen

Die VdS-Anerkennung als Berater für Cyber-Security ist schriftlich mittels Anhang A (erhältlich als separate, ausfüllbare PDF-Datei) bei der VdS-Zertifizierungsstelle zu beauftragen. Der Vordruck muss vollständig ausgefüllt und vom Auftraggeber unterschrieben eingereicht werden. Die Nachweise für Kenntnisse und Fähigkeiten sind als Anlage beizufügen.

4.1.4 Verpflichtungen

Der Auftraggeber verpflichtet sich

- nur dann tätig zu werden, wenn seine Unparteilichkeit gewährleistet ist.
  Das bedeutet u. a., dass für denselben Kunden bzw. dasselbe Objekt keine Beratungsleistung zur Cyber-Sicherheit bei gleichzeitiger oder nachgelagerter Auditierung der Cyber-Sicherheit erfolgen darf.

- an einschlägigen Fortbildungsveranstaltungen, z. B. von VdS Schadenverhütung oder VdS-akzeptierten Bildungsmaßnahmen teilzunehmen.
- seine finanziellen Verpflichtungen gegenüber VdS Schadenverhütung zu erfüllen.

4.2 Voraussetzungen für die Erteilung der Anerkennung

4.2.1 Prüfung der Unterlagen

Die Prüfung des Auftrags und der eingereichten Unterlagen und Nachweise des Auftraggebers nach Abschnitt 4.1 darf zu keinen Beanstandungen führen.

Sofern die VdS-Zertifizierungsstelle zu der Auffassung gelangt, dass eine nicht eindeutige fachliche Eignung der Person, für die eine VdS-Anerkennung beauftragt wird, vorliegt, kann die fachliche Eignung im Rahmen eines gebührenpflichtigen Witnessaudits festgestellt werden. Die Gebühren hierzu hat der Auftraggeber zu tragen und sind der Gebührentabelle der VdS-Zertifizierungsstelle zu entnehmen. Die VdS-Zertifizierungsstelle behält sich für diesen Fall eine vorläufige Berufung zum VdS-anerkannten Berater nach diesen Richtlinien vor.

4.2.2 Erteilung der Erstanerkennung

Die Anerkennung wird für einen Zeitraum von 4 Jahren ausgesprochen.

Liegen der VdS-Zertifizierungsstelle nicht innerhalb von 6 Monaten nach Auftragserteilung sämtliche geforderten Unterlagen vor, wird das Anerkennungsverfahren kostenpflichtig abgebrochen. Die bis dahin erhaltenen Unterlagen werden an den Auftraggeber zurückgesandt bzw. – bei Unterlagen in elektronischer Form – gelöscht. Alle Aufwendungen, die der VdS-Zertifizierungsstelle bis zu diesem Zeitpunkt entstanden sind, gehen zu Lasten des Auftraggebers. Danach kann das Verfahren nur durch einen vollständigen Neuauftrag gestartet werden.

4.3 Verlängerung der Anerkennung

4.3.1 Anforderungen

Eine Verlängerung der Anerkennung kann jeweils für weitere 4 Jahre beauftragt werden. Maßgebend für die Erteilung der Verlängerung sind die zum Zeitpunkt der Auftragserteilung geltenden VdS-Richtlinien. Die Verlängerung muss mindestens 4 Monate vor Ablauf der Anerkennung unter Verwendung des anhängenden Vordrucks (Anhang A) bei der VdS-Zertifizierungsstelle beauftragt werden.

Dem Auftrag sind beizufügen:

- die Teilnahmebestätigungen über mindestens zwei relevante Fortbildungen innerhalb des Anerkennungszeitraums
- ggf. Nachweise über Änderungen, welche die Grundlagen der VdS-Anerkennung betreffen
- Nachweis über mindestens acht durchgeführte Beratungsmaßnahmen auf Grundlage der VdS 3473 innerhalb des Anerkennungszeitraums.

Als Fortbildung anerkannt werden Schulungsmaßnahmen, die in ihrer Gesamtheit mindestens 5 Tage (40 Stunden) umfassen. Folgende Themenbereiche können für eine Weiterbildung relevant sein:

- IT-Governance und IT-Management
  - Sicherheits- und Datenschutzmanagement
  - Risiko- und Schwachstellenmanagement
  - Business Continuity Management und Emergency Response
  - Rechtliches – relevante Gesetze, Richtlinien und Standards zur IT-Security
- Hardware/Software
  - Penetration von IT-Systemen
  - Applikations- und Software-Entwicklung
  - Betriebssystemsicherheit – Windows/Unix
  - Hackerangriffe
  - Storage- und Backupmanagement
  - Kryptografie
- Netzwerk und Infrastruktur
  - Netzwerksicherheit und -konfiguration
  - PKI
  - Konfiguration und Absichern von Firewalls
  - Routing/Switching.

Um den Vorgaben an das Begutachtungsverfahren gemäß DIN EN ISO/IEC 17024 zu entsprechen, bleibt es der VdS Zertifizierungsstelle vorbehalten, zusätzliche Begutachtungen mittels spezifischer Methoden und Mechanismen, z. B. der Vergewisserung bezüglich des Ablaufs einer Beratung, umzusetzen. Sofern es VdS für erforderlich erachtet, an einer Beratung des VdS-anerkannten Beraters für Cyber-Security teilzunehmen, so wird dieser im Vorfeld entsprechend informiert und ist verpflichtet, beim Empfänger der Beratung dessen Einwilligung, dass VdS an der Beratung teilnehmen darf, zu erfragen.

4.3.2 Verlängerung der Anerkennung

Die Anerkennung wird um weitere 4 Jahre verlängert, wenn der Auftrag vollständig ausgefüllt und unterschrieben und mit allen erforderlichen Unterlagen versehen zeitgerecht bei der VdS-Zertifizierungsstelle eingereicht wurde und die Überprüfung des Auftrags sowie aller Unterlagen zu einem positiven Ergebnis führt.

4.4 Erlöschen der Anerkennung

Die Anerkennung erlischt nach Ablauf des Anerkennungszeitraums. Erfolgt der Auftrag zur Verlängerung später als 12 Monate nach Ablauf der Anerkennung, ist ein komplett neuer Auftrag mit sämtlichen Unterlagen nach 4.1 einzureichen.

5 Änderungen der Anerkennung

Änderungen, welche die Grundlagen der VdS-Anerkennung betreffen, sind der VdS-Zertifizierungsstelle unverzüglich unter Verwendung des Anhangs A („Änderungsauftrag“ ankreuzen) mitzuteilen.

Mitteilungspflichtige Änderungen sind u. a.:

- Wechsel der Anstellung bzw. in die Selbstständigkeit
- Änderung der Firmierung
- Verlagerung der Betriebsstätte (Umzug).

6 Widerruf

Anerkennungen können widerrufen und damit ungültig werden. Ab dem Zeitpunkt des Widerrufs darf mit der VdS-Anerkennung nicht mehr geworben werden (siehe Abschnitt 7).

Widerruf erfolgt, wenn

- die Voraussetzungen für die Anerkennung nicht mehr gegeben sind
- die dem Anerkennungsverfahren zugrunde liegenden Richtlinien sich ändern und der Auftraggeber diese Änderungen nicht innerhalb einer angemessenen Frist umsetzt
- die Anerkennung oder das VdS-Logo unkorrekt verwendet werden (z. B. unlautere Werbung)
- der Berater seinen Verpflichtungen nach diesen Richtlinien nicht nachgekommen ist
- der Berater bei berechtigter Beanstandung nicht unverzüglich für Abhilfe sorgt
- der Berater seinen finanziellen Verpflichtungen gegenüber der VdS Schadenverhütung GmbH nicht nachkommt
- sich der Berater in dieser oder einer anderen Geschäftsbeziehung zwischen Parteien als unzuverlässig erweist (z. B. durch Täuschung, Kompromittierung).

Der Widerruf der Anerkennung wird dem Berater per Einschreiben mitgeteilt. Gegen den Widerruf kann innerhalb von 2 Monaten Einspruch eingelegt werden. Der Widerruf der Anerkennung kann innerhalb von 6 Monaten zurückgenommen werden, wenn die Gründe, die zum Widerruf führten, weggefallen sind.

Ein Rechtsanspruch auf Rücknahme der Aberkennung besteht nicht. Die Anerkennung kann frühestens 12 Monate nach einem Widerruf erneut beauftragt werden. Bei der Auftragserteilung ist der Nachweis zu führen, dass der Auftraggeber alle Verpflichtungen erfüllt und evtl. Mängel aus dem vorangegangenen Verfahren beseitigt hat.

7 Werbung

Anerkannte Berater für Cyber-Security dürfen mit der VdS-Anerkennung werben. Es ist jedoch untersagt, die Marke VdS oder Abwandlungen hiervon bzw. die Zertifizierung als solche in die Firmenbezeichnung aufzunehmen. Bei einer Werbung mit der VdS-Anerkennung als Berater für Cyber-Security muss der Inhalt des Textes auf der Anerkennungsurkunde korrekt und darf nicht auf wettbewerbswidrige Art und Weise wiedergeben werden.

Die diesbezüglichen Bestimmungen auf dem Zertifikat sind einzuhalten. Die Werbung darf nur im Zusammenhang mit der anerkannten Person erfolgen. Die Werbung mit der VdS-Anerkennung darf nicht in Verbindung mit Leistungen des Auftraggebers erfolgen, die nicht durch den Anerkennungsumfang abgedeckt sind. Im Zweifelsfall ist die Werbung mit der VdS-Anerkennung mit der VdS-Zertifizierungsstelle abzustimmen.

Der VdS-anerkannte Berater für Cyber-Security darf auf seine VdS-Anerkennung mit folgendem Logo hinweisen:

Das VdS-Logo darf unter Beibehaltung der Proportionen vergrößert oder verkleinert werden. Eine Mindesthöhe von 13 mm für das Logo darf nicht unterschritten werden. Bei Farbdruck ist HKS 42 (oder gleichwertige Farbe) zu verwenden. Das Logo darf auf Briefköpfen, Werbeschriften, Veröffentlichungen und Werbebroschüren des Auftraggebers verwendet werden. Eine eigenständige Abwandlung des Logos ist untersagt. Um eine korrekte Darstellung des Logos zu gewährleisten, kann das Logo bei der VdS-Zertifizierungsstelle gebührenfrei angefordert werden.

8 Gebühren

Das Anerkennungsverfahren und die nach der Anerkennung durchgeführten Prüfungen sind gebührenpflichtig und werden dem Auftraggeber bzw. dem VdS-anerkannten Berater für Cyber-Security in Rechnung gestellt. Die Höhe der Gebühren (u. a. der Jahresgebühr) kann der Gebührentabelle der VdS-Zertifizierungsstelle entnommen werden. Diese wird Interessenten bei einer Anfrage zusammen mit diesen Richtlinien in einem Informationspaket kostenlos zugestellt. Für die Berechnung der Leistungen gelten die Gebühren nach Maßgabe der Gebührentabelle der VdS-Zertifizierungsstelle zum Zeitpunkt der Leistungserbringung.

9 Sonstiges

9.1 Allgemeine Geschäftsbedingungen

Es gelten die AGB VdS 3177 in der zum Zeitpunkt des Vertragsabschlusses gültigen Fassung.

9.2 Nebenabreden

Nebenabreden bedürfen zu ihrer Wirksamkeit der Schriftform.

10 Änderungen zur Vorversion

- redaktionelle Änderungen
- Änderungen bei den Anerkennungsvoraussetzungen
- Ergänzung des Anhangs B (Prüfung)

Anhang A Auftrag

Auftrag zur VdS-Anerkennung als Berater für Cyber-Security
auf Grundlage der VdS 3477
durch VdS Schadenverhütung GmbH
Amsterdamer Straße 174, 50735 Köln

☐ Erstauftrag ☐ Änderungsauftrag (nur Berater-Nr. und geänderte Daten ausfüllen)

☐ Verlängerungsauftrag (Abschnitt 4 nur bei Änderungen ausfüllen) Berater-Nr.:

1	**Auftraggeber**	
1.1	Unternehmensbezeichnung	
1.2	Anschrift (Straße, Hausnr., PLZ, Ort)	
1.3	E-Mailadresse	
1.4	Telefon/Telefax	
1.5	Mobiltelefon	
1.6	Internetseite	
1.7	Handelsregistereintrag	
1.8	Kontaktperson	☐ selbstständig
1.9	Telefonnummer Kontaktperson	
1.10	Internetseite	
2	**Person, für die eine VdS-Anerkennung beauftragt wird**	
2.1	Benennung der Person	
2.2	Email-Adresse	
2.3	Internetseite:	
2.4	☐ angestellt (Angaben zum Auftraggeber siehe Abschnitt 1)	
2.5	☐ selbstständig (Angaben zum Unternehmen siehe Abschnitt 1)	
3	**Anerkennungsurkunde**	
	☐ Neben der deutschsprachigen Ausfertigung der VdS-Anerkennungsurkunde wird eine englischsprachige Fassung gewünscht	

				Nachweis	Dateiname
4	**Nachweis über Kenntnisse und Fähigkeiten des Beraters**				
	(Nachweise sind als Anlage beizufügen und im Folgenden zu benennen)				
4.1	Abgeschlossene akademische Ausbildung	☐ Ja ☐ Nein		☐ Zeugnis	
4.2	Abgeschlossene Berufsausbildung	☐ Ja ☐ Nein		☐ Zeugnis	
	Berufserfahrung				
4.3	Anzahl Monate	Tätigkeit		☐ Lebenslauf	
4.4	Anzahl Monate	Tätigkeit		☐ Lebenslauf	
4.5	Anzahl Monate	Tätigkeit		☐ Lebenslauf	
4.6	Kenntnisse über gängige Angriffsmethoden, Schwachstellenanalyse, Risikoanalyse, Bewertung von Sicherheitsvorfällen, IT-Sicherheitsprodukten und IT-Sicherheitssystemen	☐ Grundkenntnisse ☐ Erweiterte Kenntn.		☐ Zertifikat ☐ Gleichwertige Bildungsmaßn.	
4.7	Erfahrung zum Schutz der IT gegen computerbasierte Angriffe, sowie über umfangreiche Kenntnisse zu IT-Sicherheitsprodukten und IT-Systemen, z.B. als Administrator	☐ Grundkenntnisse ☐ Erweiterte Kenntn.		☐ Zertifikat ☐ Detaillierte Projektliste	
4.8	Erfahrung zu IT-bezogenen Business Continuity Management-Prozessen	☐ Grundkenntnisse ☐ Erweiterte Kenntn.		☐ Zertifikat ☐ Detaillierte Projektliste	
4.9	Kenntnisse gängiger Angriffsmethoden und Fähigkeit, vorhandene IT-Systeme und IT-Strukturen auf mögliche Schwachstellen hin zu analysieren	☐ Grundkenntnisse ☐ Erweiterte Kenntn.		☐ Zertifikat ☐ Detaillierte Projektliste	
4.10	Kenntnisse über Bewertung der sich aus der IT-Landschaft ergebenden Risiken für ein Unternehmen (KMU)	☐ Grundkenntnisse ☐ Erweiterte Kenntn.		☐ Zertifikat ☐ Detaillierte Projektliste	

4.11	Kenntnisse zur Bewertung von Sicherheitsvorfällen	☐ Grundkenntnisse ☐ Erweiterte Kenntn.	☐ Zertifikat ☐ Detaillierte Projektliste	
4.12	Kenntnisse über Nutzen, Wirksamkeit und Schwachstellen gängigerweise eingesetzter IT-Produkte und –Systeme und Fähigkeit zur Beurteilung solcher Systeme aus dem Blickwinkel der IT-Security	☐ Grundkenntnisse ☐ Erweiterte Kenntn.	☐ Zertifikat ☐ Detaillierte Projektliste	
4.13	Kenntnisse über spezifische gesetzliche Regelungen		☐ Zertifikat ☐ Detaillierte Projektliste	
4.14	Kenntnisse einschlägiger VdS-Richtlinien und Sicherungsrichtlinien zur Schadenverhütung in KMU, soweit		☐ Teilnahme-bescheinigung	
4.15	Kenntnisse über das Richtlinienwerk zur Cyber-Security, insbesondere zu VdS 3473		☐ Teilnahme-bescheinigung	
4.16	bestandene Prüfung gemäß Anhang B		☐ Zertifikat	
	Sonstige Nachweise			
4.17	Polizeiliches Führungszeugnis ohne Einträge		☐ Zeugnis	

5 Vertragsbestandteile und Datenschutz

Die „Richtlinien für die Anerkennung von Beratern für Cyber-Security", VdS 3477 und die zugehörige Gebührentabelle der VdS-Zertifizierungsstelle in der jeweils gültigen Fassung sowie die Allgemeinen Geschäftsbedingungen, VdS 3177, habe(n) ich (wir) zur Kenntnis genommen und erkenne(n) sie als Vertragsbestandteil an.

5.1 ☐ Ich/wir willigen ein, dass VdS Schadenverhütung GmbH im Rahmen des Anerkennungsverfahrens Daten erhebt, verarbeitet, nutzt, in einem Verzeichnis führt und die Anerkennung als Berater für Cyber-Security Dritten mitteilt.

5.2 ☐ Ich/wir willigen ein, dass VdS Schadenverhütung GmbH mir/uns (auch) auf elektronischem Weg (z. B. E-Mail) Informationen zu VdS-Zertifizierungs- und Anerkennungsverfahren zukommen lässt. Mir/uns ist bekannt, dass ich/wir diese Zusage jederzeit und ohne Angabe von Gründen widerrufen kann/können.

5.3 ☐ Ich wünsche die Zusendung themenbezogener Informationen (i.d.R. per Email). Mir ist bekannt, dass ich diese Zusage jederzeit und ohne Angabe von Gründen widerrufen kann.

Datum — Stempel und Unterschrift des Auftraggebers bzw. eines Bevollmächtigten

6 Erklärung zur Verfügbarkeit der Normen und Richtlinien

Ich/wir bestätigen mit der nachfolgenden Unterschrift die Verfügbarkeit der erforderlichen Normen und Richtlinien.

Datum — Stempel und Unterschrift des Auftraggebers bzw. eines Bevollmächtigten

7 Erklärung des Arbeitgebers (nur bei unselbstständig Beschäftigten erforderlich)

Ich/wir bestätigen mit der nachfolgenden Unterschrift, dass der Auftraggeber die Tätigkeit als Cyber-Security-Berater uneingeschränkt ausüben kann.

Stand: 2017-08 (05) Datum — Stempel und Unterschrift des Arbeitgebers bzw. eines Bevollmächtigten

Anhang B Prüfung

1 Aufbau und Durchführung der Prüfung

1.1 Allgemeines

Die Prüfung wird bei VdS Schadenverhütung in Köln oder in Ausnahmefällen an einem von der VdS-Zertifizierungsstelle benannten Ort durchgeführt. Sie findet zu vorgegebenen Terminen statt und ist nicht öffentlich.

Vor Beginn der Prüfung werden die Teilnehmer über den Prüfungsablauf, die zur Verfügung stehende Zeit, die erlaubten Arbeits- und Hilfsmittel informiert und über die Folgen von Täuschungshandlungen belehrt.

Die Prüfung erfolgt schriftlich. Sie findet in deutscher Sprache statt. Prüfungsinhalte sind Themenstellungen, die sich aus den Anforderungen nach Abschnitt 4.1.2, Buchst. e) bis n) dieser Richtlinien ergeben.

1.2 Aufbau der Prüfung

Die Zertifizierungsstelle erstellt in Vorbereitung der Prüfung einen Fragebogen. Dieser besteht aus 40 Fragen, die aus dem Fragenkatalog ausgewählt werden. Dabei sollen alle Themenstellungen zu gleichen Teilen Berücksichtigung finden.

Die Fragen werden nach dem Multiple-Choice-Verfahren gestellt. Zu den vorgegebenen Fragen sind die richtigen Antworten anzukreuzen. Es können eine, mehrere oder alle Antwortalternativen richtig sein.

Der zugrundeliegende Fragenkatalog ist nicht öffentlich. Sowohl der Fragenkatalog, als auch der Fragebogen dürfen nicht vervielfältigt oder Dritten zugänglich gemacht werden.

1.3 Durchführung

Jeder Teilnehmer muss vor Prüfungsbeginn seine Identität nachweisen (Personalausweis, Pass oder Führerschein).

Jeder Teilnehmer erhält einen Fragebogen. Weiterhin erhält jeder Teilnehmer einen Antwortbogen, auf dem der Teilnehmer vor Beginn der Prüfung seine persönlichen Daten angeben muss.

Die Bearbeitungszeit beträgt 60 Minuten.

Zugelassenes Hilfsmittel:

– VdS-Richtlinien zu Cyber-Security, VdS 3473 in der aktuellen Fassung

Die Prüfungsunterlagen sind vom Teilnehmer dokumentenecht, z. B. mit Kugelschreiber oder Filzstift, zu bearbeiten. Antworten sind ausschließlich auf dem gestellten Antwortbogen zu vermerken. Die Unterlagen werden nach Ablauf der Bearbeitungszeit eingesammelt und verbleiben bei der VdS-Zertifizierungsstelle.

Bei jeder Frage werden die aus den Antwortalternativen für richtig erachtete Antworten auf den dazu vorgesehenen Feldern angekreuzt. Es können eine, mehrere oder alle Antwortalternativen richtig sein.

Das Ankreuzen von Feldern ist so vorzunehmen, dass jedes Kreuz eindeutig einem einzigen Feld zugeordnet werden kann. Andernfalls, d. h. insb. wenn die vorgegebene Feldumrandung beim Ankreuzen nicht eingehalten wird, gilt das jeweilige Kreuz als nicht vorhanden und wird für keines der in Betracht kommenden Felder als Antwort gewertet.

Bei Täuschungshandlungen oder Störungen des Prüfungsablaufes kann der betreffende Teilnehmer von der Prüfung ausgeschlossen werden. Die Prüfung gilt in diesem Fall als nicht bestanden; eine Wiederholungsprüfung ist nicht mehr möglich.

2 Bewertung

Jede Frage wird mit einer Punktzahl zwischen 0 und 2 bewertet. 2 Punkte werden vergeben, wenn alle richtigen Antwortmöglichkeiten markiert sind. 1 Punkt wird vergeben, wenn nur eine von mehreren richtigen Antwortmöglichkeiten markiert ist. 0 Punkte werden vergeben, wenn eine falsche Antwortmöglichkeit markiert ist, und zwar unabhängig davon, ob auch eine richtige Antwortmöglichkeit oder mehrere Antwortmöglichkeiten markiert sind, oder wenn keine Antwortmöglichkeit markiert ist.

Die Prüfung gilt als bestanden, wenn mindestens 64 Punkte (80 %) erreicht wurden.

3 Auswertung des Prüfungsergebnisses

Die Bewertung erfolgt unabhängig voneinander durch zwei Prüfer. Bei nicht übereinstimmender Beurteilung ergibt sich die Bewertung aus dem arithmetischen Mittel der Einzelbewertungen.

Die Auswertung der Prüfungsarbeit soll innerhalb von vier Wochen abgeschlossen sein.

4 Mitteilung des Prüfungsergebnisses

Der Teilnehmer wird über das Ergebnis der Prüfung schriftlich informiert.

Die Prüfungsunterlagen können nach vorheriger Terminabsprache vom Prüfungsteilnehmer bei der VdS-Zertifizierungsstelle eingesehen werden. Die Unterlagen werden mindestens zehn Jahre aufbewahrt.

5 Wiederholung

Besteht ein Teilnehmer die Prüfung nicht, kann er sie zweimal wiederholen.

6 Hinweise zum Bundesdatenschutzgesetz

Zur Erfüllung des Bundesdatenschutzgesetzes (§ 4 Abs. 1) benötigt die VdS-Zertifizierungsstelle eine offizielle, persönliche und schriftlich abgegebene Einwilligungserklärung aller Personen, deren Daten aufgrund eines VdS-Anerkennungs-/Zertifizierungsverfahrens erhoben, verarbeitet und genutzt werden. Die Einwilligungserklärung muss der VdS-Zertifizierungsstelle vor Durchführung der Prüfung unterschrieben vorliegen. Anderenfalls kann die Person nicht zur Prüfung zugelassen werden.