Zertifizierungsprogramm für IS-Manager

CIS - Certification & Information
Security Services GmbH

Headquarters

1010 Wien, Salztorgasse 2/6/14

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

Inhalt

Prolog

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 Managern, die im Bereich der Informationssicherheit Managementsysteme aufbauen und betreiben, in Form eines Zertifizierungsprozesses gemäß den Vorgaben der EN ISO/IEC 17024 zu regeln.

2 Anwendungsbereich

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

- Information Security Management Systems (ISMS) gemäß ISO 27001

aufbauen und betreiben.

Dieses Zertifizierungsprogramm bezieht sich auf

- IS-Manager (m/w).

3 Kompetenzprofile und Qualifizierungsstufen

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

- 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

6.1.1 Anforderungen an die Ausbildung

Keine speziellen Anforderungen erforderlich.

	IS-Manager
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

6.2 ANTRAG AUF ERSTZERTIFIZIERUNG

Um zur Zertifizierungsprüfung zugelassen zu werden, muss der Kandidat einen schriftlich, formellen Antrag mittels Anmeldeformular stellen. Der Antrag muss spätestens 2 Wochen vor dem Prüfungstermin bei der CIS einlangen. Dem Kandidaten wird mitgeteilt, ob er zum jeweiligen Lehrgang und Zertifizierungsprüfung zugelassen ist und gegebenenfalls der Ort mitgeteilt.

6.3 LEHRGANG

6.3.1 Die Inhalte der Lehrgangsreihe

- Normforderungen der ISO 27001 & ISO 27002 und ihre effektive Umsetzung in der Praxis
- Rechtliche Grundlagen für IS-Manager
- Psychologische Grundlagen für IS-Manager

6.3.2 Umfang

Der Umfang des Lehrganges für IS-Manager umfasst 4 Tage zu jeweils acht Stunden.

6.4 ZERTIFIZIERUNGSPRÜFUNG

6.4.1 Art der Zertifizierungsprüfung

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

6.4.2 Die Zertifizierungsprüfungsfragen

Die Zertifizierungsprüfungsfragen beziehen sich auf nachfolgende Themen:

- Normforderungen und ihre effektive Umsetzung in der Praxis
- Psychologische Grundlagen für IS-Manager
- Rechtliche Grundlagen für IS-Manager

Anzahl der Zertifizierungsprüfungsfragen: Norm-Teil 16 Fragen, Psychologische Grundlagen für IS-Manager 7 Fragen, Rechtsgrundlagen 7 Fragen.

6.4.3 Umfang

Die Multiple-Choice-Zertifizierungsprüfung besteht aus 30 Fragen, wobei es für jede Frage 4 Antwortmöglichkeiten gibt, von denen eine richtig ist.

6.4.4 Prüfungsdauer

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

6.4.5 Bewertung

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

6.4.6 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 Prüfung ist abzubrechen und gilt als „nicht durchgeführt".

6.4.7 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.

6.5 ZERTIFIKAT

6.5.1 Gültigkeitsdauer

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

6.5.2 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.

6.6 ÜBERWACHUNG

Während der Gültigkeitsdauer der Zertifizierung ist eine Überwachung durchzuführen.

6.6.1 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.

6.6.2 Ergebnis der Überwachungsmaßnahmen

I. Auf Grund der durchgeführten Überwachungen hat die Zertifizierungsstelle im Einzelfall zu entscheiden, ob das Zertifikat eines IS-Managers 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,

   wird dem jeweiligen IS-Manager das Zertifikat aberkannt.

III. Die Zertifizierungsstelle kennzeichnet in diesem Fall im Verzeichnis der zertifizierten IS-Manager das Zertifikat mit „aberkannt" und setzt den betreffenden IS-Manager 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-Manager 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 IS-Manager-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 IS-Managern muss zumindest einen Tag zu acht Stunden betragen.

7.2 ANTRAG AUF RE-ZERTIFIZIERUNG

7.2.1 Schriftlicher Antrag

Der zertifizierte IS-Manager (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 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

b. 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

8.1 SPEICHERORT

Ausgedruckte Fragebögen werden im CIS-Tresor abgelegt

Elektronischer Fragenkatalog wir 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-Büroräumlichkeiten aufhalten darf.

Diese Regelung ist nicht auf die CIS-Geschäftsführung anzuwenden.

CIS - Certification & Information
Security Services GmbH

Headquarters

1010 Wien, Salztorgasse 2/6/14

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