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

VdS-Richtlinien für die Informationssicherheit

VdS Quick-Audit für Cyber-Security

Verfahren

Die vorliegende Publikation ist unverbindlich. Anwender können im Einzelfall auch andere Sicherheitsvorkehrungen akzeptieren und anwenden, die den vorliegenden Richtlinien nicht entsprechen.

Inhalt

1 Allgemeines

1.1 Geltungsbereich

VdS Schadenverhütung (nachstehend VdS genannt) bietet KMU und sonstigen Parteien (z. B. Versicherungsunternehmen) nach Beauftragung ein unabhängiges und unparteiliches Verfahren zur Überprüfung durch Selbstauskunft getroffener Aussagen zur Informationssicherheit 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.

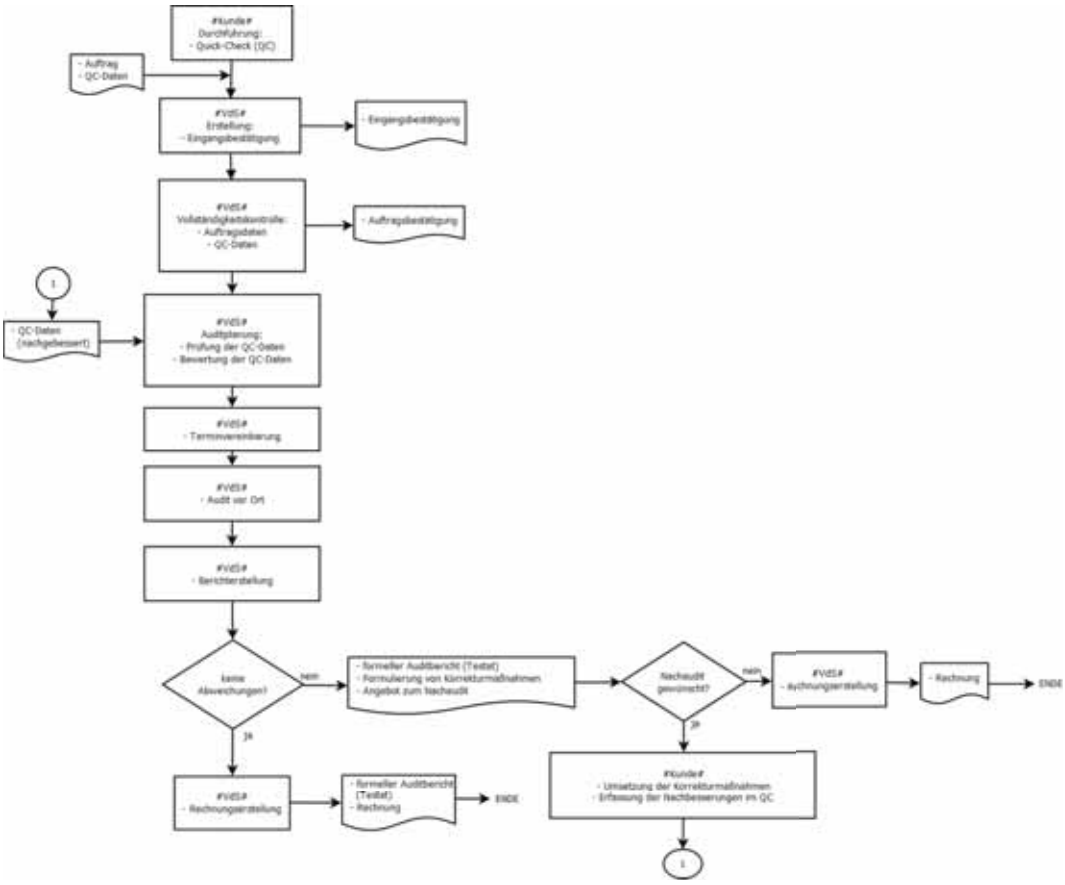

Bild 1-1: Bestätigungsverfahren, idealer Ablauf

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

1.2 Gültigkeit

Diese Richtlinien gelten ab dem 01.10.2017. Sie ersetzten die Richtlinien mit Stand 2015-11 (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

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

KMU: kleine und mittlere Unternehmen

Quick-Check (Quick-Check für Cyber-Security): Online bereitgestellte Plattform, um strukturierte und definierte Aussagen zum Zustand der Informationssicherheit 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

Unternehmen: privatwirtschaftliche oder öffentliche, üblicherweise eigenständige Organisationseinheit oder Körperschaft und Anstalten des öffentlichen Rechts

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

Ein Unternehmen, für das ein Testat gemäß VdS 3474 abgegeben werden soll, muss vor der Beauftragung den *Quick-Check für Cyber-Security* durchführen. Der Zugang zum Quick-Check ist kostenfrei (www.vds-quick-check.de) möglich.

4.2 Auftrag

Das Verfahren kann nur schriftlich unter Verwendung des beiliegenden Vordrucks (Anhang A/B) bei VdS beauftragt werden.

Die Beauftragung kann durch:

- das Unternehmen direkt (Anhang A)
- einen Dritten (Anhang A und B)

erfolgen.

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 Auftraggeber zeitnah eine Eingangsbestätigung übersandt.

Nach positiver Prüfung der Unterlagen auf Vollständigkeit wird dem Auftraggeber eine Auftragsbestätigung übersandt.

Anmerkung: Die Auftragsbestätigung kann die Eingangsbestätigung beinhalten.

Die Ergebnisse des Quick-Checks müssen dem Auftrag beigefügt werden (siehe Abschnitt 4.1).

Erfolgt die Beauftragung durch einen Dritten (z. B. Versicherungsunternehmen), so ist dem Auftrag (Anhang A) die schriftliche Einverständniserklärung des zu überprüfenden Unternehmens (Anhang B) beizulegen.

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 im Rahmen des Quick-Checks getroffenen 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 Termin- und Auditplanung

Nach Vorliegen der erforderlichen Unterlagen erfolgt die Termin- und Auditplanung, die im Wesentlichen auf Umfang und Detaillierungsgrad der eingereichten Informationen sowie ggf. der Betriebsgröße basiert.

4.3.3 Audit

Die Überprüfung der im Rahmen des Quick-Checks getroffenen Aussagen erfolgt vor Ort. Hierzu findet ein Audit vor Ort statt. Das Audit wird durch einen VdS-Auditor bzw. durch einen von VdS beauftragten, für diesen Zweck qualifizierten Auditor im Namen von VdS ausgeführt. VdS behält sich vor – ohne Weitergabe des Mehraufwandes – weitere Personen zum Audit zu entsenden.

Während der Auditierung werden die im Quick-Check getroffenen Aussagen verifiziert. Das Ergebnis wird schriftlich in einem Auditbericht dokumentiert. Der Auditbericht wird nach dem Audit dem Auftraggeber übergeben. Ist der Auftraggeber nicht identisch mit dem auditierten Unternehmen, so steht es dem Auftraggeber frei, den Auditbericht vollständig oder in Teilen dem auditierten Unternehmen zu überlassen.

4.3.4 Korrekturmaßnahmen

Wird während der Auditierung erkannt, dass die Umsetzung von Korrekturmaßnahmen sinnvoll ist, können diese von Seiten VdS formuliert werden.

Diese Maßnahmen werden mit dem Angebot, ihre Umsetzung durch ein Nachaudit zu bestätigen, dem Auftraggeber übergeben.

4.3.5 Testat

Im Nachgang zum Audit oder Nachaudit vor Ort wird dem Auftraggeber auf Wunsch ein Testat über das Audit zur Verfügung gestellt.

4.4 Gültigkeit des Verfahrens

4.4.1 Gültigkeit

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

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

- das Unternehmern
- einen Dritten

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 wird dem Auftraggeber auf Anfrage zugesandt. Für die Berechnung der Leistungen gelten die Gebühren nach Maßgabe der Gebührentabelle zum Zeitpunkt der Leistungserbringung.

Wird ein vereinbarter Audittermin aus Gründen, die das zu auditierende Unternehmen 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.

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,

A) für die die Prüfung durchgeführt und ein Testat ausgestellt werden soll.

B) die die Überprüfung eines Dritten beauftragt.

(A.1) Firmenname des Auftraggebers, wie er im Handelsregister/Gewerberegister eingetragen ist.

(A.2/B.2) Bitte genau so formulieren, wie es später im Testat erscheinen soll.

(A.4) Die Umsatzsteuer-Identifikationsnummer ist nur bei Erstaufträgen anzugeben.

(A.10) Hauptkontaktperson für dieses Verfahren

(A.11/B.9) Anzahl aller Mitarbeiter im zu prüfenden Unternehmensbereich

(A.12/B.10) Anzahl der Mitarbeiter, die für die Administration und den Betrieb der IT-Infrastruktur im zu prüfenden Unternehmensbereich zuständig sind.

(C) Falls ein entsprechendes Beratungsunternehmen im Vorfeld konsultiert wurde, kann dieses hier genannt werden.

(E) 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.

(F.1) Hier ist zum Zweck der Zuordenbarkeit und Rückverfolgbarkeit der Auftraggeber gemäß Anhang A zu nennen.

(F.2) Hier ist zum Zweck der Zuordenbarkeit und Rückverfolgbarkeit das Ausfertigungsdatum des zugehörigen Auftrags gemäß Anhang A zu nennen.

Anhang A Auftrag

Anhang A:

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	zu prüfender Unternehmensbereich	
A.3	Vertretungsberechtigt	
A.4	USt.IdNr.	
A.5	Standort (Straße, Haus-Nr.)	
A.6	Standort (Land, PLZ, Ort)	
A.7	Telefon-Nr./Fax-Nr.	
A.8	E-Mailadresse	
A.9	Internetseite	
A.10	Kontaktperson (falls abw. von A.2)	
A.11	Anzahl Mitarbeiter (gesamt)	
A.12	Anzahl Mitarbeiter (IT-Administration)	

B Angaben des Unternehmens, für das die Prüfung/Bestätigung beauftragt wird

☐ Angaben entsprechen denen unter A (Abschnitte B.3-B.10 entfallen)

☐ Angaben entsprechen nicht denen unter A (bitte Abschnitte B.3-B.10 ausfüllen und Einverständniserklärung des Unternehmens, für das die Prüfung/Bestätigung beauftragt wird, gemäß Anhang B beifügen)

B.1	Unternehmensbezeichnung	
B.2	zu prüfender Unternehmensbereich	
B.3	Standort (Straße, Haus-Nr.)	
B.4	Standort (Land, PLZ, Ort)	
B.5	Telefon-Nr./Fax-Nr.	
B.6	E-Mailadresse	
B.7	Internetseite	
B.8	Kontaktperson	
B.9	Anzahl Mitarbeiter (gesamt)	
B.10	Anzahl Mitarbeiter (IT-Administration)	

C Beratungsleistungen erbracht durch

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

D Ausfertigung des Testats/Informationen

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

☐ 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.

E Erklärung und Einwilligung

Der Auftraggeber erklärt, die Allgemeinen Geschäftsbedingungen (VdS 3177), die VdS-Richtlinien „VdS Quick-Audit für Cyber-Security" (VdS 3474) und die zugehörige Gebührentabelle (Modul Y) in der jeweils gültigen Fassung als festen Vertragsbestandteil anzuerkennen. 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: 2017-10 (03)

Anhang B Einverständniserklärung

Anhang B:

Einverständniserklärung zum 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

Im Falle eines Auftrages zur Prüfung und Bestätigung von Aussagen zur Informationssicherheit auf Grundlage der VdS 3474 für ein Unternehmen, das nicht mit dem Auftraggeber gemäß Anhang A identisch ist, muss das zu prüfende Unternehmen diese Erklärung abgeben.

F Einverständniserklärung

Diese Erklärung ist gültig in Verbindung mit folgendem Auftrag:

F.1 Auftraggeber (gemäß Anhang A) _____

F.2 vom _____

Das Unternehmen erklärt sein Einverständnis

- mit dem vorgenannten Auftrag zur Prüfung und Bestätigung von Aussagen zur Informationssicherheit auf Grundlage der VdS 3474
- die Planung und Durchführung der Prüfung im üblichen Rahmen zu unterstützen
- mit dem Verbleib der Auditaufzeichnungen beim Auftraggeber
- mit der Tatsache, dass VdS Schadenverhütung GmbH im Rahmen der Prüfung/Bestätigung personenbezogene und andere Daten erhebt, verarbeitet und nutzt

Ort, Datum: _____

Unterschrift (sowie ggf. Stempel) des zu prüfenden Unternehmens: _____

Stand: 2017-10 (03)