Zertifizierung der Informationssicherheit in kleinen und mittleren Unternehmen (KMU)

Verfahren

VdS 3475 : 2015-11 (02)

Herausgeber und Verlag: VdS Schadenverhütung GmbH

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

Copyright by VdS Schadenverhütung GmbH. Alle Rechte vorbehalten.

VdS-Richtlinien für die Informationssicherheit

Zertifizierung der Informationssicherheit in kleinen und mittleren Unternehmen (KMU)

Verfahren

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 Allgemeines ... 4
1.1 Grundlagen ... 4
1.2 Gültigkeit ... 5
2 Definitionen ... 5
3 Normative Verweisungen ... 5
4 Zertifizierungsverfahren ... 5
4.1 Auftrag ... 5
4.2 Auditierung ... 6
4.2.1 Auditplanung ... 6
4.2.2 Audit ... 6
4.2.3 Abweichungen und Verbesserungsmaßnahmen ... 6
4.2.4 Kurzfristig angekündigte Audits ... 7
4.3 Ausstellung des Zertifikates ... 7
4.4 Check-up, Re-Zertifizierung, Änderung, Ergänzung ... 7
4.4.1 Check-up ... 7
4.4.2 Re-Zertifizierung ... 8
4.4.3 Änderung/Ergänzung von Zertifikaten ... 8
4.4.4 Wiederaufnahme von widerrufenen oder eingeschränkten Zertifizierungen ... 8
5 Widerruf/Einschränkung ... 9
6 Werbung ... 10
7 Gebühren ... 10
8 Sonstiges ... 11
8.1 Verpflichtungen des Auftraggebers ... 11
8.2 Allgemeine Geschäftsbedingungen ... 11
8.3 Nebenabreden ... 11
Anhang A Auftrag ... 12
A.1 Hinweise zu Auftragsformular ... 13
Anhang B Dokumentation des Auftraggebers ... 13

1 Allgemeines

1.1 Grundlagen

Grundlagen dieser VdS-Richtlinien sind die Anforderungen der Richtlinien VdS 3473.

Die Zertifizierungsstelle von VdS Schadenverhütung (nachstehend VdS-Zertifizierungsstelle genannt) führt nach Beauftragung ein unabhängiges und unparteiliches Zertifizierungsverfahren von Informationssicherheitsstatus von Unternehmen gemäß VdS 3473 durch.

Zertifizierungsaufträge werden in der Reihenfolge Ihres Eingangs bearbeitet. Eine Bevorteilung einzelner Auftraggeber erfolgt nicht. Im Rahmen des Zertifizierungsverfahrens werden keine Beratungen durchgeführt.

Das Zertifizierungsverfahren besteht im Wesentlichen aus den im Folgenden beschriebenen Schritten.

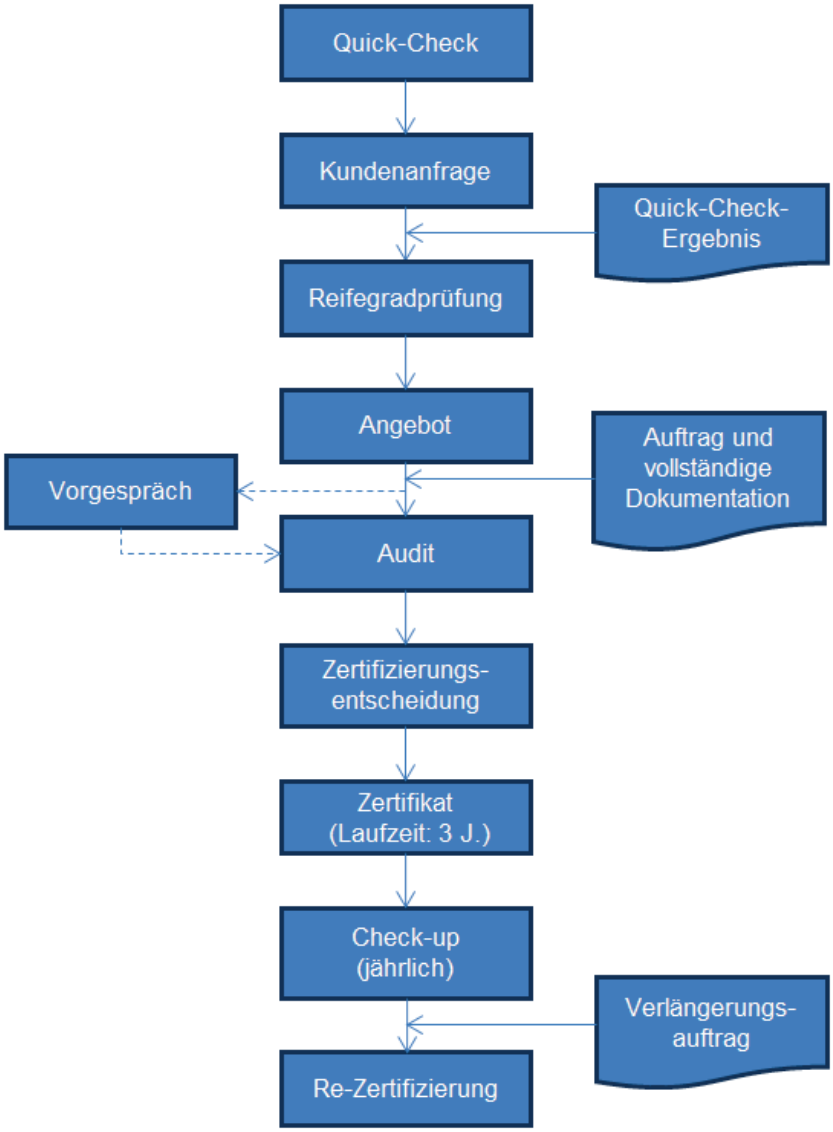

Bild 1-1: Zertifizierungsverfahren, idealer Ablauf

1.2 Gültigkeit

Diese Richtlinien gelten ab dem 01.11.2015. Sie ersetzen die Richtlinien mit Stand 2015-04 (02).

2 Definitionen

Es gelten die in den Richtlinien VdS 3473 sowie die im Folgenden genannten Definitionen.

Audit: systematischer, unabhängiger, dokumentierter Prozess zur Erlangung von Aufzeichnungen, Darlegungen von Fakten oder anderen relevanten Informationen und deren objektiver Begutachtung, um zu ermitteln, inwieweit festgelegte Anforderungen erfüllt sind

Auditor: Person mit den dargelegten persönlichen Eigenschaften und der Kompetenz, ein Audit durchzuführen

Check-up: systematischer Überwachungsprozess

Organisation: Gruppe von Personen und Einrichtungen mit einem Gefüge von Verantwortungen, Befugnissen und Beziehungen

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.

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

VdS 3473 Cyber-Security für kleine und mittlere Unternehmen (KMU), Anforderungen

VdS 3474 VdS Quick-Audit für Cyber-Security, Verfahren

4 Zertifizierungsverfahren

4.1 Auftrag

Die Erstzertifizierung kann schriftlich oder per Fax unter Verwendung des beiliegenden Vordrucks (Anhang A) bei der VdS-Zertifizierungsstelle beauftragt werden. Ergebnisse des Quick-Checks bzw. das Testat über den Quick-Check (vgl. VdS 3474) sowie die in deutscher oder englischer Sprache ausgeführte Dokumentation (Anhang B) des Auftraggebers sollte bereits dem Auftrag beigelegt werden. In Ausnahmefällen können diese Informationen auch nachgeliefert werden. Nur vollständig ausgefüllte Aufträge können bearbeitet werden. Im Einzelfall können von der VdS-Zertifizierungsstelle weitere Unterlagen oder Erläuterungen zum Auftrag angefordert werden.

Die Abwicklung des Schriftverkehrs und die Auditierung erfolgen in deutscher oder englischer Sprache.

Liegen der VdS-Zertifizierungsstelle nicht innerhalb von 6 Monaten nach Beauftragung sämtliche notwendigen Unterlagen vor, wird die Bearbeitung des Auftrages abgebrochen. Ebenso wird die Bearbeitung des Auftrages abgebrochen, wenn das Erstzertifizierungs-

verfahren nicht innerhalb von 18 Monaten nach Beauftragung mit einem positiven Ergebnis abgeschlossen werden kann. Die bis dahin erhaltenen Unterlagen werden an den Auftraggeber zurückgesandt. Alle Aufwendungen, die der VdS-Zertifizierungsstelle bis zu diesem Zeitpunkt entstanden sind, werden dem Auftraggeber in Rechnung gestellt. Danach kann das Erstzertifizierungsverfahren nur durch einen neuen Auftrag wieder aufgenommen werden.

4.2 Auditierung

4.2.1 Auditplanung

Vor jedem Audit wird der Auditaufwand ermittelt. Das geschieht auf Grundlage der Ergebnisse des Quick-Checks sowie der Größe, Struktur und der Tätigkeitsfelder des Unternehmens (Reifegradprüfung). Dazu können weitere Teile der Dokumentation beim Auftraggeber angefordert werden. Diese bestehen üblicherweise aus:

- Prozess- und/oder Ablaufbeschreibungen
- Verfahrens- und/oder Betriebsanweisungen
- Schulungsaufzeichnungen
- sonstigen Systemaufzeichnungen

Die Dokumentation muss der zum Zeitpunkt der Auditierung aktuellen Version entsprechen.

Wurde ein ausreichender Reifegrad ermittelt, wird mit dem Auftraggeber ein Auditplan abgestimmt, der das Vorgehen während des Audits beschreibt.

4.2.2 Audit

Nach der Bestätigung des Auftrages durch die VdS-Zertifizierungsstelle wird im Rahmen des Audits die Erfüllung der zugrundeliegenden Richtlinienanforderungen überprüft. Jedes Audit wird beim Auftraggeber von mindestens einem Auditor durchgeführt. Während der Auditierung wird die Erfüllung der Anforderungen gemäß VdS 3473 begutachtet und schriftlich in einem Auditbericht bewertet.

Änderungen des Auftrags (siehe Abschnitt 4.1), die dem Auditor vom Auftraggeber vor Ort mitgeteilt werden und eine Verlängerung der Auditzeit erfordern, können in der Regel nicht mehr berücksichtigt werden.

4.2.3 Abweichungen und Verbesserungsmaßnahmen

Bei Nichterfüllung von Richtlinienforderungen wird vom Auditor in der Regel ein Abweichungsbericht erstellt, in dem die Abweichung detailliert beschrieben wird. Vom Auftraggeber müssen geeignete Korrekturmaßnahmen, in der Regel innerhalb von 2 Monaten, durchgeführt werden. Die Korrekturmaßnahmen sind dem Auditor nachzuweisen. Bereits bei der Erstellung des Abweichungsberichts wird vom Auditor festgelegt, ob dieser Nachweis auf schriftlichem Wege erfolgen kann oder ob ein Nachaudit durchgeführt werden muss.

Werden die Abweichungen nicht in der festgelegten Frist beseitigt, wird dem Auftraggeber mitgeteilt, dass er sein Zertifizierungsverfahren gefährdet. Er erhält dann noch einmal eine Frist von einem Monat, innerhalb der er die Durchführung der Korrekturmaßnahmen nachweisen kann. Wenn der Auftraggeber die Korrekturmaßnahmen auch innerhalb dieser Frist nicht durchgeführt hat, muss ein Nachaudit durchgeführt werden oder das Verfahren wird abgebrochen.

Wird vom Auditor eine Nichtübereinstimmung mit den Anforderungen erkannt, die nicht als Abweichung gewertet werden muss, so kann vom Auditor anstelle des Abweichungsberichts das Formular „Verbesserungsmaßnahmen“ verwendet werden. Verbesserungsmaßnahmen zur Behebung eines solchen Sachverhalts müssen vom Auftraggeber bis zum nächsten Audit realisiert werden. Sofern die erforderlichen Maßnahmen vom Auftraggeber nicht durchgeführt werden, stellt der Auditor darüber beim nächsten Audit einen Abweichungsbericht aus.

4.2.4 Kurzfristig angekündigte Audits

In besonderen Fällen kann die Durchführung von zusätzlichen, kurzfristig angekündigten Audits erforderlich werden. Solche Fälle können begründet sein z. B. durch die Notwendigkeit der Nachverfolgung von Einsprüchen, Beschwerden oder Änderungen sowie als Konsequenz auf das Wiedereinsetzen von eingeschränkten oder widerrufenen Zertifikaten. Für kurzfristig angekündigte Audits wird ebenfalls ein Auditplan erstellt. Die VdS-Zertifizierungsstelle wird bei der Auswahl des Auditteams zusätzliche Sorgfalt walten lassen, da dem Auftraggeber in diesem Fall die Möglichkeit fehlt, gegen Mitglieder des Auditteams Einwand zu erheben.

4.3 Ausstellung des Zertifikates

Nach positivem Abschluss des Audits und – falls erforderlich – der Korrekturmaßnahmen werden die Auditergebnisse einem Mitarbeiter der VdS-Zertifizierungsstelle, der nicht an der Auditierung teilgenommen hat, zur unabhängigen Beurteilung der Zertifizierungswürdigkeit vorgelegt. Dieser Mitarbeiter kann weitere Nachweise vom Auftraggeber fordern.

Bei positiver Beurteilung wird nach nochmaliger formaler Überprüfung durch die Leitung der Zertifizierungsstelle ein Zertifikat ausgestellt und dem Auftraggeber übersandt. Die Gültigkeitsdauer der Zertifikate beträgt in der Regel 3 Jahre. Das Zertifikat wird in deutscher Sprache ausgestellt. Auf Wunsch des Auftraggebers können Zertifikate auch englischsprachig ausgestellt werden.

4.4 Check-up, Re-Zertifizierung, Änderung, Ergänzung

4.4.1 Check-up

Nach der erfolgreichen Zertifizierung vereinbart der Auditor mit dem Auftraggeber einen Termin für den nächsten Check-up. Zeitgleich wird der Auftraggeber aufgefordert, den Auditor bis zu einem vereinbarten Zeitpunkt vor dem nächsten Check-up über zwischenzeitlich erfolgte Änderungen in den Tätigkeiten, der Dokumentation oder der Organisation des Auftraggebers zu informieren.

Der erste Check-up nach einem Erst- oder Re-Zertifizierungsaudit soll in der Regel 11 Monate ± 2 Monate, der zweite Check-up 22 Monate ± 2 Monate nach dem Beginn der Laufzeit des Zertifikates durchgeführt werden. Sollte aus Gründen, die der Auftraggeber zu vertreten hat, ein Check-up nicht innerhalb der vorgegebenen Zeiträume durchgeführt werden können, so muss das Zertifikat widerrufen werden (siehe Abschnitt 5).

Werden bei den Check-ups – entweder bei der Kontrolle eingereichter Informationen oder beim entsprechenden Audit vor Ort – Abweichungen zu den Anforderungen an die IT-Sicherheit oder zu den vom Auftraggeber gemachten Angaben und den Gegebenheiten vor Ort festgestellt, wird der Auftraggeber zur Nachbesserung innerhalb einer angemessenen Frist (maximal 2 Monate) aufgefordert (siehe Abschnitt 4.2.3). Werden die Abweichungen nicht in der festgelegten Frist beseitigt, wird dem Auftraggeber mitgeteilt, dass er seine Zertifizierung gefährdet. Er erhält dann noch einmal eine Frist von einem Monat, innerhalb der er die Korrekturmaßnahmen nachweisen kann. Sollte auch diese

Frist ohne Einreichung entsprechender Nachweise ablaufen, muss das Zertifikat von der VdS-Zertifizierungsstelle widerrufen werden (siehe Abschnitt 5).

Nach positivem Abschluss der Check-ups und – falls erforderlich – der Korrekturmaßnahmen werden die Auditergebnisse einem Mitarbeiter der VdS-Zertifizierungsstelle, der nicht an der Auditierung teilgenommen hat, zur unabhängigen Beurteilung der weiteren Zertifizierungswürdigkeit vorgelegt. Dieser Mitarbeiter kann ergänzende Nachweise vom Auftraggeber fordern.

4.4.2 Re-Zertifizierung

Die Gültigkeit der Zertifizierung kann durch Beauftragung erneuert werden. Nach dem zweiten Check-up erhält der Auftraggeber dazu einen entsprechend vorbereiteten Auftragsvordruck. Dieser Auftrag zur sogenannten Re-Zertifizierung (siehe Anhang A) muss der VdS-Zertifizierungsstelle spätestens 6 Monate vor Ablauf des Zertifikats vorliegen.

Voraussetzung für die Re-Zertifizierung ist der erfolgreiche Abschluss eines Re-Audits. Das Re-Audit kann frühestens 4 Monate vor Ablauf der Gültigkeit des Zertifikates durchgeführt werden.

Das Re-Audit stellt ein komprimiertes Audit dar, in dem alle Forderungen der VdS 3473 geprüft werden. Abweichungen und Verbesserungsmaßnahmen werden gemäß Abschnitt 4.2.3 behandelt, jedoch ohne die Möglichkeit eines Nachaudits nach Ablauf der noch gültigen Zertifikatslaufzeit. Die Ausstellung eines neuen Zertifikates erfolgt dann gemäß Abschnitt 4.3. Dabei wird nach Möglichkeit ein Zertifikat ausgestellt, dessen Laufzeit nahtlos an das alte Zertifikat anschließt.

Nach Ablauf der Gültigkeit des ursprünglichen Zertifikates darf kein Re-Zertifizierungsverfahren mehr angeboten werden. Dieses muss dann durch ein Erstzertifizierungsverfahren ersetzt werden (siehe Abschnitte 4.1 – 4.3).

4.4.3 Änderung/Ergänzung von Zertifikaten

Ergänzungen (z. B. Erweiterung des Geltungsbereiches) oder Änderungen (z. B. Änderungen der Zertifizierungsgrundlagen, Umzug oder Umfirmierung) während der Laufzeit des Zertifikates sind schriftlich zu beauftragen (siehe Anhang A). In der Regel muss dann durch ein Audit nachgewiesen werden, dass die Anforderungen der VdS 3473 noch erfüllt sind. Ergänzungen und Änderungen von Zertifikaten können auch im Rahmen von Check-ups geprüft werden.

Geringfügige Änderungen und Ergänzungen (z. B. Änderung der Firmenbezeichnung) können auch ohne ein Audit vor Ort erfolgen. Einzelheiten dazu sind mit der VdS-Zertifizierungsstelle abzusprechen.

4.4.4 Wiederaufnahme von widerrufenen oder eingeschränkten Zertifizierungen

Ein durch Widerruf/Einschränkung (siehe Abschnitt 5) ungültig gewordenes VdS-Zertifikat kann nur mit einer Frist von 6 Monaten innerhalb des ursprünglichen Gültigkeitszeitraums durch ein Wiederaufnahmeverfahren wieder eingesetzt werden. Die Beauftragung hierzu erfolgt unter Verwendung der Aufträge gemäß Anhang A.

Zur Wiederaufnahme der Zertifizierung muss ein Re-Audit durchgeführt werden, in dem insbesondere die Mängel auditiert werden, die zum Widerruf/zur Einschränkung des Zertifikates geführt haben. Dabei bestimmt der erfolgreiche Abschluss des Re-Zertifizierungsverfahrens den Beginn des Zertifizierungszeitraumes. Das ursprüngliche Ende der Zertifikatsgültigkeit und die Zertifizierungsnummer werden beibehalten.

Nach Ablauf der 6-Monatsfrist bzw. der ursprünglichen Zertifikatsgültigkeit muss ein vollständiges Erstzertifizierungsverfahren (siehe Abschnitte 4.1 – 4.3) durchgeführt werden.

5 Widerruf/Einschränkung

Zertifikate können widerrufen und damit ungültig bzw. im Geltungsbereich eingeschränkt und damit teilweise ungültig werden.

Der Widerruf/die Einschränkung erfolgt, wenn

- die dem Auftrag zugrunde liegenden Richtlinien oder Normen sich ändern und diese Änderungen vom Auftraggeber nicht innerhalb einer angemessenen Frist umgesetzt werden
- der Auftraggeber es dauerhaft oder schwerwiegend versäumt hat, die Zertifizierungsanforderungen für alle Teile des Geltungsbereiches zu erfüllen
- bei den Check-ups Abweichungen festgestellt werden und diese nicht innerhalb von 3 Monaten vom Auftraggeber behoben werden
- Zertifikate oder das Zertifizierungslogo nicht korrekt verwendet werden (z. B. durch Missbrauch oder unlautere Werbung)
- der Auftraggeber seinen Pflichten (z. B. Zahlung von Gebühren) verletzt
- Check-ups nicht rechtzeitig durchgeführt werden
- sich der Auftraggeber in dieser oder einer anderen Geschäftsbeziehung zwischen den Parteien als unzuverlässig erweist (z. B. Täuschung, Kompromittierung)
- der Auftraggeber den Widerruf/die Einschränkung freiwillig schriftlich verlangt.

Der Widerruf/die Einschränkung der Zertifizierung wird dem Auftraggeber schriftlich mitgeteilt. Dagegen kann innerhalb von 2 Monaten Einspruch erhoben werden.

Nach dem Widerruf/der Einschränkung des Zertifikates verpflichtet sich der Auftraggeber, jegliche Werbung, die sich in irgendeiner Weise auf die Zertifizierung bezieht, sofort zu unterlassen bzw. zu korrigieren und sämtliche von der Zertifizierungsstelle geforderten Zertifizierungsdokumente zurückzugeben. Die VdS-Zertifizierungsstelle muss auf Anfragen einer beliebigen Partei den gegenwärtigen Zertifizierungsstatus korrekt angeben.

6 Werbung

Die Werbung mit der VdS-Zertifizierung muss den Inhalt des aktuell ausgestellten Zertifikates korrekt wiedergeben. Die Werbung darf nicht den Eindruck erwecken, dass Produkte oder Dienstleistungen des Auftraggebers VdS-zertifiziert wurden oder dass eine VdS-Anerkennung als Fachfirma ausgesprochen wurde; es sei denn, es bestehen solche Anerkennungen. Die diesbezüglichen Vorgaben auf dem Zertifikat sind einzuhalten.

Es ist untersagt, die Marke *VdS* oder Abwandlungen hiervon bzw. die Zertifizierung als solche in die Firmenbezeichnung aufzunehmen.

Der Auftraggeber darf auf seine VdS Zertifizierung mit folgendem Logo hinweisen:

Das Logo darf unter Beibehaltung der Proportionen vergrößert oder verkleinert werden. Eine Mindesthöhe von 13 mm für die quadratische Umrandung des VdS-Zeichens darf nicht unterschritten werden. Bei Farbdruck ist HKS 42 (oder eine vergleichbare Farbe) zu verwenden. Das Logo darf auf Briefköpfen, Werbeschriften und Veröffentlichungen des Auftraggebers verwendet werden, nicht jedoch direkt auf Produkten oder Produktverpackungen. Das Logo darf nicht in Verbindung mit Leistungen des Auftraggebers gebracht werden, die nicht durch den Zertifizierungsumfang abgedeckt sind.

Das Zeichen darf nicht auf Produkten oder Produktverpackungen des Auftraggebers aufgebracht werden.

Im Zweifelsfall sind die Werbung und die Verwendung des Logos mit der VdS-Zertifizierungsstelle abzustimmen.

7 Gebühren

Das Zertifizierungsverfahren sowie die Prüf- und Audittätigkeiten der VdS-Zertifizierungsstelle sind gebührenpflichtig. Die Höhe der Gebühren kann der Gebührentabelle der VdS-Zertifizierungsstelle entnommen werden. Die Gebührentabelle kann dem Auftraggeber auf Anfrage zugesandt werden. Für die Berechnung der Leistungen gelten die Gebühren nach Maßgabe der Gebührentabelle zum Zeitpunkt der Leistungserbringung.

Wird ein vereinbarter Audittermin aus Gründen, die der Auftraggeber zu vertreten hat, abgesagt oder verschoben, werden dem Auftraggeber folgende Gebühren in Rechnung gestellt:

- Bei einer Absage/Verschiebung, die kurzfristiger als vier Wochen vor dem vereinbarten Audittermin erfolgt: 25 % der veranschlagten Auditkosten.
- Bei einer Absage/Verschiebung, die kurzfristiger als zwei Wochen vor dem vereinbarten Audittermin erfolgt: 50 % der veranschlagten Auditkosten.
- Bei einer Absage/Verschiebung, die kurzfristiger als eine Woche vor dem vereinbarten Audittermin erfolgt: 100 % der veranschlagten Auditkosten.

Die veranschlagten Auditkosten werden nach gültiger Gebührentabelle ermittelt. Reisekosten werden nur berechnet, sofern Stornierungskosten entstanden sind.

8 Sonstiges

8.1 Verpflichtungen des Auftraggebers

Der Auftraggeber muss alle Beanstandungen mit Bezug auf die Zertifizierung und die daraufhin eingeleiteten Maßnahmen detailliert aufzeichnen und dem Auditor auf Verlangen zur Verfügung stellen.

Der Auftraggeber verpflichtet sich, der VdS-Zertifizierungsstelle unverzüglich alle Änderungen mit Bezug auf die Zertifizierung mitzuteilen. Hierzu gehören auch Änderungen wie Umzug, Umfirmierung oder ein Personalwechsel in der Führungsebene bzw. von vertretungsberechtigten Personen.

Weiterhin verpflichtet er sich, sich in regelmäßigen Abständen im Internet unter der Adresse www.vds.de zu informieren, ob neue, für ihn zutreffende Regelwerke von der VdS-Zertifizierungsstelle veröffentlicht wurden. Zu diesen Regelwerken gehören auch Merkblätter und Hinweise, die Bestandteil dieser Richtlinien sind.

Zusätzlich zu dem Angebot im Internet können alle Regelwerke auch in Papierform schriftlich angefordert werden bei.

8.2 Allgemeine Geschäftsbedingungen

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

8.3 Nebenabreden

Nebenabreden bedürfen zu ihrer Wirksamkeit der Schriftform.

9 Änderungen zur Vorversion

- Anpassung des Auftrags (Anhang A) dahingehend, dass der Betriebsstandort, für den die Zertifizierung ausgesprochen werden soll, vom Betriebsstandort des Auftraggebers abweichen darf.

Anhang A Auftrag

Auftrag zur Zertifizierung der Informationssicherheit in kleinen und mittleren Unternehmen (KMU) auf Grundlage der VdS 3475

durch die Zertifizierungsstelle von VdS Schadenverhütung GmbH
Amsterdamer Str. 174, 50735 Köln

A Art des Auftrags (bei Folgeauftrag bitte die Anerkennungsnummer angeben)

☐ Erstauftrag ☐ Verlängerungsauftrag Nr. ITS - _____
☐ Vorgespräch ☐ Änderung/Ergänzung

B Auftraggeber

B.1 Unternehmensbezeichnung _____
B.2 Vertretungsberechtigt _____
B.3 Handelsregistereintrag _____
B.4 Standort (Straße, Haus-Nr.) _____
B.5 Standort (Land, PLZ, Ort) _____
B.6 Telefon-Nr./Fax-Nr. _____
B.7 E-Mailadresse _____
B.8 Internetseite _____
B.9 Kontaktperson (falls abw. von B.2) _____
B.10 Anzahl Mitarbeiter (gesamt) _____
B.11 Anzahl Mitarbeiter (IT-Administration) _____

C Unternehmen bzw. Unternehmensbereich für das/den die Zertifizierung beauftragt wird

C.1 Benennung des Unternehmens _____
C.2 ☐ Standort entspricht den Angaben unter B (Abschnitte C.3-C.7 entfallen)

Falls abweichend bitte nachfolgende Abschnitte ausfüllen:

C.3 Unternehmensbezeichnung _____
C.4 Standort (Straße, Haus-Nr.) _____
C.5 Standort (Land, PLZ, Ort) _____
C.6 Telefon-Nr./Fax-Nr. _____
C.7 E-Mailadresse _____

D Beratungsleistungen erbracht durch

D.1 Unternehmensbezeichnung _____
D.2 Standort (Straße, Haus-Nr.) _____
D.3 Standort (Land, PLZ, Ort) _____

E Ausfertigung des Zertifikats

E.1 ☐ Neben der deutschsprachigen Ausfertigung des Zertifikats wird eine englischsprachige Fassung gewünscht.

F Informationen

F.1 ☐ Der Auftraggeber wünscht die Zusendung themenbezogener Informationen (i.d.R. per Mail);
dem Auftraggeber ist bekannt, dass die Zusage jederzeit ohne Angabe von Gründen widerrufen werden kann.

G Erklärung und Einwilligung

Der Auftraggeber erklärt:
Die

- *Allgemeinen Geschäftsbedingungen*, VdS 3177
- VdS-Richtlinien *Zertifizierung der Informationssicherheit in kleinen und mittleren Unternehmen (KMU)*, VdS 3475
- *Gebührentabelle* für Auditierung und Zertifizierung auf Basis der Richtlinien VdS 3475

erkenne(n) ich (wir) in der jeweils gültigen Fassung als festen Vertragsbestandteil an.

Der Auftraggeber willigt ein,
dass VdS Schadenverhütung GmbH im Rahmen der Zertifizierung personenbezogene und andere Daten erhebt, verarbeitet und nutzt.

Ort, Datum: _____

Unterschrift (sowie ggf. Stempel) des Auftraggebers
(bzw. eines Bevollmächtigten): _____

Stand: 2015-11 (02)

A.1 Hinweise zu Auftragsformular

Bevor Sie den Auftrag ausfüllen, lesen Sie bitte die Richtlinien *Cyber-Security für kleine und mittlere Unternehmen (KMU), Anforderungen,* VdS 3473 und die folgenden Hinweise zum Auftragsformular sorgfältig durch.

(A) Der Auftraggeber ist die zu zertifizierende Stelle, vertreten durch den Rechtsträger oder den Handlungsbevollmächtigten.

(A.2) Firmenname des Auftraggebers, wie er im Handelsregister/Gewerberegister eingetragen ist.

(A.3) Die Umsatzsteuer-Identifikationsnummer ist nur bei Erstaufträgen anzugeben.

(A.7) Angaben zur E-Mail-Adresse des Auftraggebers sind erforderlich, da Informationen überwiegend über dieses Medium ausgetauscht werden.

(A.8) Angaben freiwillig

(A.9) Hauptkontaktperson für dieses Zertifizierungsverfahren

(A.10) Anzahl aller Mitarbeiter im Unternehmen

(A.11) Anzahl der in der IT-Administration tätigen Mitarbeiter

(C.1) Bitte genauso formulieren, wie der Geltungsbereich später auf dem Zertifikat erscheinen soll.

(G) Rechtsverbindliche Unterschrift des Rechtsträgers des Auftraggebers oder eines Handlungsbevollmächtigten. Wurden externe Stellen (z. B. Berater) vom Auftraggeber mit der Auftragsstellung beauftragt, muss die externe Stelle eine Kopie der Handlungsvollmacht des Auftraggebers beilegen.

Anhang B Dokumentation des Auftraggebers

Die Dokumentation beinhaltet unabhängig von individuellen Absprachen mit dem Auftraggeber mindestens:

- Leitlinien zur Informationssicherheit gemäß VdS 3473
- Richtlinien zur Informationssicherheit gemäß VdS 3473