VdS Quick-Audit für Cyber-Security

Verfahren

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

VdS Quick-Audit für Cyber-Security

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 Geltungsbereich ... 4
1.2 Gültigkeit ... 4
2 Definitionen ... 5
3 Normative Verweisungen ... 5
4 Zertifizierungsverfahren ... 5
4.1 Vorarbeiten ... 5
4.2 Auftrag ... 5
4.3 Auditierung ... 6
4.3.1 Allgemeines ... 6
4.3.2 Auditplanung ... 6
4.3.3 Audit ... 6
4.3.4 Korrekturmaßnahmen ... 6
4.3.5 Testat ... 6
4.4 Gültigkeit des Verfahrens ... 7
4.4.1 Gültigkeit ... 7
4.4.2 Wiederholung des Verfahrens ... 7
5 Werbung ... 7
6 Gebühren ... 7
7 Sonstiges ... 7
7.1 Allgemeine Geschäftsbedingungen ... 7
7.2 Nebenabreden ... 7
8 Änderungen zur Vorversion ... 8
Anhang A Auftrag ... 9
A.1 Hinweise zu Auftragsformular ... 10

1 Allgemeines

1.1 Geltungsbereich

VdS Schadenverhütung (nachstehend VdS genannt) bietet KMU nach Beauftragung ein unabhängiges und unparteiliches Verfahren zur Bestätigung kundenseitig getroffener Aussagen zur Informationssicherheit des beauftragenden Unternehmen an.

Aufträge gemäß VdS 3474 werden in der Reihenfolge ihres Eingangs bearbeitet. Eine Bevorteilung einzelner Auftraggeber erfolgt nicht.

Im Rahmen des Bestätigungsverfahrens werden keine Beratungen durchgeführt.

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

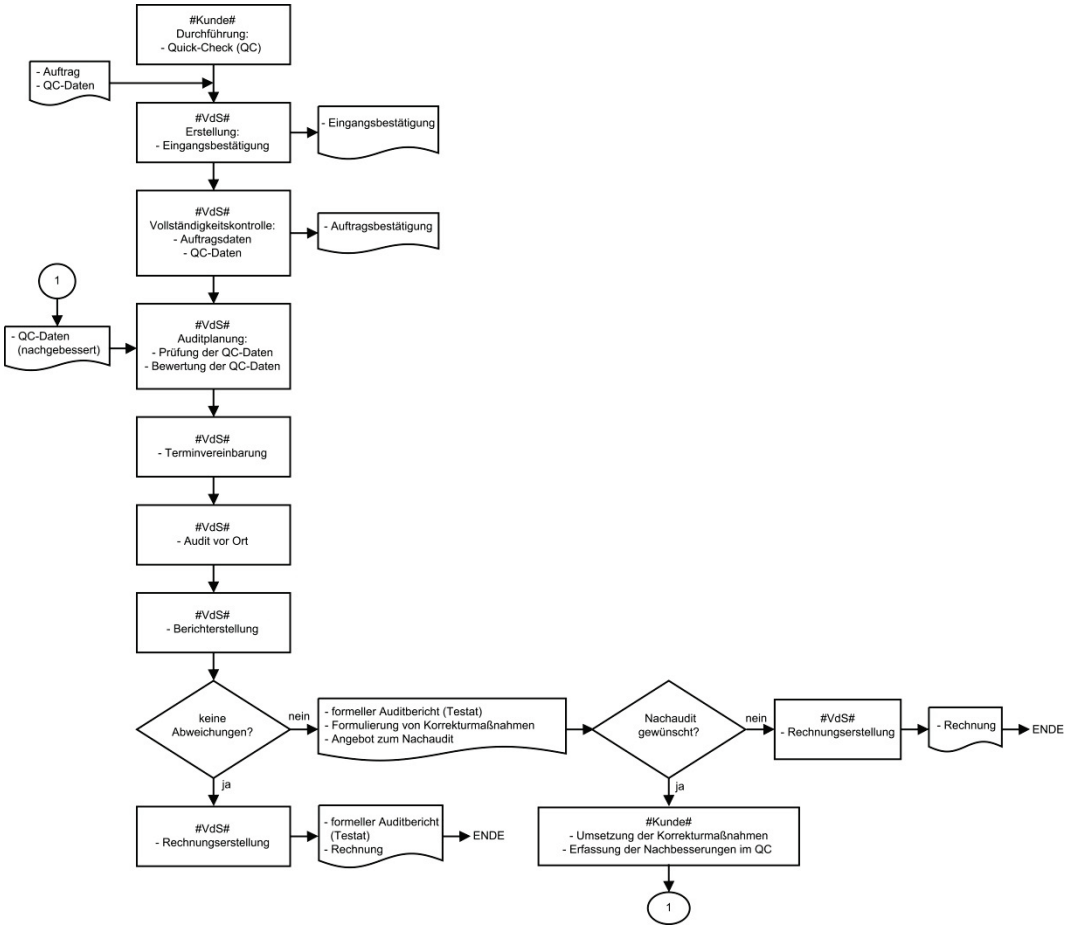

Bild 1-1: Bestätigungsverfahren, idealer Ablauf

1.2 Gültigkeit

Diese Richtlinien gelten ab dem 01.11.2015. Sie ersetzten die Richtlinien mit Stand 2015-03 (01).

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.

Anmerkung: Die Ermittlung, inwieweit festgelegte Anforderungen erfüllt sind, kann im Audit oder im Nachgang zum Audit, durch den Kunden, den Auditor oder einen Dritten erfolgen.

Auditor: Person mit hinreichenden persönlichen Eigenschaften und der Kompetenz, ein Audit durchzuführen.

Quick-Check (Quick-Check für Cyber-Security): Online bereitgestellte Plattform, um strukturierte und definierte Aussagen zum Zustand der Informationstechnik des den Quick-Check bearbeitenden Unternehmens zu machen.

Anmerkung: Zugriff auf den Quick-Check erfolgt unter www.vds-quick-check.de.

Testat: Bestätigung der Übereinstimmung der Aussagen des Auftraggebers zum Quick-Check mit den Gegebenheiten vor Ort zum Zeitpunkt der Begutachtung.

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

4 Zertifizierungsverfahren

4.1 Vorarbeiten

Der Interessent, der ein Testat gemäß VdS 3474 in Auftrag geben möchte, muss vor der Beauftragung den *Quick-Check für Cyber-Security* durchführen. Der Zugang zum Quick-Check ist jedermann kostenfrei (www.vds-quick-check.de) möglich.

4.2 Auftrag

Das Verfahren kann schriftlich unter Verwendung des beiliegenden Vordrucks (Anhang A) bei VdS beauftragt werden. Die Abwicklung des Schriftverkehrs und die Auditierung erfolgen in deutscher oder englischer Sprache. Nur vollständig ausgefüllte Aufträge können bearbeitet werden.

Nach Eingang der Unterlagen wird dem Kunden zeitnah eine Eingangsbestätigung übersandt. Nach positiver Prüfung der Unterlagen auf Vollständigkeit wird dem Kunden eine Auftragsbestätigung übersandt.

Anmerkung: Die Auftragsbestätigung kann die Eingangsbestätigung beinhalten.

Die Ergebnisse des Quick-Checks (ausgedruckt und unterschrieben) müssen dem Auftrag beigelegt werden. In Ausnahmefällen können einzelne Informationen nachgeliefert werden. VdS ist berechtigt, weitere Unterlagen oder Erläuterungen zum Auftrag anzufordern.

Wird das Verfahren nicht innerhalb von 6 Monaten nach Beauftragung abgeschlossen, sei es, weil nicht sämtliche notwendigen Unterlagen vorliegen oder aus anderen Gründen, wird die Bearbeitung des Auftrages abgebrochen. Nach Abbruch des Verfahrens, werden alle VdS bis dahin übergebenen Unterlagen an den Auftraggeber zurückgesandt.

Alle Aufwendungen, die VdS bis zu diesem Zeitpunkt entstanden sind, werden dem Auftraggeber in Rechnung gestellt. Unbenommen hiervon bleibt eine erneute Beauftragung.

4.3 Auditierung

4.3.1 Allgemeines

Die Auditierung hat das Ziel, die vom Kunden im Rahmen des Quick-Check gemachten Aussagen und Ergebnisse zu überprüfen.

Die Bewertung der Angaben hinsichtlich eines Erfüllungsgrades, bezogen auf kundenseitig oder von einem Dritten formulierte Anforderungen bzw. Vorgaben, erfolgt nicht.

4.3.2 Auditplanung

Nach Vorliegen der erforderlichen Unterlagen erfolgt die Auditplanung, die im Wesentlichen auf dem Umfang sowie der Informationstiefe der eingereichten Informationen sowie ggf. der Betriebsgröße fußt.

4.3.3 Audit

Die Überprüfung der vom Kunden im Rahmen des Quick-Checks getroffenen Aussagen erfolgt vor Ort. Hierzu findet ein Audit vor Ort statt. Die Dauer des Audit richtet sich u. a. nach der Unternehmensgröße. Das Audit wird durch eine Fachkraft von VdS bzw. durch eine von VdS beauftragte Fachkraft im Namen von VdS ausgeführt. VdS behält sich vor – ohne Weitergabe des Mehraufwandes – weitere Personen zum Audit zu entsenden.

Während der Auditierung werden die kundenseitigen Aussagen zum Quick-Check verifiziert. Das Ergebnis wird schriftlich in einem vorläufigen Auditbericht dokumentiert.

4.3.4 Korrekturmaßnahmen

Wird bei Auditierung des Quick-Check erkannt, dass die Umsetzung von Korrekturmaßnahmen sinnvoll ist, werden diese vonseiten VdS formuliert. Dem Auftraggeber werden diese Maßnahmen mit dem Angebot, ihre Umsetzung durch ein Nachaudit zu bestätigen, übergeben.

4.3.5 Testat

Im Nachgang zum Audit oder Nachaudit vor Ort wird dem Kunden zeitnah ein Testat über das Audit (formeller Auditbericht) zur Verfügung gestellt.

4.4 Gültigkeit des Verfahrens

4.4.1 Gültigkeit

Die im Testat getroffenen Aussagen beziehen sich ausschließlich auf die VdS im Rahmen des konkreten Verfahrens vorgelegten und vor Ort verifizierten Angaben zur Sicherheit der Informationssicherheit des Auftraggebers.

4.4.2 Wiederholung des Verfahrens

Das Verfahren gemäß VdS 3474 kann nach Abbruch oder nach formeller und ordnungsgemäßer Beendung jederzeit nach erneuter Beauftragung durch den Kunden wiederholt durchlaufen werden.

Anmerkung: Dies kann sinnvoll sein, wenn sich z. B. die Rahmenbedingungen beim Unternehmen geändert haben und diese Dritten gegenüber bestätigt werden sollen.

5 Werbung

Werbung mit dem Durchlaufen des Verfahrens gemäß VdS 3474 darf nicht erfolgen.

Anmerkung: Dritten darf das Testat (vgl. Kap. 4.3.5) vollständig und in unveränderter Form zu Nachweiszwecken ausgehändigt werden.

6 Gebühren

Das Bestätigungsverfahren sowie die Prüf- und Audittätigkeiten von VdS sind gebührenpflichtig. Die Höhe der Gebühren kann der Gebührentabelle von VdS 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.

7 Sonstiges

7.1 Allgemeine Geschäftsbedingungen

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

7.2 Nebenabreden

Nebenabreden bedürfen zu ihrer Wirksamkeit der Schriftform.

8 Änderungen zur Vorversion

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

Anhang A Auftrag

Auftrag zur Prüfung und Bestätigung von Aussagen zur Informationssicherheit auf Grundlage der VdS 3474

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

A Auftraggeber

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

B Unternehmen bzw. Unternehmensbereich für das/den die Prüfung/Bestätigung beauftragt wird

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

Falls abweichend bitte nachfolgende Abschnitte ausfüllen:

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

C Beratungsleistungen erbracht durch

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

D Ausfertigung des Testats

D.1 ☐ Neben der deutschsprachigen Ausfertigung des Testats wird eine englischsprachige Fassung gewünscht.

E Informationen

E.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.

F Erklärung und Einwilligung

Der Auftraggeber erklärt:

Die
- *Allgemeinen Geschäftsbedingungen*, VdS 3177
- VdS-Richtlinien *VdS Quick-Audit für Cyber-Security*, VdS 3474
- *Gebührentabelle* für Auditierung und Testierung auf Basis der Richtlinien VdS 3474

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

Der Auftraggeber willigt ein,
dass VdS Schadenverhütung GmbH im Rahmen der Prüfung/Bestätigung 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 *VdS Quick-Audit für Cyber-Security*, VdS 3474 und die folgenden Hinweise zum Auftragsformular sorgfältig durch.

(A) Der Auftraggeber ist die Stelle, vertreten durch den Rechtsträger oder den Handlungsbevollmächtigten, für die ein Testat ausgestellt werden soll.

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

(A.3) Der Handelsregistereintrag 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

(B.1) Bitte genauso formulieren, wie der Geltungsbereich später im Auditbericht erscheinen soll.

(F) 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.