

Zertifizierungsprogramm für IS-Auditoren

CIS - Certification & Information
Security Services GmbH

Headquarters

1010 Wien, Saltzorgasse 2/6/14

Tel.: +43 1 532 98 90
Fax: +43 1 532 98 90 89
office@cis-cert.com
www.cis-cert.com

© CIS 20.10.2021: Nachdruck und Vervielfältigung, auch auszugsweise, nur mit schriftlicher Genehmigung der CIS.

Inhalt

1	Einleitung	3
2	Anwendungsbereich	3
3	Kompetenzprofile und Qualifizierungsstufen	3
4	Normative Verweisungen	4
5	Begriffe	4
6	Prozess der Erstzertifizierung	4
6.1	Zugangsvoraussetzungen zum Lehrgang und Zertifizierungsprüfung	4
6.2	Antrag auf Erstzertifizierung	4
6.3	Zulassungsprüfung (Technische Einstiegsprüfung)	5
6.4	Lehrgang	5
6.5	Zertifizierungsprüfung	5
6.6	Zertifikat	7
6.7	Überwachung	7
7	Prozess der Re-Zertifizierung	8
7.1	Zugangsvoraussetzungen zur Re-Zertifizierungsprüfung	8
7.2	Antrag auf Re-Zertifizierung	9
7.3	Re-Zertifizierungsprüfung	9
8	Verwaltung der Prüfungsfragen	9
8.1	Speicherort	9
8.2	Zugriffsschutz	10
9	Archivierung der Prüfungen	10
9.1	Speicherort	10
9.2	Zugriffsschutz	10

Prolog

© 20.10.2021 CIS: Alle Inhalte, insbesondere Texte, Fotografien und Grafiken sind urheberrechtlich geschützt. Alle Rechte, einschließlich der Vervielfältigung, Veröffentlichung, Bearbeitung und Übersetzung, bleiben vorbehalten, CIS – Certification & Information Security Services GmbH (CIS).

Alle geschlechtsspezifischen Ausdrücke gelten immer für beide Geschlechter gleichermaßen. Aus Gründen der Lesbarkeit wird auf die doppelte Ansprache verzichtet.

1 Einleitung

Ziel dieses Zertifizierungsprogramms ist es, die Anforderungen an das Verfahren der Qualifizierung von Auditoren, die im Bereich der Informationssicherheit Audits durchführen, in Form eines Zertifizierungsprozesses gemäß den Vorgaben der ISO 17024 zu regeln.

2 Anwendungsbereich

Dieses Zertifizierungsprogramm legt ein System für die Qualifizierung und Zertifizierung von Personen fest, das Audits von

- Information Security Management Systems (ISMS) gemäß ISO 27001

durchführt.

Dieses Zertifizierungsprogramm bezieht sich auf

- IS-Auditoren (m/w).

3 Kompetenzprofile und Qualifizierungsstufen

Eine Person, die als IS-Auditor zertifiziert ist, hat ihre Fähigkeit nachgewiesen, Managementsysteme von Organisationen auf Basis der jeweils zur Anwendung gelangenden, obig angeführten internationalen Norm

- zu prüfen und zu bewerten,
- Stärken und Verbesserungspotenziale zu erkennen,
- die involvierten Mitarbeiter zu motivieren, das System entsprechend weiter zu entwickeln.

4 Normative Verweisungen

Die folgenden zitierten Dokumente sind für Anwendung dieses Zertifizierungsprogramms erforderlich:

- EN ISO 9001:2015, Qualitätsmanagementsysteme – Anforderungen
- EN ISO 19011:2018, Leitfaden zur Auditierung von Managementsystemen
- EN ISO/IEC 17024:2012, Konformitätsbewertung – Allgemeine Anforderungen an Stellen, die Personen zertifizieren
- ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems - Requirements

5 Begriffe

Für die Anwendung dieses Dokumentes gelten die Begriffe nach ISO/IEC Guide 2 sowie die Begriffe der EN ISO/IEC 17024:2012.

6 Prozess der Erstzertifizierung

6.1 ZUGANGSVORAUSSETZUNGEN ZUM LEHRGANG UND ZERTIFIZIERUNGSPRÜFUNG

6.1.1 Anforderungen an die Ausbildung

Für die Zertifizierung zum IS-Auditor sind sowohl Berufserfahrung als auch Auditerfahrung in der Berufsausübung erforderlich.

	IS-Auditor
Grundausbildung	CIS IS-Manager oder gleichwertige Ausbildung
Weiterbildung	Besuch des CIS-Refreshing Lehrgangs mindestens 1 x innerhalb von 3 Jahren oder gleichwertige Ausbildung bzw. Inhalte oder Wissen des Lehrgangs
Berufserfahrung	4 jährige Berufspraxis, davon mindestens 2 Jahre im Gültigkeitsbereich Informationssicherheit
Berufsausübung	Praxisnachweise, mindestens 4 vollständige Audits mit insgesamt mindestens 20 Audittagen inkl. Vor- und Nachbearbeitung und/oder Projekte im Informationssicherheitsumfeld nachzuweisen

6.2 ANTRAG AUF ERSTZERTIFIZIERUNG

Um zur Zulassungsprüfung zugelassen zu werden, muss der Kandidat einen schriftlich, formellen Antrag mittels Anmeldeformular stellen. Der Antrag, sowie alle erforderlichen Unterlagen, die dazu geeignet sind die Anforderungen des Punktes 6.1.1 nachzuweisen, müssen spätestens 2 Wochen vor dem Prüfungstermin bei der CIS einlangen. Dem Kandidaten wird mitgeteilt, ob er zum jeweiligen Lehrgang und zur Zertifizierungsprüfung zugelassen ist und gegebenenfalls der Ort mitgeteilt.

6.3 ZULASSUNGSPRÜFUNG (TECHNISCHE EINSTIEGSPRÜFUNG)

6.3.1 Art der Zulassungsprüfung

Die Zertifizierungsprüfung wird in Form eines Multiple Choice Test (MC-Test) durchgeführt.

6.3.2 Umfang

Die Multiple-Choice-Zertifizierungsprüfung besteht aus 100 Fragen, wobei es für jede Frage 4 Antwortmöglichkeiten gibt, von denen eine richtig ist.

6.3.3 Prüfungsdauer

Für die Beantwortung der Fragen steht ein Zeitraum von 120 Minuten zur Verfügung.

6.3.4 Bewertung

Die Multiple-Choice-Zertifizierungsprüfung gilt als bestanden, wenn mindestens 50% der Fragen richtig beantwortet wurden.

Im Falle der bestandenen Zulassungsprüfung ist der Kandidat berechtigt am jeweiligen Lehrgang und der Zertifizierungsprüfung teilzunehmen.

6.3.5 Ausschluss von der Zulassungsprüfung

Bezüglich Ausschluss und Wiederholung der Zulassungsprüfung gelten die Bestimmungen der Punkte 6.5.6 und 6.5.7 sinngemäß.

6.4 LEHRGANG

6.4.1 Die Inhalte der Lehrgangreihe

- Zertifizierungsverfahren
- Audit-Planung, -Durchführung, -Bewertung, -Dokumentation und -Folgebemaßnahmen
- rechtliche und normative Anforderungen
- Grundlagen des Informationssicherheits-/Servicemanagements
- ISMS Modelle
- ISMS Instrumente.

6.4.2 Umfang

Der Umfang des Lehrganges für IS-Auditoren umfasst 3 Tage zu jeweils acht Stunden.

6.5 ZERTIFIZIERUNGSPRÜFUNG

6.5.1 Art der Zertifizierungsprüfung

Die Zertifizierungsprüfung wird in Form eines Multiple Choice Test (MC-Test) durchgeführt.

6.5.2 Die Zertifizierungsprüfungsfragen

Die Zertifizierungsprüfungsfragen beziehen sich auf nachfolgende Themen:

- Die gesamte Praxis zur Durchführung interner und externer Audits
- Die verschiedenen Auditarten für unterschiedliche Typen von Organisationen
- Die verschiedenen Arbeitsschritte: Vorbereitung des Audits, Anwendung der Auditfragen, Vorab-Prüfung, Vor-Ort-Audit, Auditanalyse (mit Methoden)
- Erstellung des Auditberichts.
- Soziale Kompetenz
- Die Fähigkeit vernetzt zu denken und abteilungsübergreifende Systemzusammenhänge zu erkennen
- Einblicke in die Grundregeln der Kommunikation

Anzahl der Zertifizierungsprüfungsfragen: Modul Psychologische Grundlagen für IS-Auditoren 8 Fragen, Modul Audittechniken 12 Fragen.

6.5.3 Umfang

Die Multiple-Choice-Zertifizierungsprüfung besteht aus 20 Fragen, wobei es für jede Frage 4 Antwortmöglichkeiten gibt, von denen eine richtig ist.

6.5.4 Prüfungsdauer

Für die Beantwortung der Fragen steht ein Zeitraum von 60 Minuten zur Verfügung stehen.

6.5.5 Bewertung

Die Multiple-Choice-Zertifizierungsprüfung gilt als bestanden, wenn mindestens 50% der Fragen pro Modul richtig beantwortet wurden.

6.5.6 Ausschluss von der Zertifizierungsprüfung

- I. Die Verwendung von Hilfsmittel zur Beantwortung der Fragen, wie z.B. Mitschriften, Skripten und dergleichen, ist während der Zertifizierungsprüfung untersagt.
- II. Macht sich der Kandidat einer Täuschungshandlung bzw. der Verwendung unerlaubter Hilfsmittel schuldig, so wird dies auf den Prüfungsunterlagen des Kandidaten vermerkt. Die Zertifizierungsprüfung wird abgebrochen und als negativ gewertet.
- III. Kandidaten, die eine Störung des Prüfungsablaufes verursachen, werden von der Zertifizierungsprüfung ausgeschlossen. Die Zertifizierungsprüfung ist abzubrechen und gilt als „nicht durchgeführt“.

6.5.7 Wiederholung der Zertifizierungsprüfung

- I. Wenn das Ergebnis der Zertifizierungsprüfung als „nicht bestanden“ (negativ) beurteilt wurde, kann im Zuge der nächsten regulären Zertifizierungsprüfung die Prüfung wiederholt werden.
- II. Fällt das Ergebnis der Wiederholung der Zertifizierungsprüfung wieder negativ aus, hat der Zertifizierungswerber nur noch einmal die Möglichkeit die Zertifizierungsprüfung zu

wiederholen. Fällt das Ergebnis wieder negativ aus, hat der Zertifizierungswerber vor einem neuerlichen Antritt den Lehrgang zu wiederholen.

- III. Bei einem nochmaligen negativen Ergebnis der Zertifizierungsprüfung ist kein weiterer Antritt mehr möglich.

6.6 ZERTIFIKAT

6.6.1 Gültigkeitsdauer

Im Falle einer positiven Zertifizierungsentscheidung wird dem Kandidaten ein Zertifikat mit 36-monatiger Gültigkeitsdauer ausgestellt.

6.6.2 Veröffentlichung

Mit der Zertifizierung willigt der Zertifikatsinhaber ein, dass sein Name, die zertifizierte Kompetenz sowie das Ausstellungs- und Ablaufdatum der Zertifizierung in einem über Internet verfügbaren, öffentlich zugänglichem Verzeichnis der zertifizierten Personen aufgenommen werden kann und der Status der Zertifizierung (gültig, nicht verlängert, aberkannt) kenntlich gemacht werden kann.

6.7 ÜBERWACHUNG

Während der Gültigkeitsdauer der Zertifizierung ist eine Überwachung durchzuführen.

6.7.1 Passive Überwachungsmaßnahmen (ständig)

- I. Der Zertifikatsinhaber ist verpflichtet
 - a. sämtliche Änderungen der persönlichen und beruflichen Daten, (die in Zusammenhang mit den Zugangsvoraussetzungen zur Zertifizierung gemäß 6.1.1 stehen,)
 - b. sämtliche Beschwerden in Zusammenhang mit der Leistungserbringung der Zertifizierungsstelle unverzüglich und schriftlich mitzuteilen.
- II. Auf Grund von Mitteilungen gemäß Absatz I oder von Beschwerden Dritter, die direkt an die Zertifizierungsstelle gerichtet werden, beurteilt die Zertifizierungsstelle die Sachlage und leitet gegebenenfalls geeignete Maßnahmen ein.

6.7.2 Aktive Überwachungsmaßnahmen

- I. Der Zertifikatsinhaber ist verpflichtet, der Zertifizierungsstelle auf deren Aufforderung
 - a. alle durchgeführten Audits (inkl. interne Audits) mitzuteilen.

6.7.3 Ergebnis der Überwachungsmaßnahmen

- I. Auf Grund der durchgeführten Überwachungen hat die Zertifizierungsstelle im Einzelfall zu entscheiden, ob das Zertifikat eines IS-Auditors aufrecht bleiben kann.
- II. Wird im Zuge der Überwachung festgestellt, dass
 - a. eine Beschwerde Dritter an die Zertifizierungsstelle vorgebracht wurde, die sich nach Evaluierung durch die Zertifizierungsstelle als gerechtfertigt erweist, oder

- b. keine Audits durchgeführt wurden, oder
- c. die Auditleistung auf Basis der vorgelegten Berichte zumindest zweimal als nicht zufriedenstellend bewertet wurde,

wird dem jeweiligen IS-Auditor das Zertifikat aberkannt.

- III. Die Zertifizierungsstelle kennzeichnet in diesem Fall im Verzeichnis der zertifizierten IS-Auditor das Zertifikat mit „aberkannt“ und setzt den betreffenden IS-Auditor von der Aberkennung der Zertifizierung schriftlich in Kenntnis.

7 Prozess der Re-Zertifizierung

7.1 ZUGANGSVORAUSSETZUNGEN ZUR RE-ZERTIFIZIERUNGSPRÜFUNG

7.1.1 Gültiges Zertifikat

IS-Auditoren die sich der Re-Zertifizierungsprüfung unterziehen wollen, müssen über ein gültiges (maximal 6 Monate nach Ablauf der Gültigkeitsdauer) Zertifikat verfügen.

7.1.2 Auffrischungsschulung

Die Voraussetzung zur Teilnahme an der Re-Zertifizierungsprüfung ist die Teilnahme an einer Schulung, die von der Zertifizierungsstelle durchgeführt wird und die nicht länger als ein Jahr zurückliegen darf oder eine gleichwertige Ausbildung bzw. Inhalte oder Wissen des Lehrgangs.

7.1.3 Inhalte und Themen

Die Inhalte der Auffrischung und sie Re-Zertifizierungsprüfungsfragen beziehen sich auf nachfolgende Themen:

- Weiterentwicklung von ISMS nach ISO 27001 / ISO 27002
- Normforderungen und ihre effektive Umsetzung in der Praxis
- Neue Subnormen, neue Norminhalte im Rahmen der Normenreihe ISO 27000
- Neue Methoden und Erkenntnisse aus der internationalen Auditoren-Community
- Interne und externe Audits: Synergien und Systemoptimierung durch strukturiertes Vorgehen
- Strategie- und Organisationsentwicklung
- Fragestellungen zur betrieblichen Umsetzung, die Teilnehmer selbst einbringen

7.1.4 Umfang

Der Mindestumfang für die Auffrischungsschulung von Auditoren muss zumindest einen Tag zu acht Stunden betragen.

7.2 ANTRAG AUF RE-ZERTIFIZIERUNG

7.2.1 Schriftlicher Antrag

Der zertifizierte IS-Auditor (Zertifikatsinhaber) hat einen schriftlich, formellen Antrag auf Re-Zertifizierung vor Ablauf der Gültigkeitsdauer des Zertifikates zu stellen.

7.2.2 Annahme des Antrags

Der Antrag auf Re-Zertifizierung wird von der Zertifizierungsstelle angenommen, wenn

- a. die Zugangsvoraussetzungen zur Zertifizierung gemäß 6.1.1 weiterhin gegeben sind,
- b. bezüglich der abgelaufenen Periode Nachweise über die Durchführung von mindestens 3 vollständigen Audits beigebracht werden,
- c. die erforderliche Schulung nachgewiesen wurde, bzw. die Möglichkeit besteht, diese innerhalb einer Frist von sechs Monaten nach Ablauf der Gültigkeitsdauer des bestehenden Zertifikates nachzuweisen oder eine gleichwertige Ausbildung bzgl. Inhalte oder Wissen des Lehrgangs und
- d. die Re-Zertifizierungsprüfung innerhalb einer Frist von sechs Monaten nach Ablauf der Gültigkeitsdauer des bestehenden Zertifikates absolviert werden kann.

7.2.3 Ablehnung des Antrags

Werden die Anforderungen der Punkte 7.2.1 und 7.2.2 nicht erfüllt, wird das jeweilige Zertifikat im Verzeichnis der zertifizierten Personen als ungültig gekennzeichnet und die betreffende Person über diesen Umstand schriftlich informiert. Im Falle des weiterbestehenden Interesses der betreffenden Person ist das Verfahren der Erstzertifizierung durchzuführen.

7.3 RE-ZERTIFIZIERUNGSPRÜFUNG

7.3.1 Umfang

Im Falle einer Re-Zertifizierung besteht die Re-Zertifizierungsprüfung aus einem Multiple-Choice-Test, der aus 10 Fragen besteht, wobei es für jede Frage 4 Antwortmöglichkeiten gibt, von denen eine richtig ist.

8 Verwaltung der Prüfungsfragen

Die folgenden Punkte gelten in gleichem Maße sowohl für die Zulassungsprüfung (Techn. Einstiegsprüfung) als auch für die Zertifizierungsprüfung.

8.1 SPEICHERORT

Ausgedruckte Fragebögen werden im CIS-Tresor abgelegt

Elektronischer Fragenkatalog wird auf dem Serverlaufwerk P:\CIS abgelegt.

8.2 ZUGRIFFSSCHUTZ

Für den CIS-Tresor haben nur definierte CIS-Mitarbeiter eine Berechtigung.

Der elektronische Fragenkatalog wird durch das bestehende Windows Berechtigungskonzept geschützt. Es haben nur berechtigte Mitarbeiter der CIS Zugriff.

9 Archivierung der Prüfungen

Es werden alle Prüfungen mindestens 10 Jahre aufbewahrt.

9.1 SPEICHERORT

Es werden alle Prüfungen in Papierform im CIS-SK-Büro archiviert.

9.2 ZUGRIFFSSCHUTZ

Durch die installierte Alarmanlage beim Bürohaupteingang und dadurch, dass niemand (z.B. Reinigungspersonal, Kursteilnehmer, Trainer, Auditoren) unbeaufsichtigt sich in den CIS-Büorräumlichkeiten aufhalten darf.

Diese Regelung ist nicht auf die CIS-Geschäftsführung anzuwenden.



CIS - Certification & Information
Security Services GmbH

Headquarters

1010 Wien, Saltzorgasse 2/6/14

Tel.: +43 1 532 98 90

Fax: +43 1 532 98 90 89

office@cis-cert.com

www.cis-cert.com

© CIS 20.08.2020:
Nachdruck und Vervielfältigung,
auch auszugsweise, nur mit schriftlicher
Genehmigung der CIS.