

Inhalt

1. Geltungsbereich 1

2. Anmeldung und Zulassung..... 1

3. Prüfung 2

4. Prüfer/Prüfungsaufsicht 2

5. Prüfungsbewertung 2

6. Prüfungswiederholung..... 3

7. Zertifizierung..... 3

8. Rezertifizierung..... 3

9. Persönliches Prüfzeichen-Signet 4

10. Überwachung 4

11. Gebühren..... 4

12. Revision 4

Anlage 1 – Prüfungsinhalte 5

1. Geltungsbereich

Diese Prüfungs- und Zertifizierungsordnung (PZO) gilt für das Verfahren zur Durchführung von Prüfungen und Zertifizierungen von Personen nach den Vorgaben von PersCert TÜV und in Anlehnung an die ISO/IEC 17024 für den folgenden Abschluss:

- TeleTrust Information Security Professional (T.I.S.P.) mit TÜV Rheinland geprüfter Qualifikation

Zusätzlich gelten die Allgemeinen Geschäftsbedingungen (AGB), die Allgemeinen Prüfungs- und Zertifizierungsbedingungen (APZB) von PersCert TÜV, die jederzeit zur Einsicht und zum Herunterladen auf der Webseite von PersCert TÜV (<https://go.tuv.com/perscert-dokumente>) verfügbar sind.

2. Anmeldung und Zulassung

Die Beauftragung der Prüfung und Zertifizierung durch den Antragsteller selbst erfolgt ausschließlich über den Bildungsanbieter isits AG International School of IT Security.

Zur Prüfung können nur Personen zugelassen werden, die die folgenden Zulassungsvoraussetzungen (ZV) erfüllen:

ZV1:	Nachweise, die geeignet sind, die theoretischen Vorkenntnisse des Kandidaten zu belegen. Als Nachweise werden anerkannt: a) Zeugnisse, Zertifikate oder Teilnahmebestätigungen über einschlägige Berufsausbildungen bzw. Bildungsmaßnahmen im Bereich der IT-Sicherheit oder b) Projektreferenzen mit der Darlegung der inhaltlichen Schwerpunkte aus den letzten drei Jahren. Diese Nachweise sind vor allem notwendig bei selbständiger Tätigkeit.
-------------	---

Prüfungs- und Zertifizierungsordnung TeleTrusT Information Security Professional (T.I.S.P.) mit TÜV Rheinland geprüfter Qualifikation	
DOC 327; Revision 3; gültig seit 24.02.2026	

ZV2:	Nachweis einer mindestens dreijährigen Berufstätigkeit im Bereich IT-Sicherheit mit aussagekräftiger Beschreibung der bearbeiteten Themenschwerpunkte (Arbeitszeugnisse, Zwischenzeugnisse oder ähnliche aussagekräftige Bestätigungen des Arbeitgebers)
ZV3:	Nachweis, dass der Kandidat an einer anerkannten T.I.S.P.-Schulung der isits AG International School of IT Security nach dem Curriculum des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) teilgenommen hat. Die Prüfungsleistung ist innerhalb von 12 Monaten ab dem Datum der erfolgreichen Absolvierung der T.I.S.P.-Schulung zu erbringen. Nach Überschreitung dieser Frist erlischt die Prüfungsberechtigung. In begründeten Härtefällen kann auf Antrag eine Ausnahme zugelassen werden; die Entscheidung erfolgt im Einzelfall.

Die Nachweispflicht liegt beim Antragsteller und erfolgt durch Vorlage von objektiven Nachweisen, die die Zulassungsvoraussetzungen belegen. PersCert TÜV ist berechtigt, weitere Nachweise anzufordern, sofern auf Basis der eingereichten Nachweise keine Zulassungsentscheidung getroffen werden kann. Abweichende Nachweise können nur in Ausnahmen anerkannt werden und sofern die Gleichwertigkeit durch PersCert TÜV festgestellt wurde. PersCert TÜV prüft die Anmeldung und entscheidet über die Zulassung zur Prüfung nach eigenem Ermessen. Anspruch auf die Zulassung zur Prüfung besteht nicht. PersCert TÜV überträgt die Prüfung der Zulassungsvoraussetzungen an isits AG International School of IT Security.

3. Prüfung

Die Prüfungsaufgaben werden von PersCert TÜV aus dem zum Zeitpunkt der Prüfung gültigen Aufgabenpool ausgewählt (Prüfungsinhalte siehe **Anlage 1**).

Die Prüfung zum Nachweis der im Zertifizierungsprogramm definierten Kompetenzen besteht aus einer schriftlichen Prüfung.

Die Prüfung beinhaltet insgesamt 180 Prüfungsaufgaben (Multiple-Choice-Fragen).

Die Dauer der gesamten Prüfung beträgt 180 Minuten.

Die maximal zu erreichende Punktzahl beträgt 180.

In der Prüfung zugelassene Hilfsmittel:

- keine

Die Prüfungssprache ist Deutsch.

Die Verantwortung für die Organisation und Durchführung der Prüfung liegt bei PersCert TÜV. PersCert TÜV kann die Organisation an Dritte delegieren.

4. Prüfer/Prüfungsaufsicht

Die Prüfung wird von einem oder mehreren von PersCert TÜV zugelassenen und für die Durchführung der Prüfung beauftragten Prüfern/Prüfungsaufsichten durchgeführt.

5. Prüfungsbewertung

Die Bewertung der Prüfung erfolgt nach einem Punktesystem. Jede Prüfungsaufgabe ist mit einer max. erreichbaren Punktzahl ausgewiesen.

Die maximal zu erreichende Punktzahl ist unter Punkt 3 geregelt.

Eine Multiple-Choice-Frage (MC) besteht aus mehreren Antwortalternativen, wobei eine oder mehrere Antworten richtig sein können. Die Anzahl der richtigen Antworten ist jeweils in Klammern hinter der Frage angegeben. Jede vollständig richtig beantwortete MC-Frage wird mit einem Punkt bewertet. Jede falsch beantwortete, nur teilweise richtig beantwortete oder nicht beantwortete MC-Frage wird mit null Punkten bewertet.

Die Prüfung gilt als bestanden, wenn mindestens 126 der maximal erreichbaren Punkte (70 %) erreicht wurden.

Prüfungs- und Zertifizierungsordnung TeleTrusT Information Security Professional (T.I.S.P.) mit TÜV Rheinland geprüfter Qualifikation	
DOC 327; Revision 3; gültig seit 24.02.2026	

Der Kandidat wird über das Ergebnis der Prüfung in Textform benachrichtigt.

6. Prüfungswiederholung

Eine nicht bestandene Prüfung kann einmal wiederholt werden.

Die Wiederholungsprüfung kann erst nach der schriftlichen Benachrichtigung des Kandidaten über die Zertifizierungsentscheidung und ausschließlich über den Bildungsanbieter isits AG International School of IT Security beauftragt werden. Weitere Informationen sind der schriftlichen Benachrichtigung zu entnehmen. Die Wiederholungsprüfung kann bei der nächstmöglichen Gelegenheit, muss jedoch spätestens innerhalb eines Jahres nach dem Datum der schriftlichen Benachrichtigung erfolgen. Der Termin der Wiederholungsprüfung ist mit isits AG International School of IT Security abzustimmen.

Im Falle einer nicht bestandenen Wiederholungsprüfung gilt das Verfahren als abgeschlossen. Für eine erneute Prüfung gelten die Bedingungen der Erstzertifizierung.

7. Zertifizierung

Die Zertifizierungsentscheidung trifft PersCert TÜV. Der Kandidat erhält eine Benachrichtigung über die getroffene Zertifizierungsentscheidung sowie bei positiver Zertifizierungsentscheidung ein PersCert TÜV Zertifikat. Bei einer negativen Zertifizierungsentscheidung wird kein Zertifikat erteilt.

Voraussetzung für die Erteilung eines PersCert TÜV Zertifikates ist die Erfüllung aller Anforderungen des Zertifizierungsprogramms durch den Antragsteller.

Die Gültigkeit des Zertifikates beträgt max. 3 Jahre, ausgehend von dem Datum der Zertifizierungsentscheidung. Für die Verlängerung der Zertifizierung ist eine Rezertifizierung bei PersCert TÜV zu beantragen (gemäß Punkt 8 dieser PZO).

Das Zertifikat bleibt Eigentum von PersCert TÜV. Die Nutzungsbedingungen für das Zertifikat sind in den APZB geregelt.

8. Rezertifizierung

Die zertifizierte Person hat die Möglichkeit frühestens 3 Monate vor und maximal 12 Monate nach dem Ablauf der Gültigkeit der bisherigen Zertifizierung eine Rezertifizierung (Verlängerung der Zertifizierung) bei PersCert TÜV zu beauftragen.

Der Antrag wird erst bearbeitet, wenn die für die Rezertifizierung notwendigen Unterlagen vollständig eingereicht wurden.

Die Rezertifizierungsprüfung besteht aus einer einfachen Dokumentenprüfung. Die Zertifizierung kann nur dann verlängert werden, wenn die folgenden Rezertifizierungsvoraussetzungen (RV) erfüllt sind:

RV1:	Tätigkeitsbeschreibung des Arbeitgebers oder bei Selbstständigen eine aussagekräftige Projektliste. Dabei ist der Umfang der praktischen Tätigkeit zu quantifizieren (in % des persönlichen Arbeitsvolumens).
RV2:	Besuch mindestens eines T.I.S.P. Community Meetings innerhalb der letzten drei Jahre
RV3:	Nachweise zu Fortbildungen/ Weiterentwicklung aus dem Bereich IT-Sicherheit/ Informationssicherheit im Volumen von durchschnittlich 20 Stunden pro Jahr. Anerkannt werden: • Teilnahme an geeigneten betrieblichen und/oder externen Weiterbildungsangeboten, Seminaren, Workshops oder Tagungen/Konferenzen (8h pro Tag); • Teilnahme an weiteren T.I.S.P. Community Meetings (8h pro Meeting);

Prüfungs- und Zertifizierungsordnung TeleTrusT Information Security Professional (T.I.S.P.) mit TÜV Rheinland geprüfter Qualifikation	 TÜVRheinland®
DOC 327; Revision 3; gültig seit 24.02.2026	

	• Anerkannte Publikationen über eigene Forschungs- und Entwicklungstätigkeiten zu aktuellen Themen der Informationssicherheit (max. 20 h); • Nachweis über die persönliche Konzeption von Weiterbildungsangeboten zu aktuellen Themen der Informationssicherheit, die geeignet sind, das persönliche Wissen weiterzuentwickeln. (max. 20 h); • Dokumentation von Projekten zu aktuellen Themen der Informationssicherheit, die geeignet sind, das persönliche Wissen weiterzuentwickeln (persönliche Beteiligung am Arbeitsvolumens des Projektes von mind. 50% (max. 20h).
--	---

Die Nachweispflicht liegt beim Antragsteller und erfolgt durch Vorlage von objektiven Nachweisen, die die Rezertifizierungs Voraussetzungen belegen. PersCert TÜV ist berechtigt, weitere Nachweise anzufordern, sofern auf Basis der eingereichten Nachweise keine Rezertifizierungsentscheidung getroffen werden kann.

Die endgültige Entscheidung über die Rezertifizierung trifft PersCert TÜV nach eigenem Ermessen. Anspruch auf die Rezertifizierung besteht nicht.

Wird die Rezertifizierung rechtzeitig durchgeführt, schließt die erteilte Zertifizierung an das Ablaufdatum der bisherigen Zertifizierung an. Beantragt die zertifizierte Person die Rezertifizierung erst nach dem Ablauf der aktuell gültigen Zertifizierung bzw. zu kurzfristig, um rechtzeitig vor dem Ablauf der aktuell gültigen Zertifizierung die Rezertifizierung durchzuführen, wird die neue Zertifizierung verkürzt erteilt. Mit der Erteilung des neuen Zertifikates verliert das bisherige Zertifikat seine Gültigkeit.

Für die Rezertifizierung gelten die Bestimmungen gemäß Punkt 7 dieser PZO ebenso.

Nach Ablauf der Rezertifizierungsfrist gelten für die Erteilung einer neuen Zertifizierung die Bedingungen der Erstzertifizierung.

9. Persönliches Prüfzeichen-Signet

Der zertifizierten Person wird die Möglichkeit eingeräumt, ein persönliches Prüfzeichen-Signet mit persönlicher ID zu werblichen Zwecken zu erwerben. Prüfzeichen-Signets sind separat bei PersCert TÜV über die Webseite (<https://go.tuv.com/signetbestellung>) zu beantragen. Die Gültigkeit des persönlichen Prüfzeichen-Signets orientiert sich an der Gültigkeit der erteilten Zertifizierung. In übrigen Fällen beträgt die Gültigkeit 2 Jahre.

Die Nutzungsbedingungen für das Prüfzeichen-Signet sind in den APZB geregelt.

10. Überwachung

Die Zertifizierung unterliegt der Überwachung durch PersCert TÜV. Die allgemeinen Überwachungstätigkeiten sind in den APZB geregelt.

11. Gebühren

Prüfungs- und Zertifizierungsverfahren sind gebührenpflichtig. Die Höhe der Gebühren richtet sich nach der jeweils zum Zeitpunkt der Beauftragung gültigen Gebührenliste, sofern nichts anderes schriftlich vereinbart wurde.

12. Revision

PersCert TÜV ist berechtigt das Zertifizierungsprogramm zu ändern oder einzustellen. Die Änderungen werden im Internet veröffentlicht. Über die Änderungen an dem Zertifizierungsprogramm informiert sich der Kandidat bzw. die zertifizierte Person eigenständig. Es gilt die zum Zeitpunkt der Prüfung gültige PZO.

Prüfungs- und Zertifizierungsordnung

TeleTrusT Information Security Professional (T.I.S.P.) mit TÜV Rheinland geprüfter
Qualifikation



DOC 327; Revision 3; gültig seit 24.02.2026

Anlage 1 – Prüfungsinhalte

- Allgemeine Grundlagen
 - Netzwerksicherheit
 - Firewalls
 - Intrusion Detection
 - Hackermethoden, wichtige Angriffsszenarien
 - VPN
 - Anwendungssicherheit
 - Sicherheit in mobilen Netzen
- Kryptographie
 - Grundlagen
 - Symmetrische / asymmetrische Verschlüsselung
 - PKI
- Sicherheitsmanagement
 - Information Security Management
 - Authentisierung
 - Autorisierung
 - Berechtigungsmanagement
 - BCM
 - Notfallmanagement
 - Security Awareness
 - Physische Sicherheit
 - Betriebswirtschaftliche Aspekte der IT-Sicherheit
- Rechtliche Grundlagen
- Systemsicherheit
 - Computer-Viren und Content Security
 - Betriebssystemsicherheit (Windows, Unix / Linux)
- Cloud Security
- Virtualisierung