



Guidelines for the approval of consultants for Cyber Security

Publisher and publishing house: VdS Schadenverhütung GmbH

Amsterdamer Str. 172-174

50735 Köln, Germany

Phone: +49 221 77 66 0; Fax: +49 221 77 66 341

Copyright by VdS Schadenverhütung GmbH. All rights reserved.

VdS Guidelines for Information Security

Guidelines for the approval of consultants for Cyber Security

The present publication is not binding. Third parties may in single cases accept other security precautions based on conditions which were determined at their own discretion and which do not correspond with these procedure guidelines.

Content

1	Scope	4
1.1	General	4
1.2	Validity	4
2	Definitions	4
3	Normative references	4
4	VdS approval	5
4.1	Requirements for the applicant	5
4.1.1	Approval procedure.....	5
4.1.2	Conditions for approval	5
4.1.3	Placing of order and documentation to be handed in	8
4.1.4	Obligations	8
4.2	Preconditions for granting the approval	8
4.2.1	Check of documentation	8
4.2.2	Issue of the initial approval	9
4.3	Prolongation of the approval	9
4.3.1	Requirements.....	9
4.3.2	Prolongation of the approval	10
4.4	Expiry of the approval	10
5	Modification of the approval	10
6	Revocation	10
7	Advertising	11
8	Fees	11
9	Miscellaneous	11
9.1	General Terms and Conditions	11
9.2	Supplements	12
10	Changes to prior version	12
Annex A	Application	13

1 Scope

1.1 General

It is essential for the success of a company to offer competitive products or services. Also, the use of modern information technology (IT) for the challenge of economic, logistic and technical business processes as well as the permanent networking via the internet is essential to counteract the worldwide competition. Digitalization and networking have multiple advantages, but cover also new risks which companies have to consider in their risk management. A well-organized internal information security reduces the risks by mitigating weak spots and thus limiting possible negative effects on the company.

The guidelines VdS 3473 describe requirements on the information security in companies and are tuned to the protection necessities of small and medium-sized enterprises (SMEs). They base on the knowledge of the BSI IT-Grundschutz Catalogues, the BSI standards and the standards ISO 27001 and 27002.

Consultancy services by providers in the sense of these guidelines should aim to check the IT security of SMEs and to enable the enterprise which has been consulted to toughen up its IT security in such way, that a formal VdS-approval (VdS quick audit according to VdS 3474 or certification of the information security according to VdS 3475) may be realized.

The certification body of VdS Schadenverhütung GmbH (in the following VdS certification body), on respective application, approves service providers for the consultancy of information security technology (cyber security). This approval will be pronounced, provided all requirements of these guidelines are fulfilled, by VdS certification body and is timely limited. The approval is documented by a certificate. VdS-approved IT-consultants are listed on the VdS website.

1.2 Validity

These guidelines are valid from 01.11.2015. They replace the version 2015-10 (02).

Note: This document is a translation of the German version. In case of discrepancies the German version shall be binding.

2 Definitions

The definitions as in the guidelines VdS 3473 apply.

3 Normative references

These guidelines include dated and undated references to other publications. The normative references are cited at the relevant sections, the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to these guidelines only when announced by a change of these guidelines. For undated references the latest edition of the publication referred to will be applied.

DIN EN ISO/IEC 17024	Konformitätsbewertung – Allgemeine Anforderungen an Stellen, die Personen zertifizieren (Conformity assessment – General requirements for bodies operating certification of persons)
-----------------------------	--

VdS 3177	AGB der VdS Schadenverhütung GmbH für die Erbringung von Prüf- und Zertifizierungsdienstleistungen (General Terms and Conditions of VdS Schadenverhütung GmbH for providing testing and certification services)
VdS 3473	Informationssicherheit in kleinen und mittleren Unternehmen (KMU), Anforderungen (Information security in small and medium-sized enterprises (SMEs), requirements)
VdS 3474	VdS Quick-Audit für Cyber-Security, Verfahren (VdS quick audit for cyber security, procedure)
VdS 3475	Zertifizierung der Informationssicherheit in kleinen und mittleren Unternehmen (KMU), Verfahren (Certification of information security in small and medium-sized enterprises (SMEs), procedure)
ISO/IEC 27001	Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (Information technology – Security techniques – Information security management systems – Requirements)

4 VdS approval

4.1 Requirements for the applicant

4.1.1 Approval procedure

Applications for approval are handled in sequence of receipt.

If the applicant fulfills the approval requirements, he receives an approval with a limited validity of 4 years. This approval may be prolonged – if the requirements of the guidelines are fulfilled – on respective application for further four years.

The applicant shall fulfill all approval requirements. The VdS certification body reserves the right to assess the compliance with these requirements by suitable measures.

The applicant acknowledges

- a) the present guidelines VdS 3477 as fix part of the contract as well as basis for the VdS approval as IT-consultant
- b.1) the guidelines VdS 3473 as basis for his consulting services
- b.2) the guidelines VdS 3474 as basis for the consulting target *VdS quick audit*
- b.3) the guidelines VdS 3475 as basis for the consulting target *VdS certification of the information security*

4.1.2 Conditions for approval

The approval as consultant for cyber security requires that all conditions listed in the following are fulfilled and have been confirmed to VdS certification body by respective proofs.

The applicant

- a) has a completed academic study on informatics (academy or technical college).

Proof: Copy of graduation certificate.

and

- a.1) has at least a 3-year practical and founded experience in information technology (consulting, planning, administration or implementation services with the focus on IT security), which has been gained within the last 5 years. The professional activity during this time covers at least 50 % of a full-time job.

Proof: Personal data sheet including a detailed description of activities (description in respect of content and duration of activity).

Alternatively – without completed academic study of the informatics (academy or technical college):

- a.2) has at least 5 year practical and founded experience in information technology (consulting, planning, administration or implementation services with the focus on IT security) which has been gained within the last 7 years before application. The professional activity during this time covers at least 50 % of a full-time job.

Proof: Personal data sheet including detailed description of activities (description in respect of content and duration of activity).

- b) is currently working as a consultant for cyber security (at least 6 months within the last year before application). The professional activity during this time covers at least 50 % of a full-time job.

Proof: Personal data sheet including detailed activity description (description in respect of content and duration of the activities).

- c) possesses a clearance certificate without remarks which has been issued at the most 6 months before application.

Proof: copy of the clearance certificate.

- d) assures – if no freelance work is given – that he is able to unrestrictedly exercise the activity as consultant for cyber security.

Proof: Confirmation of the employer that no restriction on content or labor legislation exists to realize activities as a VdS-approved cyber consultant.

Note: In each case a free and objective consultancy service in all conscience shall be possible, independently of a possible economic dependency to the employer.

- e) gives proof of knowledge on popular attack methods, analysis of critical points, risk analysis, evaluation of security events, IT security products and IT security systems.

Proof: Certificate on approved formations which have been gained at the most 3 years before application or to which regular trainings can be proven.

Admitted formations are e. g.:

- Certified Information Security Manager (CISM)
- Certified Information System Auditor (CISA)
- ITIL-Expert
- Certified Information System Security Professional (CISSP)
- Teletrust Information Security Professional (TISP)

- Certified Security Practitioner
- ISMS Auditor/Lead Auditor according to ISO/IEC 27001
- ISO 27001-Auditor on base of the IT-Grundschutz
- All IT-Professionals/Operative Professionals as well as other formation attainments with focus on IT security which were gained at chambers under public law.

Proof: Certificate.

Alternatively, similar trainings may be accepted which lasted at least 5 days (40 h), which trained the following items and which have confirmed the formation aim by a test:

- IT-Governance and IT-Management
 - Security and data protection management
 - Risk and weak points management
 - Business Continuity Management and Emergency Response
 - Judicially – relevant laws, guidelines and standards on IT security
- Hardware/Software
 - Penetration of IT systems
 - Applications and software development
 - Security of system software – Windows/Unix
 - Hacker attacks
 - Storage and backup management
 - Cryptography
- Network and infrastructure
 - Network security and configuration
 - Public-Key-Infrastructure (PKI)
 - Configuration and securing of firewalls
 - Routing/Switching

Proof: Certificate with description of training contents and timely extent.

Furthermore, the applicant gives proof to VdS of the extensive knowledge of at least three of the topics mentioned under f) to k) in the following.

The applicant has

- f) administrator experience for the protection against computer based attacks as well as extensive knowledge on IT security products and IT systems
- g) experience on IT-related business continuity management processes
- h) knowledge of current attack methods and the ability to analyze existing IT systems and structures for possible weak spots
- i) knowledge on the evaluation of risks for an enterprise (SME) arising from the IT landscape
- j) knowledge on the evaluation of security events

- k) knowledge on profit, effectivity and weak spots of currently used IT products and ability to evaluate such systems from the IT security perspective

Proof of the requirements according to f) to k): Detailed description of activity by the applicant or in form of a job reference.

- l) knowledge of specific legal regulations

Proof: Certificate of successful training as data security officer or via the VdS-training for information security officers.

- m) knowledge of the guidelines on cyber security, especially of VdS 3473.

Proof: Confirmation of successful attendance of relevant trainings, e. g. VdS-training for information security officers, training on the guidelines VdS 3473, ISO/IEC 27000-series, on BSI-Grundschutzkatalog or similar.

- n) Furthermore the applicant confirms bindingly that he in possession or has short-notice access to all necessary standards and guidelines in the actual version (e. g. ISO/IEC 27000-series as well as the VdS guidelines on cyber security).

4.1.3 Placing of order and documentation to be handed in

The approval as VdS-approved IT-consultant shall be applied for in writing by Annex A (available as separate pdf-file) at the VdS certification body. The form shall be filled in completely and be signed by the applicant. The proofs on knowledge and abilities shall be attached as annexes.

4.1.4 Obligations

The applicant commits to

- become active only if his impartiality is guaranteed.
- That means inter alia that no consultancy services on cyber security shall be offered to customers resp. objects simultaneously to audits of the cyber security.
- to take part at relevant advanced trainings, e. g. offered by VdS Schadenverhütung or by VdS-accepted trainings.
- to fulfil his financial obligations towards VdS Schadenverhütung.

4.2 Preconditions for granting the approval

4.2.1 Check of documentation

The check of the application and the handed-in documentation and proofs of the applicant according to clause 4.1 shall not lead to objections.

If VdS certification is of the opinion, that the expert ability of a person, for whom an application is handed in, is not unambiguously given, this expert ability may be determined in the frame of a chargeable witness audit. The applicant has to bear the fees, which may be taken from the table of fees of VdS certification body. VdS certification body in this case reserves the right to pronounce a provisional approval as VdS IT consultant according to these guidelines.

4.2.2 Issue of the initial approval

The approval is issued for a period of 4 years.

If at the most 6 months after application all requested documentation is not handed in to VdS certification body, the procedure shall be stopped, liable to payment of all costs. The documentation received up to that date will be re-sent to the applicant resp. electronic documentation will be deleted. All expenses arisen for VdS certification body up to that date will be charged to the applicant. The procedure may be re-started only upon new application.

4.3 Prolongation of the approval

4.3.1 Requirements

A prolongation of approval may be applied for further four years. Decisive for the prolongation are the VdS guidelines being valid at time of application. The prolongation shall be handed in at VdS certification body at least 4 months before expiry of the approval by using the annexed form (Annex A).

The application shall be accompanied by

- the participation conformation of at least two relevant trainings within the approval validity
- if given, proofs on changes, which concern the base of the VdS approval
- proof of at least eight consultancy measures on base of VdS 3473 being performed within the validity of the approval.

Training measures are accepted which comprise in their totality at least 5 days (40 h). The following subjects may be relevant for trainings:

- IT governance and IT management
 - Security and data protection management
 - Risk and weak spots management
 - Business Continuity Management and Emergency Response
 - Judicially – relevant laws, guidelines and standards on IT security
- Hardware/Software
 - Penetration of IT systems
 - Applications and software development
 - Security of system software – Windows/Unix
 - Hacker attacks
 - Storage and backup management
 - Cryptografie
- Network and infrastructure
 - Network security and configuration
 - PKI
 - Configuration and securing firewalls
 - Routing/Switching.

In order to ensure the fulfilment of the assessment procedure requirements according to DIN EN ISO/IEC 17024, VdS reserves the right to perform additional assessments by specific methods, to ensure e. g. the procedure of a consultancy. If VdS deems necessary to participate at a consultancy date of a VdS-approved consultant for cyber security, the consultant will be informed in advance and is obliged to collect the agreement of the person who will be consulted, that VdS may participate.

4.3.2 Prolongation of the approval

The approval will be prolonged by further 4 years, if the application is completely filled-in and signed and handed in together with all required documentation in due time at VdS certification body and the assessment of the application as well as all documents lead to a positive result.

4.4 Expiry of the approval

The approval expires after the term of approval validity. If the application on prolongation is handed in later than 12 months after expiry of the approval, a completely new application with all documentation according to clause 4.1 shall be handed in.

5 Modification of the approval

VdS certification body shall be informed immediately on changes which concern the bases of the VdS-approval by using annex A (tick "modification application").

Changes requiring mandatory information are, inter alia.:

- Change of employment resp. to freelance work
- Change of company structure
- Change of company premises (move)

6 Revocation

Approvals may be revoked, thus becoming invalid. From the date of revocation any advertising with the VdS-approval is forbidden (see clause 7).

Revocations will occur, if

- the preconditions for the approval are no more given
- the guidelines, on which the approval procedure is based, are changed and the applicant has not implemented these changes within due time
- the approval or the VdS logo are used incorrectly (e. g. unfair advertising)
- the IT consultant did not fulfil his obligations according to these guidelines
- the IT consultant does not solve problems immediately in case of justified complaints
- the IT consultant does not fulfil his financial obligations vis-à-vis VdS Schadenverhütung GmbH
- the IT consultant turns to be unreliable in this or another business relationship (e. g. by fraud, compromising).

The IT consultant will be informed on the revocation of the approval by registered mail. An appeal against the revocation may be raised within 2 months. The revocation of the

approval may be withdrawn within 6 months, if the reasons having led to the revocation are removed.

There is no legitimate claim on the cancellation of the revocation. New approval may be applied for 12 months after a revocation at the earliest. When applying, a proof is required that the applicant fulfils all obligations and possible deficiencies from earlier procedures were remedied.

7 Advertising

VdS-approved IT consultants are admitted to advertise with the approval. However, it is not admitted to include the “VdS” mark or any modifications hereof as well as the approval as such in the applicants company name. Any advertising with the VdS approval as IT consultant shall reflect the content of the actual certificate correctly and shall not violate the competition regulations.

The regulations as indicated on the certificate shall be kept. Advertising shall be made only in connection with the approved person. Advertising with the VdS-approval shall not be made with services of the applicant, which are not covered by the scope of the approval. In case of doubt, any advertising with the VdS approval shall be agreed with VdS certification body.

The VdS approved IT consultant may point at his VdS approval with the following logo:



The logo may be enlarged or reduced in size maintaining the aspect ratio. The square frame of the VdS mark shall not fall below a minimum height of 13 mm. For color printing HKS 42 (or a similar color) may be used. The logo may be used on letter heads, advertising material or publishing items and advertising brochures of the applicant. Any modification of the logo is forbidden. In order to guarantee a correct presentation of the logo, it may be ordered free of charge at VdS certification body.

8 Fees

The approval procedure as well as the assessment activities, which are performed after approval, will be subject to fees and will be charged to the applicant resp. to the VdS approved IT-consultant. The fees are specified in the table of fees of VdS certification body. On demand the table of fees will be sent to the applicant free of charge, together with these guidelines. For the invoicing of services the fees will be referred to which are valid at the time of service delivery.

9 Miscellaneous

9.1 General Terms and Conditions

The General Terms and Conditions, VdS 3177 which is valid on the date of the finalization of the contract shall be applicable.

9.2 Supplements


Supplements to the agreement shall be in written form to become effective.

10 Changes to prior version

- Editorial changes
- Consideration of DIN EN ISO/IEC 17024 for prolongations of approvals.
- Adaption of the order form (Annex A) such that the premises of the approved consultant may differ from the premises of the applicant.

Annex A Application

Application for VdS approval as a consultant for cyber security according to VdS 3477
 by VdS Schadenverhütung GmbH
 Amsterdamer Str. 174, 50735 Köln



Consultant Approval no (if given): _____

Initial application (fill in the form completely)
 Prolongation application (fill in consultant approval no as well as clauses A, B, C and E)
 Modification application (fill in consultant approval no as well as clauses A, B, C and E)

A Applicant

A.1 Company name _____

A.2 Location (street, house no.) _____

A.3 Location (country, postal code, town) _____

A.4 E-mail address _____

A.5 Phone no _____

A.6 Contact person _____

A.7 Phone extension _____

A.8 Website _____

A.9 Commercial register _____

B Person, to whom the approval will apply
 Published listing acc. to B.1, B.2, B.3

B.1 Nomination of person _____

B.2 E-Mail address _____

B.3 Website _____

B.4 Employed (indication on employer see clause A)

B.5 Free-lancer (indication on company see clause A)

C Agreements

C.1 Issue of certificate
 Besides the German version an English certificate is requested

C.2 Information
 The applicant requests sending of relevant information (normally by e-mail);
 The applicant is aware that the commitment may be withdrawn at any time without indication of reasons.

D Requirements (see VdS 3477, clause 4.1.2)

D.1 Proofs **Copies are annexed to the application**

D.1.1 Completed academic study on informatics Evidence of formation
 Name of pdf-file: _____

D.1.2 Completed professional training in informatics (alternatively to D.1.1) Evidence of formation
 Name of pdf-file: _____

D.1.3 Clearance certificate without remarks (not elder than 6 months) Clearance certificate
 Name of pdf-file: _____

D.1.4 Professional experience Personal data sheet
 Name of pdf-file: _____

Job reference

Denomination of file(-s): _____

References

Denomination of file(-s): _____

Stand: 2015-11 (03)

D.2 Required confirmation of experience and knowledge**D.2.1 Professional experience**

- D.2.1.1 _____ Months (number) employed at _____ (Name or company);
Working as _____
- D.2.1.2 _____ Months (number) employed at _____ (Name or company);
Working as _____
- D.2.1.3 _____ Months (number) employed at _____ (Name or company);
Working as _____
- D.2.1.4 _____ Months (number) employed at _____ (Name or company);
Working as _____
- D.2.1.5 _____ Months (number) employed at _____ (Name or company);
Working as _____

D.2.2 Competence

- D.2.2.1 Knowledge of current attack methods and ability to analyse existing IT systems and structures on possible weak spots
- D.2.2.2 Knowledge on evaluation of risks for an enterprise (SMEs) arising from the IT landscape
- D.2.2.3 Knowledge on evaluation of security events
- D.2.2.4 Knowledge and experience for installation, configuration and administration of networked information and telecommunication, especially such for the protection against computerised attacks for evaluation of security events
- D.2.2.5 Knowledge on benefit, effectivity and weak spots of currently used IT products and systems and ability to evaluate such systems from the IT security perspective
- D.2.2.6 Knowledge on measures for the protection of IT systems (evaluation and control of robustness, data protection, secure and reliable operation of IT systems and networks, management of access and access rights; methods for fail safe and restart control)
- D.2.2.7 Knowledge on specific legal regulations
- D.2.2.8 Knowledge on VdS-guidelines and security guidelines for SME as far as these are relevant in connection with IT security
- D.2.2.9 Knowledge of the VdS guidelines for cyber security
 Proofs on formation and trainings are annexed to the application
Name of pdf-file(-s): _____

D.2.3 Availabilities and restrictions

- D.2.3.1 The availability of required standards and guidelines is confirmed
- D.2.3.2 For employed applicants: Declaration of employer that the person (B.1) may unrestrictedly practice the work as IT consultant is annexed to this application
Name of pdf-file: _____

E Declaration and agreement**The applicant declares:**

I/we accept the following rules

- VdS Guidelines for the approval of consultants for Cyber Security, VdS 3477
 - General Terms and Conditions of VdS Schadenverhütung GmbH, VdS 3177
 - Table of fees for the approval procedures according to VdS 3477 for IT consultants
- in the valid version as fix part of the contract.

The applicant accepts that,

VdS Schadenverhütung GmbH collects, processes and uses data on persons and other data in the frame of the certification process and maintains a list and informs third parties of the approval as consultant.

The applicant confirms,

that all indications made in the application (see especially clause D.2) are absolutely true.

Place, date: _____

Signature (as well as stamp) of applicant
(resp. a representative): _____

Stand: 2015-11 (03)