Personnel Certification

Swiss Association for Quality

SAQ Swiss Association for Quality
Personnel Certification

Zertifizierungen integrale Sicherheit

Zertifizierungsprogramm Manager:in ITSCM und Informationssicherheit Professional SAQ

Version V1.0 anerkannt 2024 09 24

Personnel Certification
SAQ Swiss Association for Quality
Ramuzstrasse 15
CH-30127 Bern

T +41 (0)31 330 99 00
pc@saq.ch
www.personnelcertification.ch

Personnel Certification

Swiss Association for Quality

Inhaltsverzeichnis

Zur besseren Lesbarkeit wird im vorliegenden Dokument ausschliesslich die männliche Schreibform verwendet. Wir weisen darauf hin, dass die ausschliessliche Verwendung der männlichen Form geschlechtsunabhängig verstanden werden soll.

Personnel Certification

Swiss Association for Quality

1 Anwendungsbereich

Die Zertifizierung erfolgt aufgrund der Vorgaben der Normativen Grundlage. Das Zertifizierungsprogramm beschreibt die erforderlichen Lerninhalte, definiert die Anforderungen an die Prüfungen sowie die zugelassenen Re-Zertifizierungsmassnahmen.

2 Zulassung zum Qualifikationsverfahren / Anforderungen

Für die Zulassung zu dieser Prüfung ist ein Grundverständnis in Business Continuity Management BCM, Informationssicherheit und Anwendung von Datenschutz im Alltag, IT-Service Continuity Management ITSCM nötig, das in verschiedener Form angeeignet werden kann (Ausbildung, Praxiserfahrung).

Mögliche Kandidaten kommen aus den unterschiedlichsten Branchen und sind beschäftigen sich mit Themen wie (Aufzählung ist nicht abschliessend)

- Notfall- und Krisenmanagement
- Business Continuity Management
- Compliance- und / oder Risk Management
- Supply Chain Management
- Physische Sicherheit von Arealen, Gebäuden, Räumen
- Versorgungssicherheit
- Sicherheit für Daten und Informationen
- Sicherheit für Mensch und Umwelt
- Management der Nachhaltigkeit / Sustainable Development Goals
- Sicherheit in Transport und Logistik
- Ausfallsicherheit für Einrichtungen des Gesundheitswesens
- Integrale Sicherheit
- weitere

Eine spezifische Rolle und / oder Führungsstufe ist nicht erforderlich. Bereits vorhandene Praxiserfahrung ist von grossem Vorteil.

Zudem wird ein Basiswissen und Praxiserfahrung empfohlen zu Themen wie Einrichtung und Pflege von Managementsystemen, zu Risikomanagement, zu Compliance und Controlling-Aufgaben.

3 Prüfung

3.1 Prüfung „Manager:in ITSCM und Informationssicherheit SAQ“

- Die Prüfung findet schriftlich in den Räumen des Prüfungsanbieters, on remote, oder in geeigneten anderen Räumen statt. Wird die Prüfung on remote abgelegt, ist der Kandidat / die Kandidatin selbst verantwortlich für eine geeignete Prüfungsumgebung.
- Die Anmeldung zur Prüfung findet durch den Kandidaten / die Kandidatin selbständig via online-Portal statt: 4m2s-Academy.com
- Die Prüfungsdauer beträgt rund 120 Minuten.
- Die Prüfung gilt als bestanden, wenn mindestens 80% der möglichen Punktzahl erreicht wird.
- Die Prüfung kann 1 Mal wiederholt werden. Eine weitere Wiederholung ist nach jeweils vorgängigem kostenpflichtigem 1:1-Training / Coaching möglich.
- Die Prüfung erfolgt open book, es dürfen alle Unterlagen und Hilfsmittel benutzt werden.
- Kosten für die Prüfung sind beim jeweiligen Anbieter anzufragen

Prüfungsform:

Es sind Wissensfragen ebenso zu beantworten wie die Anwendung des Stoffes in Fallbeispielen. Es sind Stichworte, ganze Sätze oder auch Skizzen verlangt resp. möglich.

3.2 Prüfungsziele

Mit der Prüfung wird ermittelt, ob die Kandidaten

- erkennen, wie sie in einer Unternehmenseinheit die Gesamtverantwortung für ein effizientes ITSCM und Aufrechterhaltung der Informationssicherheit im Alltag wie im Ereignis wahrnehmen können
- ein ITSCM und ISMS im PDCA-Zyklus unterhalten und via Steuerung der relevanten Aktivitäten kontinuierlich weiterentwickeln können
- die Zusammenarbeit mit andern Managementsystem-Verantwortlichen aufbauen und optimieren können
- adäquate Instrumente entwickeln, deren Einsatz steuern und verbessern können: verstehen der Kritikalität, Impact Analysen, Massnahmen zur Aufrechterhaltung der ITSCM sowie der Informationssicherheit, Schulungen, Tests, Übungen, Messgrössen, interne Audits, Lieferantenaudits, Third Party Audits, Management Review, strukturierte kontinuierliche Weiterentwicklung (KVP)

Basis für die Beurteilung der Antworten sind die jeweils gültigen Versionen der Normen ISO 2000, ISO 22301 und ISO 27001.

Es gelten die Taxonomiestufen 4 und 5 gemäss Bloom, für einzelne Fragen zur Theorie kann auch die Stufe 3 gelten.

3.3 Lernthemen

Die Fragen basieren auf den Anforderungen der 3 Normen ISO 2000, ISO 22301 und ISO 27001. Es gilt die jeweils gültige Normversion. Der Schwierigkeitsgrad richtet sich nach den Taxonomiestufen 3 - 5 gemäss Modell von B.Bloom.
Die Prüfungsfragen richten sich nicht nach den Normkapiteln der ISO-Normen, sondern ermöglichen den Kandidaten die jeweiligen Themen integriert anzuwenden. Die gesamthafte Zuordnung der Fragen gliedert sich wie folgt:

Themen ISMS & ITSCM	*Erforderliches Wissen*	*Anzahl Fragen und Punktzahl*
ISMS-Massnahmen planen und Umsetzung steuern	Aufbau und Reifegradentwicklung eines Managementsystems zur Sicherstellung der Informationssicherheit: - analysieren und bestimmen kritische Erwartungen seitens Stakeholder, kritische Momente der Informationssicherheit im Alltag wie im Ereignis, rechtliche und regulatorische Anforderungen - Policy - Planen und umsetzen ISMS-Massnahmen und erkennen deren Wirksamkeit	1-3 Fragen 10-30 Punkte
ITSCM- Massnahmen planen und Umsetzung steuern	Aufbau und Reifegradentwicklung eines ITSCM-Systems, das die kritischen Erwartungen der Stakeholder erkennt und bedient und dennoch wirtschaftlich betrieben wird: - erforderliche Organisation, Kompetenzen und Verantwortlichkeiten zur effektiven Umsetzung von IT-SCM - Planung und Steuerung der Resilienz der IT-Services inkl. des Impactmanagements (BIA), Audits und Management Review, Massnahmen, Notfallpläne, Tests & Übungen, Dokumentation	1-3 Fragen 10-30 Punkte
branchenspezifische Compliance-Anforderungen kennen und deren Einhaltung steuern	Kennen der ITSCM & ISMS Anforderungen und Erwartungen rechtlich, organisatorisch, personell, seitens kritischer Stakeholder, seitens erforderlicher Awareness im integrierten Management.	1-3 Fragen 5-15 Punkte
Prozesse und Schnittstellen mit heiklem Informationsfluss überwachen	Sicherstellen von erforderlichen ITSCM & ISMS Ressourcen, Kommunikation und Dokumentation für das Erkennen heikler Momente für sicheren Informationsfluss, im Alltag wie im Ereignis, sowie im Wiederaufbau nach einem Ereignis. Datenschutzanforderungen lokalisieren und zielgerichtet deren Einhaltung steuern.	1-3 Fragen 5-15 Punkte
relevante Phasen im PDCA-Zyklus steuern	Umsetzung von ITSCM- und ISMS-Anforderungen, inkl. der Planung, Massnahmen zur Resilienz, Tests / Übungen und Verbesserungsmassnahmen via eines integrierten Managementsystems im PDCA-Zyklus.	1-5 Fragen 10-30 Punkte

Messen, Bewerten und Weiterentwickeln	Wirksames Controlling zum ISMS- und ITSCM-Reifegrad mit aussagekräftigen KPI's, Audits und KVP unterhalten.	1-3 Fragen 5-15 Punkte
integrale Sicherheit	Kennen, wie und wo Anforderungen des ITSCM und ISMS' in Strukturen der Notfall- und Krisenorganisation eingebunden sein sollten, intern und bei externen Partnern.	1-3 Fragen 5-15 Punkte
Totale	*Pro Frage können Inhalte mehrerer Kapitel kombiniert werden.*	*Total 7-9 Fragen* *Total 90 Punkte*

Die Prüfung gilt als bestanden bei Erreichen von mind. 80% der Punktzahl.

4 Rezertifizierung

Das Zertifikat ist für 3 Jahre ab bestandener Prüfung gültig

Für die Aufrechterhaltung des Zertifikats ist ein Nachweis einer mind. 2stündigen Weiterbildungsveranstaltung pro Jahr nötig, auf dem Niveau der Taxonomiestufen 4 resp. 5 von B.Bloom. Werden weitere Abschlüsse erfolgreich durchlaufen, die mehr Wissen als für dieses Zertifikat erforderlich, vermitteln, wird dadurch das Zertifikat validiert.

Für die Re-Zertifizierung ist spätestens zum Zeitpunkt des Ablaufs des Zertifikats ein Nachweis zu erbringen. Die Zertifikatsinhaber weisen gegenüber der Zertifizierungsstelle nach, dass sie in der bisherigen Zertifikatslaufzeit ihr Fachwissen und ihre Praxiskompetenz auf dem Gebiet des Business Continuity Management aktuell gehalten haben.

Mögliche Nachweise für Fachwissen und Praxiskompetenz (nicht abschliessend):

- Fachveranstaltung
- Einschlägige Netzwerkveranstaltung
- Höhere Ausbildungen im Thema
- Praxisarbeit in der Fachverantwortung
- Praxisarbeit als Expertin / als Experte
- Weitere adäquate Aus- / Weiterbildungen und Tätigkeiten

Der Antrag zur Re-Zertifizierung muss proaktiv durch die Zertifikatsinhaber erbracht werden.

5 SAQ Zertifikat

- Das Zertifikat ist nach erfolgter Erstzertifizierung drei Jahre gültig
- Das Zertifikat ist Eigentum der SAQ
- Das Zertifikat wird nach bestandener Prüfung auf Antrag der Prüfstelle durch SAQ ausgestellt. Die Übermittlung an die Kandidaten erfolgt durch die Prüfstelle.

- Das Zertifikat wird in der Prüfungssprache ausgestellt.
- Für die Ausstellung des Zertifikates (Erst- und Re-Zertifizierung) wir dem Kandidaten eine Gebühr verrechnet. Die Kosten sind beim jeweiligen Anbieter anzufragen.

Weitere Bestimmungen siehe Prüfungs- und Zertifizierungsreglement.

6 Anhänge

Spezifische/Detaillierte Informationen, welche nicht für die Öffentlichkeit gedacht sind, sondern für Unterauftragnehmer

- Lernthemenkatalog (genaue Inhalte mit Taxonomien): Lernthemenkatalog Manager:in ITSCM & Informationssicherheit 1.P.3