Zertifizierungsprogramm P89

Zertifiziertes Leitungsorgan gem. NISG 2024 / EU Richtlinie 2022/2555

Version 1.0: 2024-04-24

Medieninhaber und Hersteller
Austrian Standards plus GmbH Heinestraße 38, 1020 Wien

E-Mail: certification@austrian-standards.at
Internet: www.austrian-standards.at

Inhaltsverzeichnis

1 Geltungsbereich

Das vorliegende Zertifizierungsschema legt die Vorgangsweise zur Zertifizierung der Kompetenz von Leitungsorganen gem. NISG 2024[1] sowie der EU-Richtlinie 2022/2555[2] durch Austrian Standards plus Certification (AS+C), dem Geschäftsbereich Zertifizierung der Austrian Standards plus GmbH, fest.

Gegenstand der Zertifizierung ist ausschließlich die Kompetenz natürlicher Personen. Die Zertifizierung erfolgt nach den Grundsätzen der ISO/IEC 17024[3].

2 Anforderungen an die Kompetenz

2.1 Kompetenz- & Tätigkeitsprofil

Zertifizierte Leitungsorgane verfügen über rechtliches Wissen in Bezug auf nationale und europäische Regelungen im Bereich der Netz- und Informationssicherheit. Sie sind kompetent, Prozesse auf der Grundlage des NISG 2024 sowie der Europäischen Richtlinie 2022/ 2555 zu definieren und zu überwachen. Sie kennen die Anforderungen an die diesbezüglichen Berichtspflichten sowie die damit verbundenen unternehmerischen und persönlichen Haftungsrisiken. Sie sind kompetent Risikomanagementmaßnahmen auf deren Notwendigkeit im Sinne des NISG hin zu überprüfen und deren Umsetzung zu überwachen.

2.2 Anforderungen an Wissen und Fertigkeiten

Personen, die gemäß diesem Zertifizierungsschema zertifiziert sind, müssen Kompetenzen und Wissen gemäß der Abschnitte 2.2.1 bis 2.2.2 aufweisen.

2.2.1 Grundkenntnisse im Bereich Sicherheit von Netz- und Informationssystemen, Richtlinien und Standards

Zertifizierte Personen

- verfügen über grundlegendes Wissen im Zusammenhang mit internen Kontrollsystemen zur Sicherstellung der Sicherheit von Netz- und Informationssystemen.
- sind in der Lage die Regeln im Zusammenhang mit den „Business Judgement Rules“ bei der Implementierung eines Informationssicherheitsmanagementsystems anzuwenden.
- kennen die EU-Richtlinie 2022/2555 der europäischen Union und das Netz- und Informationssystemsicherheitsgesetz 2024 (NISG 2024).
- haben ein Grundverständnis, wie Standards (wie z.B. ISO/IEC 27001[4]) der Informationssicherheit zur Umsetzung der Richtlinie 2022/2555 angewendet werden können.

2.2.2 Managementsystem zur Sicherstellung von Netz- und Informationssystemsicherheit

Zertifizierte Personen

- kennen die Anforderungen an ein Managementsystem im Sinne der Richtline 2022/2555 und des NISG 2024.
- können Risiken im Zusammenhang mit der Sicherheit von Netz- und Informationssystemen identifizieren und bewerten.

---

[1] Netz- und Informationssicherheitsgesetz 2024.

[2] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (Text von Bedeutung für den EWR).

[3] ISO/IEC 17024:2012-07 Konformitätsbewertung - Allgemeine Anforderungen an Stellen, die Personen zertifizieren.

[4] ÖVE/ÖNORM EN ISO/IEC 27001: 2023-09 Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme – Anforderungen.

- können Risikomanagementmaßnahmen definieren, bewerten und überwachen.
- kennen die damit verbundenen unternehmerischen und etwaigen persönlichen Haftungsrisiken.
- können die Sicherheit von Netz- und Informationssystemen im Rahmen der IT-Strategie sowie die damit verbundene Prozesse der Einrichtung überwachen.

3 Prüfung

Die Prüfung wird in Form eines Single-Choice-Tests abgehalten und umfasst 30 Fragen aus den zwei Themengebieten gemäß Abschnitt 2.2.1 bis 2.2.2. wie folgt:

- 15 Fragen gem. Abschnitt 2.2.1
- 15 Fragen gem. Abschnitt 2.2.2

Die maximale Dauer der schriftlichen Prüfung ist mit 45 Minuten festgelegt.

Anmerkung: die Nutzung von Fachliteratur, Vortragsunterlagen, Mitschriften sowie die Nutzung des Internets (zu Recherchezwecken) ist erlaubt.

4 Bewertungskriterien

Es können maximal 30 Punkte erreicht werden, wobei jede richtig beantwortete Frage mit einem Punkt bewertet wird.

Zur positiven Absolvierung der Gesamtprüfung müssen mindestens 60% der Gesamtpunktzahl (=18 von insgesamt 30 Punkten) erreicht werden.

5 Zertifizierungsvoraussetzungen Erst-Zertifizierung

Folgende Voraussetzungen müssen für die Ausstellung eines Zertifikates erfüllt sein:

1. Nachweise einer absolvierten Ausbildung bezogen auf die Inhalte gem. Abschnitt 2 im Ausmaß von mind. 16 Wochenstunden
2. positives Prüfungsergebnis (gem. Abschnitt 4 Bewertungskriterien)

Die Zertifikate haben eine Gültigkeit von 3 Jahren.

6 Beschwerde, Einspruch, Prüfungseinsicht/-auskunft

6.1 Einspruch: Prüfungsteilnehmende haben das Recht, Einspruch gegen das Prüfungsergebnis einzulegen. Die Zertifizierungsstelle von Austrian Standards folgt der in der ISO/IEC 17024 vorgegebenen Definition eines Einspruchs: „Mit dem Einspruch bringt der Anbieter eines Gegenstandes der Konformitätsbewertung gegenüber der Konformitätsbewertungsstelle sein Verlangen zum Ausdruck, die Entscheidung bezüglich dieses Gegenstandes zu überprüfen“.

6.2 Beschwerde: Prüfungsteilnehmende haben das Recht, Beschwerde bei der Zertifizierungsstelle einzulegen. Die Zertifizierungsstelle von Austrian Standards folgt der in der ISO/IEC 17024 vorgegebenen Definition einer Beschwerde: „Mit der Beschwerde bringt eine Person oder eine Organisation ihre Unzufriedenheit bezüglich der Tätigkeit der Konformitätsbewertungsstelle zum Ausdruck und erwartet eine Antwort“.

Beschwerden und Einsprüche sind schriftlich bei der Zertifizierungsstelle einzureichen.

6.3 Prüfungseinsicht und -auskunft: Eine Prüfungseinsicht sowie eine Prüfungsauskunft (erreichte Punkteanzahl) kann ausschließlich bei Nicht-Bestehen der Prüfung im Rahmen eines Einspruchsverfahrens vorgenommen/erteilt werden.

7 Rezertifizierung

7.1 Kriterien zur Verlängerung des Zertifikates

Zur Verlängerung des Zertifikates muss die Zertifikatsinhaberin/der Zertifikatsinhaber die folgenden Kriterien erfüllen:

7.1.1 Die Zertifikatsinhaberin/der Zertifikatsinhaber muss Nachweise über facheinschlägige Weiterbildungen im Ausmaß von mindestens 24 Stunden für den gesamten Zertifizierungszyklus erbringen.

7.1.2 Die Zertifikatsinhaberin/der Zertifikatsinhaber muss Nachweise über die aufrechte, einschlägige Tätigkeit erbringen. Dies hat in Form von Tätigkeits- bzw. Projektbeschreibung zu erfolgen.

7.2 Ausstellung des Zertifikates

Nach Erfüllung aller Kriterien gemäß 7.1.1 und 7.1.2 wird das Zertifikat für drei Jahre verlängert.

7.3 Fristen

Die Rezertifizierung muss vor dem Ablauf des Zertifikates erfolgen. In Ausnahmefällen kann die Rezertifizierung auch nach Ablauf des Zertifikates erfolgen. Hierbei gelten folgende Bedingungen:

7.3.1 Erfolgt die Rezertifizierung nach Ablauf der Gültigkeit eines Zertifikats innerhalb eines Zeitraums von maximal sechs Monaten, wird die Rezertifizierung gemäß den Kriterien und dem Prozess gemäß Abschnitt 7.1 durchgeführt. Andernfalls ist eine Prüfung im Umfang der Erstzertifizierung gemäß Abschnitt 3 durchzuführen.

7.3.2 Die Gültigkeit des Zertifikats richtet sich immer nach dem Datum der Erstzertifizierung. Das heißt, es wird immer vom Datum der Erstzertifizierung ausgegangen, unabhängig von dem Datum der tatsächlich erfolgten Rezertifizierung.