Bundeskanzleramt

Bundesministerium
Inneres

Qualifizierte Stellen

NIS Fact Sheet 7/2019 – Version 3

Wien, Februar 2024

Inhalt

1 Einleitung

1.1 Rahmen

Betreiber wesentlicher Dienste haben gemäß § 17 Abs. 3 des Netz- und Informationssystemsicherheitsgesetzes (NISG) mindestens alle drei Jahre nach deren Identifizierung gegenüber dem Bundesminister für Inneres nachzuweisen, dass sie geeignete und verhältnismäßige Sicherheitsvorkehrungen hinsichtlich jener Netz- und Informationssysteme getroffen haben, die sie für die Bereitstellung des wesentlichen Dienstes nutzen. Qualifizierte Stellen nehmen dabei eine zentrale Rolle ein, da sie als **Prüfstellen für Betreiber wesentlicher Dienste** fungieren und von diesen auch heranzuziehen sind. Die Formalia der Überprüfung selbst sind zwischen dem jeweiligen Betreiber und der jeweiligen qualifizierten Stelle mittels Vertrag bzw. Ausschreibung zu regeln.

Mit der Verordnung zur Festlegung der Erfordernisse und besonderer Kriterien für qualifizierte Stellen nach dem Netz- und Informationssystemsicherheitsgesetz (**Verordnung über qualifizierte Stellen – QuaSteV**) legt der Bundesminister für Inneres, im Einvernehmen mit dem damals zuständigen Kanzleramtsminister jene Erfordernisse fest, die qualifizierte Stellen erfüllen müssen, um Betreiber wesentlicher Dienste nach dem NISG überprüfen zu können.

1.2 Anwendungsbereich

Dieses NIS Fact Sheet dient als **Leitfaden** für Antragstellerinnen[1] und qualifizierte Stellen und führt relevante Punkte wie z. B. den Ablauf des Verfahrens zur Feststellung von qualifizierten Stellen oder die Beurteilung von Prüfern näher aus.

[1] Falls nicht näher erläutert, beziehen sich die verwendeten Begriffe in diesem Fact Sheet auf jene des NISG und der QuaSteV (zB Antragstellerin als Einrichtung im Sinne des § 3 Z 11 NISG, die mit Bescheid als qualifizierte Stelle festgestellt werden möchte).

Hinsichtlich des elektronischen Verkehrs zwischen Antragstellerin bzw. qualifizierter Stelle und der zuständigen Organisationseinheit ist dieses NIS Fact Sheet zudem als **Bekanntmachung gemäß § 13 Abs. 2 AVG** zu werten.

1.3 Zuständigkeit und Kommunikation

Nach der Organisationsstruktur des Bundesministeriums für Inneres ist die Abteilung IV/S/2-Netz und Informationssystemsicherheit als zuständige Organisationseinheit für den Bundesminister für Inneres („operative NIS-Behörde“) im Rahmen des NISG mit der Feststellung und Überprüfung der qualifizierten Stellen befasst. Die im Folgenden dargestellten Kommunikationskanäle und aktuellen Kontaktdaten finden sich zusammengefasst auch auf www.nis.gv.at/kontakt.

1.3.1 E-Mail

Das offizielle E-Mailpostfach der Abteilung IV/S/2 als zuständige Organisationseinheit lautet:
post@nis.gv.at

Die zugehörigen Schlüssel / Zertifikate zur verschlüsselten E-Mailkommunikation finden sich auf https://securemail.bmi.gv.at, wobei über den Menüpunkt „Suchen“ die zuvor angegebene E-Mailadresse einzugeben ist.

1.3.2 Telefon

Die telefonische Erreichbarkeit der Abteilung IV/S/2 ist unter folgender Rufnummer gegeben:
+43 591 33-989480

1.3.3 BMI-Cryptshare

Der BMI-Cryptshare (erreichbar unter https://cryptshare.bmi.gv.at) ist eine **Webanwendung**, die einen verschlüsselten (256 Bit AES) Datenaustausch zwischen zwei Stellen gewährleistet. Er kann als alternatives Medium für die Kommunikation zwischen zuständiger Organisationseinheit und Antragstellerinnen bzw. qualifizierten Stellen vice versa verwendet werden.

Unter https://www.bmi.gv.at/Impressum/files/Cryptshare_Leitfaden_20181215.pdf findet sich die allgemeine Anleitung zur Verwendung des BMI-Cryptshare.

1.4 Arten der Überprüfung von Betreibern wesentlicher Dienste

Der „Aufgabenbereich" einer qualifizierten Stelle gemäß § 2 Z 2 QuaSteV legt fest, welche Kategorien und Sicherheitsmaßnahmen der Netz- und Informationssystemsicherheitsverordnung (NISV)[2] in organisatorischer und/oder technischer Hinsicht von dieser bei Betreibern wesentlicher Dienste überprüft werden dürfen. Nachfolgend wird auf den Unterschied zwischen einer Überprüfung in organisatorischer und einer in technischer Hinsicht näher eingegangen.

1.4.1 Überprüfung in organisatorischer Hinsicht

Unter einer Überprüfung in organisatorischer Hinsicht sind all jene Prüftätigkeiten zu verstehen, die den Nachweis der Konzeptionierung, der Regelung und des Managements eines Informationssicherheitssystems hinsichtlich geeigneter und verhältnismäßiger Sicherheitsvorkehrungen ergeben. Die Art und Weise einer organisatorischen Überprüfung entspricht hierbei im Grunde der eines Dokumentenaudits.

1.4.2 Überprüfung in technischer Hinsicht

Die Überprüfung in technischer Hinsicht fasst all jene Prüftätigkeiten zusammen, die erforderlich sind, um die Implementierung, die Wirksamkeit und die Widerstandsfähigkeit der getroffenen Sicherheitsvorkehrungen nachzuweisen. Diese technische Überprüfung erfolgt hierbei im Zuge der üblichen Überprüfung der tatsächlichen Umsetzung der einzelnen Sicherheitsmaßnahmen im Sinne eines Vor-Ort-Audits.

[2] § 11 iVm Anlage 1 NISV

Die Überprüfung mit geeigneten Werkzeugen ist als Teil einer technischen Überprüfung zu betrachten. Hierbei erfolgt eine tiefergehende Überprüfung der Sicherheitsvorkehrungen unter Zuhilfenahme geeigneter Werkzeuge (technische Instrumente oder Hilfsmittel). Bspw. sei hier die Anwendung von Instrumenten zur Analyse von Netzwerkstrukturen erwähnt. Dabei erfüllt nicht jede Sicherheitsmaßnahme (z. B. 1.2-Sicherheitsrichtlinie gemäß Anlage 1 NISV) die Voraussetzungen oder ist geeignet durch ein bestimmtes, geeignetes Werkzeug geprüft zu werden.

2 Ablauf der Feststellung einer qualifizierten Stelle

Die folgende Grafik bietet eine Prozessübersicht. Die einzelnen Schritte werden in den folgenden Kapiteln näher erläutert.

Abbildung 1 Prozessübersicht

Bei der Feststellung von qualifizierten Stellen handelt es sich um ein Verwaltungsverfahren, das neben § 9 QuaSteV anhand der entsprechenden Bestimmungen des Allgemeinen Verwaltungsverfahrensgesetz (AVG) durchzuführen ist. Demnach haben sämtliche Nachweise (einschließlich der Sicherheitsüberprüfung der notwendigen Prüfer) bereits im Zeitpunkt der Antragstellung vorzuliegen und sind mit der Antragstellung oder unmittelbar danach an die zuständige Organisationseinheit zu übermitteln. Nachweise können auch zu einem späteren Zeitpunkt des Verfahrens noch spezifiziert werden.

2.1 Antragschreiben

Es handelt sich dabei um einen **formlosen Antrag**, der von der Antragstellerin elektronisch per E-Mail an post@nis.gv.at übermittelt wird. Dabei hat die Antragstellerin nach Möglichkeit bereits die E-Mailadresse ihrer Kontaktstelle gemäß Kapitel 2.2.1 oder alternativ die offizielle E-Mailadresse zu verwenden, mit der sie üblicherweise im elektronischen Geschäftsverkehr nach außen hin tätig wird.

Aus dem Antrag hat hervorzugehen, um **welche Einrichtung** (Name, Rechtsform etc.) es sich handelt und wo sich deren **Niederlassung** befindet. Der Antrag hat zudem darzulegen, in welchem **Aufgabenbereich** (d. h. welche Kategorie(n) oder einzelne Sicherheitsmaßnahme(n) der Anlage 1 zur NISV) die Antragstellerin tätig werden möchte.

Die Antragstellung hat förmlich **durch eine oder mehrere vertretungsbefugten Personen der Antragstellerin**, abhängig von den jeweiligen rechtlichen Gegebenheiten, oder durch einen von dieser oder diesen Personen bevollmächtigten Mitarbeiter zu erfolgen. Dabei ist der von der bzw. den entsprechenden Personen **unterfertigte** Antrag mit dem oben genannten Inhalt als Anhang im **PDF-Format** zu übermitteln. An dieser Stelle sei auch auf weitere Möglichkeiten wie bspw. die Verwendung von qualifizierten elektronischen Signaturen hingewiesen.

2.2 Übermittlung der Nachweise

Folgende Erfordernisse, die der Übersichtlichkeit halber kategorisch aufgezählt werden, haben Antragstellerinnen im Rahmen der Vorgaben der QuaSteV nachzuweisen. Alle Nachweise sind nach Möglichkeit im **PDF-Format** zu übermitteln und entsprechend ihres Inhalts zu kennzeichnen. Hierbei ist auch auf möglichst geringe Dateinamen- und Pfadlängen zu achten. Die Übermittlung hat ebenfalls wie die Antragstellung förmlich durch die jeweilige(n) vertretungsbefugte(n) Person(en) der Antragstellerin oder durch einen von dieser oder diesen Personen bevollmächtigten Mitarbeiter zu erfolgen.

Die Übermittlung der Nachweise hat **in gesammelter Form und verschlüsselt per E-Mail** bereits mit dem Antragschreiben oder unmittelbar danach an post@nis.gv.at zu erfolgen.

Alternativ kann der **BMI-Cryptshare** verwendet werden. Folgende Schritte der allgemeinen Anleitung zur Verwendung des BMI-Cryptshare sind im Sinne der gegenständlichen Verwendung zu spezifizieren[3]:

- Bei Schritt 2 sind die jeweilige Firma im Namensfeld, eine entsprechende Telefonnummer (sinnvollerweise jene der zukünftig vorgesehenen Kontaktstelle) sowie die offizielle E-Mailadresse der Antragstellerin anzugeben.
- Bei Schritt 4 ist post@nis.gv.at als Empfänger anzugeben.
- Bei Schritt 6 ist das Ablaufdatum so zu wählen, dass der Abruf für die zuständige Organisationseinheit sieben Tage (eine Woche) möglich ist.
- Falls ein Kennwort gesetzt wurde, wird dieses seitens der zuständigen Organisationseinheit von der Antragstellerin rückgefragt.

[3] https://www.bmi.gv.at/Impressum/files/Cryptshare_Leitfaden_20181215.pdf

2.2.1 Kontaktstelle

Die Antragstellerin hat gemäß § 3 Abs. 2 QuaSteV eine Kontaktstelle für die Kommunikation mit der zuständigen Organisationseinheit bekanntzugeben. Diese Kontaktstelle soll in der Praxis als **Single Point of Contact (SPOC)** der jeweiligen qualifizierten Stelle für die zuständige Organisationseinheit dienen und den Kommunikationsfluss vereinfachen.

Es reicht, wenn als Kontaktstelle eine E-Mailadresse und eine entsprechende Telefonnummer bekanntgeben werden. Die verschlüsselte Kommunikation mit der zuständigen Organisationseinheit sollte gewährleistet sein.

2.2.2 Prüfer

Qualifizierte Stellen müssen generell gemäß § 3 Abs. 1 QuaSteV befähigte sicherheitsüberprüfte Prüfer einsetzen, um Überprüfungen von Betreibern wesentlicher Dienste vornehmen zu können. Details zu Prüfern finden sich im Kapitel 3, in dem auch auf die zu erbringenden Nachweise näher eingegangen wird.

Im Rahmen des Verfahrens zur Feststellung der qualifizierten Stelle hat die Antragstellerin nach § 4 QuaSteV nachzuweisen, dass sie für jede Kategorie ihres beantragten Aufgabenbereichs **zumindest** über **einen Prüfer mit mehr als fünfjähriger und zwei Prüfer mit mehr als dreijähriger** auf die jeweilige Kategorie bezogene **Prüferfahrung** verfügt, welche entsprechende Zertifizierungen aufweisen und sicherheitsüberprüft sind. Die Antragstellerin hat somit zumindest für drei Personen als Prüfer den Nachweis über deren Befähigung zu erbringen.

Für diese potenziellen Prüfer ist Folgendes nachzuweisen:

- Durchgeführte Sicherheitsüberprüfung
- Einschlägige Berufserfahrung (z. B. durch Dienstzeugnisse)
- Ausbildung(en), Zertifizierung(en) sowie sonstige äquivalente Nachweise der Kenntnis im jeweiligen Fachbereich (organisatorisch und/oder technisch)

2.2.3 Sicherheitsvorkehrungen

Qualifizierte Stellen haben gemäß § 5 Abs. 1 QuaSteV **technische und organisatorische Sicherheitsvorkehrungen** in Hinblick auf ihre Netz- und Informationssysteme zu treffen, die geeignet, verhältnismäßig und dem Risiko angemessen sind sowie den Stand der Technik

berücksichtigen. Der Anwendungsbereich (Scope) der Sicherheitsvorkehrungen liegt dabei auf jenen Netz- und Informationssystemen, die im Zuge einer Überprüfung genutzt werden. Die Sicherheitsmaßnahmen der Anlage 1 zur NISV sind hierbei als Richtlinie zu betrachten.

Die Antragstellerin hat durch eine **detaillierte Aufstellung** (bspw. durch eine gültige und entsprechende ISO/IEC 27001 Zertifizierung, Prüfberichte, Maßnahmenbeschreibungen usw.) nachzuweisen, dass die getroffenen Sicherheitsvorkehrungen den Vorgaben entsprechen und ausreichend sind.

2.2.4 Werkzeuge

Qualifizierte Stellen haben gemäß § 6 Abs. 1 QuaSteV geeignete Werkzeuge für eine Überprüfung zu verwenden, die den Stand der Technik berücksichtigen.

Die Antragstellerin hat darzulegen, welche **Werkzeuge** (= technische Instrumente oder Hilfsmittel) für **Überprüfungen** von Betreibern wesentlicher Dienste verwendet werden sollen, um den Vorgaben zu entsprechen. Dabei sind insb. jene Werkzeuge anzuführen und zu erläutern, die zur Überprüfung der Sicherheitsvorkehrungen in technischer Hinsicht verwendet werden sollen. Generische Auflistungen, die nicht eindeutig erkennen lassen, welches Werkzeug (z. B. entsprechendes Softwareprodukt) eingesetzt werden soll, sind nicht ausreichend.

2.2.5 Prüfprozess

Qualifizierte Stellen haben gemäß § 7 Abs. 1 QuaSteV einen geeigneten **Prüfprozess** für die Überprüfung von Betreibern wesentlicher Dienste anzuwenden (Wie wird aus prozessualer und inhaltlicher Sicht geprüft?).

Zudem haben qualifizierte Stellen gemäß § 7 Abs. 2 QuaSteV durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, dass die **Sicherheit der Prüfdaten** ein entsprechendes Schutzniveau erreicht.

Um den Vorgaben zu entsprechen, hat die Antragstellerin

- den von ihr zukünftig angewendeten **Prüfprozess detailliert und aussagekräftig** zu beschreiben,

- darzulegen, wie und in welcher Form **Prüfdaten aufgearbeitet und bewertet** werden sollen sowie
- darzulegen, welche technischen und organisatorischen Maßnahmen zur Gewährleistung der **Sicherheit der Prüfdaten** getroffen werden.

2.2.6 Meldeprozess

Qualifizierte Stellen haben gemäß § 8 Abs. 1 QuaSteV bei Vorfällen, die ihre Netz- und Informationssysteme derart stören, dass die Integrität oder Vertraulichkeit der Prüfdaten nicht mehr gewährleistet werden kann, einen geeigneten **internen und externen Meldeprozess** anzuwenden.

Die Antragstellerin hat diesen zukünftig anzuwendenden Meldeprozess systematisch zu beschreiben und darzulegen, wie ein solcher Vorfall der zuständigen Organisationseinheit gemeldet werden wird.

2.3 Prüfung der Nachweise und Erledigung mittels Bescheid

Die zuständige Organisationseinheit prüft einerseits die **formale** Vollständigkeit der übermittelten Nachweise und andererseits, ob die übermittelten Nachweise **inhaltlich** den Vorgaben der QuaSteV entsprechen.

Bei **formalen Mängeln** wird der Antragstellerin die Möglichkeit zur Verbesserung (Mängelbehebungsauftrag) erteilt, dem innerhalb der von der zuständigen Organisationseinheit gesetzten Frist nachzukommen ist, ansonsten das Verfahren zurückzuweisen wäre.

Der Antragstellerin wird nach inhaltlicher Prüfung eine **Beurteilung aus inhaltlicher Sicht** der zuständigen Organisationseinheit übermittelt und die Möglichkeit gegeben, innerhalb einer angemessenen Frist allfällige inhaltliche Spezifizierungen bzw. Berichtigungen vorzunehmen.

Am Ende des Verfahrens wird mittels Bescheid ausgesprochen, ob und für welchen Aufgabenbereich die Antragstellerin als qualifizierte Stelle tätig werden kann. Bei einem rechtskräftigen positiven Bescheid wird die qualifizierte Stelle in die von der zuständigen Organisationseinheit geführte Liste gemäß § 18 Abs. 4 NISG eingetragen. In diese Liste wird Betreibern wesentlicher Dienste auf Anfrage Einsicht gewährt.

3 Prüfer

Wie bereits im Kapitel 2.2.2 erwähnt, müssen qualifizierte Stellen generell gemäß § 3 Abs. 1 QuaSteV befähigte sicherheitsüberprüfte Prüfer einsetzen, um Überprüfungen von Betreibern wesentlicher Dienste vornehmen zu können. Die entsprechende Befähigung bzw. Eignung eines potenziellen Prüfers ist dabei grundsätzlich durch die qualifizierten Stellen und Antragstellerinnen **selbständig** gemäß den Anforderungen des § 4 QuaSteV zu **beurteilen**.

In diesem Kapitel werden diese Anforderungen erläutert und präzisiert, um den Antragstellerinnen und qualifizierten Stellen einen entsprechenden Rahmen zur selbständigen Beurteilung zu bieten.

Die qualifizierte Stelle hat dafür Sorge zu tragen, dass die derart ermittelten Prüfer der zuständigen Stelle zeitgerecht, jedenfalls vor einer etwaigen Überprüfung eines Betreibers wesentlicher Dienste, bekanntgegeben werden. Die Art und Weise dieser Bekanntgabe wird in Kapitel 3.2 näher ausgeführt.

3.1 Prüfertypen

Prüfer von qualifizierten Stellen lassen sich grob in die Prüfertypen ISMS-Prüfer, Technischer Prüfer und NIS-Prüfer einteilen Die nachfolgende Erläuterung des jeweiligen Prüfertypus soll als Kategorisierungshilfe für Antragstellerinnen bzw. qualifizierte Stellen hinsichtlich der Erfahrung und Qualifikation potenzieller Prüferkandidaten dienen.

3.1.1 ISMS-Prüfer

Der ISMS-Prüfer charakterisiert sich durch seine Qualifikation im Bereich der **Prüfung und Auditierung von Managementsystemen** (z. B. ISM[4], RM[5], BCM[6]). Diese wird durch relevante, gültige und anerkannte Zertifizierungen für die Auditierung ebendieser Managementsysteme nachgewiesen. Die einschlägige Berufserfahrung ergibt sich aus einer ent-

[4] Information Security Management – Informationssicherheitsmanagement (ISM)
[5] Risk Management – Risikomanagement (RM)
[6] Business Continuity Management – Betriebskontinuitätsmanagement (BCM)

sprechend nachgewiesen Prüftätigkeit. Abhängig von den jeweiligen Managementsystemen ergeben sich Kompetenzen für unterschiedliche Kategorien bzw. Sicherheitsmaßnahmen in organisatorischer und/oder technischer Hinsicht.

Der Unterschied zu den anderen beiden Prüfertypen besteht vorrangig darin, dass für die Anwendung von geeigneten Werkzeugen zur technischen Überprüfung, z. B. in den Bereichen IT[7]/OT[8] oder ICS[9], keine oder keine ausreichende Qualifikation oder Berufserfahrung vorliegt bzw. objektiv nachgewiesen werden kann.

Ein ISMS-Prüfer kann somit durch eine qualifizierte Stelle für Überprüfungen in ihrem Aufgabenbereich **eingeschränkt** in organisatorischer und/oder technischer Hinsicht eingesetzt werden.

3.1.2 Technischer Prüfer

Der Technische Prüfer zeichnet sich durch Qualifikation und Erfahrung im **Umgang mit geeigneten Werkzeugen zur technischen Überprüfung** von Sicherheitsvorkehrungen aus. Durch gültige und anerkannte Zertifizierung wird die Qualifikation nachgewiesen. Das ausreichende Maß an einschlägiger Berufserfahrung wird durch Nachweise, z. B. von Prüfungen in den Bereichen IT/OT oder ICS, erbracht.

Der Unterschied zu den anderen beiden Prüfertypen besteht vorrangig darin, dass für die Prüfung und Auditierung von Managementsystemen (z. B. ISM, RM, BCM) keine oder keine ausreichende Qualifikation oder Berufserfahrung vorliegt bzw. objektiv nachgewiesen werden kann.

Ein Technischer Prüfer kann somit durch eine qualifizierte Stelle für Überprüfungen in ihrem Aufgabenbereich **eingeschränkt**, vorrangig hinsichtlich technischer Überprüfungen, eingesetzt werden.

3.1.3 NIS-Prüfer

Der NIS-Prüfer bezeichnet Personen, die **alle Kategorien bzw. Sicherheitsmaßnahmen** vollumfänglich in organisatorischer als auch technischer Hinsicht zu ihrem Fachbereich zählen.

[7] Information Technology (IT), bspw. Office Netzwerke
[8] Operational Technology (OT), bspw. Prozessnetzwerke
[9] Industrial Control System (ICS), bspw. Systeme in Prozessnetzwerken

Durch gültige und anerkannte Zertifizierungen wird für sämtliche Aufgabenbereiche eine relevante fachliche Qualifikation nachgewiesen. Aus den Dienstzeugnissen ergeben sich ebenso für alle Aufgabenbereiche ausreichende Zeiten der Berufserfahrung, wobei hier v.a. Erfahrungen als Prüfer bzw. Auditor von Bedeutung sind.

Ein NIS-Prüfer kann somit durch eine qualifizierte Stelle für **Überprüfungen in ihrem gesamten Aufgabenbereich**, organisatorisch wie technisch, eingesetzt werden.

3.1.4 Fachbereiche nach Prüfertypen

In der nachstehenden Tabelle 1 werden den einzelnen Prüfertypen die entsprechenden Qualifikationen in den jeweiligen Sicherheitsmaßnahmen gemäß Anlage 1 NISV zugeordnet. Hierbei ist zu berücksichtigen, dass von dieser Kategorisierung Prüfer individuell, z. B. in einzelnen Sicherheitsmaßnahmen, aufgrund spezifischer Befähigung abweichen können.

Tabelle 1 Fachbereiche nach Prüfertypen

Kategorie	org./ techn.	Sicherheitsmaßnahme	NIS Prüfer	ISMS Prüfer	techn. Prüfer
1.1	org.	Risikoanalyse	X	X	
1.1	techn.	Risikoanalyse	X	X	
1.2	org.	Sicherheitsrichtlinie	X	X	
1.2	techn.	Sicherheitsrichtlinie	X	X	
1.3	org.	Überprüfungsplan der Netz- und Informationssysteme	X	X	
1.3	techn.	Überprüfungsplan der Netz- und Informationssysteme	X	X	
1.4	org.	Ressourcenmanagement	X	X	
1.4	techn.	Ressourcenmanagement	X	X	
1.5	org.	Informationssicherheitsmanagement-systemprüfung	X	X	
1.5	techn.	Informationssicherheitsmanagement-systemprüfung	X	X	
1.6	org.	Personalwesen	X	X	
1.6	techn.	Personalwesen	X	X	

Kategorie	org./ techn.	Sicherheitsmaßnahme	NIS Prüfer	ISMS Prüfer	techn. Prüfer
2.1	org.	Beziehungen mit Dienstleistern, Lieferanten und Dritten	X	X	
2.1	techn.	Beziehungen mit Dienstleistern, Lieferanten und Dritten	X	X	
2.2	org.	Leistungsvereinbarungen mit Dienstleistern und Dritten	X	X	
2.2	techn.	Leistungsvereinbarungen mit Dienstleistern und Dritten	X	X	
3.1	org.	Systemkonfiguration	X	X	X
3.1	techn.	Systemkonfiguration	X		X
3.2	org.	Vermögenswerte	X	X	X
3.2	techn.	Vermögenswerte	X		X
3.3	org.	Netzwerksegmentierung	X	X	X
3.3	techn.	Netzwerksegmentierung	X		X
3.4	org.	Netzwerksicherheit	X	X	X
3.4	techn.	Netzwerksicherheit	X		X
3.5	org.	Kryptographie	X	X	X
3.5	techn.	Kryptographie	X		X
4.1	org.	Administrative Zugangsrechte	X	X	X
4.1	techn.	Administrative Zugangsrechte	X	X	X
4.2	org.	Systeme und Anwendungen zur Systemadministration	X	X	X
4.2	techn.	Systeme und Anwendungen zur Systemadministration	X	X	X
5.1	org.	Identifikation und Authentifikation	X	X	X
5.1	techn.	Identifikation und Authentifikation	X	X	X
5.2	org.	Autorisierung	X	X	X
5.2	techn.	Autorisierung	X	X	X
6.1	org.	Systemwartung und Betrieb	X	X	X
6.1	techn.	Systemwartung und Betrieb	X	X	X

Kategorie	org./ techn.	Sicherheitsmaßnahme	NIS Prüfer	ISMS Prüfer	techn. Prüfer
6.2	org.	Fernzugriff	X	X	X
6.2	techn.	Fernzugriff	X		X
7.1	org.	Physische Sicherheit	X	X	X
7.1	techn.	Physische Sicherheit	X	X	X
8.1	org.	Erkennung	X	X	X
8.1	techn.	Erkennung	X	X	X
8.2	org.	Protokollierung und Monitoring	X	X	X
8.2	techn.	Protokollierung und Monitoring	X	X	X
8.3	org.	Korrelation und Analyse	X	X	X
8.3	techn.	Korrelation und Analyse	X	X	X
9.1	org.	Vorfallsreaktion	X	X	X
9.1	techn.	Vorfallsreaktion	X	X	X
9.2	org.	Vorfallsmeldung	X	X	X
9.2	techn.	Vorfallsmeldung	X	X	X
9.3	org.	Vorfallsanalyse	X	X	X
9.3	techn.	Vorfallsanalyse	X	X	X
10.1	org.	Betriebskontinuitätsmanagement	X	X	
10.1	techn.	Betriebskontinuitätsmanagement	X	X	
10.2	org.	Notfallmanagement	X	X	
10.2	techn.	Notfallmanagement	X	X	
11.1	org.	Krisenmanagement	X	X	
11.1	techn.	Krisenmanagement	X	X	

3.2 Bekanntgabe von Prüfern

Personen, die als Prüfer durch qualifizierte Stellen zur Überprüfung der getroffenen Sicherheitsvorkehrungen bei Betreibern wesentlicher Dienste eingesetzt werden sollen, sind durch Antragstellerinnen bzw. qualifizierte Stelle im Rahmen des Verfahrens zur Feststellung als qualifizierte Stelle bzw. vor der Durchführung von Überprüfungen bei Betreibern

wesentlicher Dienste bekannt zu geben. Die Bekanntgabe von Prüfern ist dabei nach Maßgabe der Ausführungen in Kapitel 1.3. verschlüsselt an post@nis.gv.at zu richten. Die Bekanntgabe hat förmlich durch die jeweilige(n) vertretungsbefugte(n) Person(en) der Antragstellerin bzw. qualifizierten Stelle oder durch einen von dieser oder diesen Personen bevollmächtigten Mitarbeiter über die Kontaktstelle zu erfolgen.

In nachstehender Tabelle 2 sind jene Fälle angeführt, in denen eine Bekanntgabe von Prüfern durch Antragstellerinnen bzw. qualifizierten Stellen mit folgenden Inhalten und Anlagen erforderlich ist. Bei den Anlagen handelt es sich in der Regel um die Grundlagen der selbständigen Beurteilung (relevante Dienstzeugnisse, Zertifizierungen, Sicherheitsüberprüfung).

Tabelle 2 Anwendungsfälle Bekanntgabe

Wann	**initiales Feststellungsverfahren**	**zusätzlicher Aufgabenbereich**	**neue bzw. ergänzte Prüfer**
Wer	Antragstellerin	Qualifizierte Stelle	Qualifizierte Stelle
Inhalt	Angaben zur Person	Angaben zur Person	Angaben zur Person
Anlagen	Tabelle Selbstbeurteilung relevante Beurteilungsgrundlagen[10]	Tabelle Selbstbeurteilung relevante Beurteilungsgrundlagen	---

3.2.1 Bekanntgabe neuer oder ergänzter Prüfer

Bei der Bekanntgabe von neuen oder ergänzten Prüfern **durch bereits festgestellte qualifizierte Stellen** sind weder die Tabelle der Selbstbeurteilung noch die Beurteilungsgrundlagen zu übermitteln. Die zuständige Organisationeinheit kann in diesem Fall nach Bekanntgabe bei Bedarf an die qualifizierte Stelle herantreten und diese im Rahmen der Überprüfung der Erfordernisse gemäß § 18 Abs. 3 NISG („Einschaurecht“) auffordern, die entsprechenden Beurteilungsgrundlagen bzw. Nachweise zu übermitteln.

[10] Die relevanten Beurteilungsgrundlagen stellen die Nachweise dar, anhand derer die Antragstellerin bzw. qualifizierte Stelle den jeweiligen Prüfer beurteilt hat.

Der Fall „ergänzte Prüfer“ bezieht sich nur auf bereits bestehende Prüfer, bei denen durch Erweiterung ihrer Qualifikation, z. B. durch zusätzlich erworbene Berufserfahrung oder Zertifizierung, ihre Befähigung auf bestimmte Kategorien bzw. Sicherheitsmaßnahmen des Aufgabenbereichs der qualifizierten Stelle erweitert werden soll.

3.2.2 Bekanntgabe von Prüfern im Rahmen des initialen Feststellungsverfahrens bzw. bei Beantragung eines zusätzlichen Aufgabenbereiches

Die Bekanntgabe von Prüfern im Rahmen des initialen (erstmaligen) Feststellungsverfahrens, oder bei Beantragung der Erweiterung des Aufgabenbereiches einer bereits festgestellten qualifizierten Stelle erfordert, dem Anbringen an die Behörde auch die Tabelle der Beurteilung des jeweiligen Prüfers durch die Antragstellerin bzw. qualifizierte Stelle sowie sämtliche die Qualifikation bzw. die Berufserfahrung des Prüfers nachweisenden Dokumente beizufügen. Die selbständig durchzuführende Beurteilung hinsichtlich der Qualifikation in den Fachbereichen ist anhand einer tabellarischen Zuordnung zu den einzelnen Kategorien und Sicherheitsmaßnahmen unter Angabe der jeweiligen relevanten Berufserfahrung darzustellen.

3.3 Anforderungen an Prüfer

Jede Person, die als Prüfer eingesetzt werden soll, hat folgende Anforderungen zu erfüllen, die entsprechend nachzuweisen sind:

- Einschlägige **Berufserfahrung der Prüftätigkeit** (z. B. durch Dienstzeugnisse)
- Akademische **Ausbildung(en)**, gültige **Zertifizierung(en)** zum **Nachweise der Kenntnis** im jeweiligen Fachbereich (organisatorisch und/oder technisch)
- **Gültige Sicherheitsüberprüfung** der Stufe „geheim“

3.3.1 Berufserfahrung

Unter „[…] einschlägiger Berufserfahrung im Bereich der Sicherheit von Netz- und Informationssystemen […]“ gemäß § 4 Abs. 1 QuaSteV sind v.a. **Erfahrungen im Bereich der Überprüfung (Audit)** von Informationssicherheitsmanagementsystemen (ISMS) oder Cybersicherheitsmanagementsystemen (CSMS) sowie Sicherheitslösungen im IT-/OT-Umfeld zu verstehen.

Der Nachweis hierüber muss in einer **objektivierbaren Form**, bspw. durch ein Dienstzeugnis oder eine Arbeitsbestätigung, vorgelegt werden. Der bloße Nachweisversuch mittels Curriculum Vitae (CV) ist keinesfalls ausreichend. Erfahrungen in der Beratung oder Implementierung von ISMS bzw. von Sicherheitslösungen im IT-/OT-Umfeld werden angerechnet, wenn diese in verantwortlicher Position erworben wurden.

Aus den objektiv nachgewiesenen Zeiten errechnet sich schlussendlich die einschlägige Berufserfahrung, die zumindest drei Jahre betragen muss.

3.3.2 Zertifizierung

Bei der persönlichen Qualifikation eines Prüfers „[…] durch zumindest eine anerkannte Zertifizierung im Bereich der Sicherheit von Netz- und Informationssystemen […]“ gemäß § 4 Abs. 2 QuaSteV sind entweder **abgeschlossene facheinschlägige Studien** (z. B. Bachelor-, Master- oder Diplomstudium in den Studienrichtungen IT-Sicherheit, Informationssicherheit oder Informationssicherheitsmanagement) mit NIS-relevanten Studienschwerpunkten oder **gültige Personenzertifizierungen** (z. B. für die Auditierung von ISMS oder für die technische Überprüfung von IT-/OT-Umgebungen oder ICS) von renommierten, üblicherweise in der Branche der Sicherheit von Netz- und Informationssystemen herangezogenen Anbietern als Nachweise relevant. Reine Produktzertifizierungen, z. B. für spezifische IT-Security Appliances oder Risikomanagement-Tools, werden nicht anerkannt.

In der nachstehenden Tabelle 3 sind beispielhaft Bereiche von Zertifizierungen angeführt, die auf die unterschiedlichen Prüfertypen referenzieren und somit in Kombination mit Tabelle 1 zu verstehen sind. Auf die Namhaftmachung expliziter Personenzertifizierungen oder Studiengänge wird bewusst verzichtet.

Tabelle 3 Zertifizierungsbereiche beispielhaft

Zertifizierungen für die Fachbereiche, die den jeweiligen Prüfertypen zugerechnet werden können	**NIS Prüfer**	**ISMS Prüfer**	**techn. Prüfer**
für Auditierung nach ISO 27001	X	X	
für Prüfen von IT/OT-Architekturen	X		X
für Auditierung nach ISO 22301	X	X	
für Durchführen von Penetrationstests	X		X
…			
Akademischer Abschluss mit Schwerpunkt ISMS	X	X	
Akademischer Abschluss mit Schwerpunkt IT-Security	X		X
…			

3.3.3 Sicherheitsüberprüfung

Die Vorlage einer Sicherheitsüberprüfung nach §§ 55 ff des Sicherheitspolizeigesetzes (SPG) dient dem Nachweis der Vertrauenswürdigkeit des Prüfers, v. a. im Umgang mit sensiblen Prüfdaten. Nähere Details zur Sicherheitsüberprüfung und deren Durchführung finden sich im Kapitel 5.

Die Anerkennung einer ausländischen Sicherheitsüberprüfung muss von Fall zu Fall geprüft werden und ist insbesondere auch von rechtlichen Anerkennungsregimen wie z. B. zwischenstaatlichen Vereinbarungen abhängig.

4 Jährlicher Statusbericht

Qualifizierte Stellen haben gemäß § 3 Abs. 4 QuaSteV jährlich ab Zustellung des Bescheids in einem Statusbericht über ihre Tätigkeiten zu berichten. Der Statusbericht ist in übersichtlicher Form im **PDF-Format** an die zuständige Organisationeinheit **fristgerecht und verschlüsselt per E-Mail** durch die Kontaktstelle zu übermitteln. Dieser Statusbericht hat dabei mindestens folgende Punkte zu beinhalten:

- Durchgeführte Überprüfungen mit eingesetzten Prüfern (vgl. Tabelle)
- Weiterbildungsmaßnahmen (vgl. Tabelle 5)

4.1 Durchgeführte Überprüfungen

Die im Beobachtungszeitraum stattgefundenen Überprüfungen von Sicherheitsvorkehrungen durch QuaSten bei Betreibern wesentlicher Dienste (BwD) sind unabhängig davon, ob die betreffenden Überprüfung bereits zur Gänze abgeschlossen sind oder durch die beauftragenden BwD als Nachweise gemäß § 17 Abs. 3 NISG an die Behörde übermittelt wurden, aufzulisten.

4.2 Weiterbildungsmaßnahmen

Der Nachweis der verpflichtenden Weiterbildungsmaßnahmen gemäß § 4 Abs. 5 QuaSteV ist für sämtliche bekanntgegebene Prüfer und Prüferinnen gemäß den formalen Vorgaben der Tabelle 10 für den betreffenden Beobachtungszeitraum des abgelaufenen Jahres zu erbringen. Als Richtwert des zeitlichen Umfangs der Weiterbildungsmaßnahmen werden in etwa 40 Stunden je Person innerhalb des Beobachtungszeitraums erwartet. Die Inhalte sollten sich hierbei an den Fachbereichen der Prüfer bzw. Prüferinnen orientieren.

Der Umfang von 40 Stunden wird insofern als angemessen erachtet, da dieses Ausmaß idR auch für die Aufrechterhaltung einschlägige Personenzertifizierungen (z.B. CISSP, CISA, CISM) erforderlich ist. Derartige Aufwendungen (z.B. Continuing Professional Education; 1 CPE = 1 Stunde) können als Weiterbildungsmaßnahmen eines Prüfers bzw. einer Prüferin geltend gemacht werden. Gleiches gilt für Aufwendungen, die in Form von ECTS (European

Credit Transfer and Accumulation System) nachgewiesen werden können. Hierbei gilt, dass 1 ECTS = 25 Stunden repräsentiert und folglich der Umfang von 40 Stunden in etwa 1,5 ECTS entspricht. Neben der üblichen präsenten oder virtuellen Absolvierung von Kursen und Lehrgängen ist bspw. auch die Vortrags- oder Lehrtätigkeit im jeweiligen Fachbereich zulässig. Zur Berechnung des empfohlenen Richtwerts werden entweder die exakt angegebenen Stunden oder acht Stunden je Kalendertag herangezogen.

Die Weiterbildungsmaßnahmen sollten sich inhaltlich an den Fachbereichen der Prüfer und Prüferinnen orientieren und ein ausgewogenes Maß an Fachkursen und andere Formen der Wissensvermittlung beinhalten. Die ausschließliche Durchführung von Besprechungen oder Seminaren innerhalb der QuaSte zum Erfahrungsaustausch zwischen den dortigen Prüfern und Prüferinnen ist jedoch nicht ausreichend.

Sollten für diesen Personenkreis unbegründet keine entsprechenden Weiterbildungsmaßnahmen aufgelistet sein, so stellt dies einen groben Mangel und somit eine Nichterfüllung der Erfordernisse einer QuaSte dar.

Sollte sich aus den Weiterbildungsmaßnahmen auch der Wunsch nach einer Anpassung der Aufgabenbereiche der qualifizierten Stelle oder der Fachbereiche der Prüfer ergeben, so ist dies gesondert gemäß den Vorgaben aus Kapitel 3.2 als Bekanntgabe ergänzter Prüfer entsprechend oder als Beantragung eines zusätzlichen Aufgabenbereichs entsprechend mitzuteilen.

Tabelle 4 Mustertabelle durchgeführte Überprüfungen

Von - Bis	**Betreiber wesentlicher Dienst**	**Kategorien / Sicherheitsmaßnahmen**	**eingesetzte Prüfer**
…	…	…	
01.10.2023 - 12.10.2023	Versorger AG	1.1o, …, 3.1o, 3.1t …,, 7.1t, …	Max Mustermann Rosa Roth (Lead)
…	…	…	…

Tabelle 5 Mustertabelle Weiterbildungsmaßnahmen

Von - Bis	**Anbieter**	**Kursbezeichnung**	**Prüfer**
…	…	…	…
18.12.2022	Musterprüfer GmbH (inhouse)	Seminar Neuerungen im NIS Umfeld	Max Mustermann Rosa Roth
15.01.2023 - 17.01.2023	Ausbilder GmbH	Audit bei kritischen Infrastrukturen	Rosa Roth
…	…	…	…

5 Exkurs Sicherheitsüberprüfungen

5.1 Überblick

Die Sicherheitsüberprüfung ist die **Abklärung der Vertrauenswürdigkeit eines Menschen** anhand personenbezogener Daten, die Aufschluss darüber geben, ob Anhaltspunkte dafür bestehen, dass er gefährliche Angriffe begehen werde.

Eine Sicherheitsüberprüfung hat u. a. zu erfolgen (gemäß § 55a Abs. 2 SPG):

„3a. auf begründetes Ersuchen jenes Unternehmens, in dem der Betroffene eine Tätigkeit wahrnimmt oder anstrebt, bei der er Zugang zu vertraulicher Information hat, deren unzulässige Verwertung eine nachhaltige Funktionsstörung oder Zerstörung einer **kritischen Infrastruktur** *bewirken würde“.*

Die Zulässigkeit einer Sicherheitsüberprüfung setzt die **Zustimmung** des zu Überprüfenden und seine **„Sicherheitserklärung“** voraus (die Zustimmung und eine Erklärung des Betroffenen hinsichtlich seines Vorlebens und seiner gegenwärtigen Lebensumstände). Diese Zustimmung muss auch für die Übermittlung des Ergebnisses der Überprüfung an das ersuchende Unternehmen vorliegen.

Das Unternehmen, das um die Durchführung der Sicherheitsüberprüfung ersucht, hat deren Kosten zu tragen. Der Pauschalsatz für die Durchführung der Sicherheitsüberprüfung bei einer Sicherheitserklärung für den Zugang zu geheimer Information beträgt gemäß § 5 Z 2 der Sicherheitsgebühren-Verordnung (SGV) derzeit **593,- Euro**. Die Sicherheitsüberprüfung wird zentral von der Direktion für Staatsschutz und Nachrichtendienst (DSN) durchgeführt.

Unter https://www.bmi.gv.at/Downloads/Sicherheitserklaerung.aspx finden sich das zu verwendende **Formular** für Sicherheitserklärungen der Stufe "geheim", wobei nach Möglichkeit das Formular in Deutsch zu verwenden ist, sowie ein allgemeines Merkblatt zur Sicherheitsüberprüfung.

5.2 Vorgehensweise bei Prüfern

Das Unternehmen hat für jeden Prüfer bzw. jede Person, die als Prüfer tätig werden soll, das Ersuchen auf Sicherheitsüberprüfung separat per E-Mail an s4-sue@dsn.gv.at[11] zu richten. Das zuständige Referat für Sicherheitsüberprüfungen in der DSN führt die Abklärung durch und übermittelt das Ergebnis der Sicherheitsüberprüfung an das ersuchende Unternehmen.

Bei der Beantragung von Sicherheitsüberprüfungen ist die nachfolgende Form (vgl. Tabelle) zu wahren.

Tabelle 6 Muster E-Mail Antrag auf Sicherheitsüberprüfung

Von:	nis-spoc@musterpruefer.com
An:	s4-sue@dsn.gv.at
Betreff:	Sicherheitsüberprüfung Musterprüfer GmbH – NIS-Quaste
Angefügt:	Sicherheitserklärung.pdf Identitätsnachweis.pdf
… Das Unternehmen Musterprüfer GmbH ersucht um Sicherheitsüberprüfung des/der Beschäftigten Rosa Roth gemäß § 55 SPG für die Stufe „geheim“ (SE Anlage B). Begründung der Notwendigkeit: … Rechnungsanschrift: … UID- und Firmenbuchnummer: … Erledigungsadresse: … … *(siehe nachfolgende Erläuterungen)*	

[11] Die Übertragung in verschlüsselter und signierter Form wird empfohlen. (siehe hierzu https://dsn.gv.at/Kontakt/start.aspx)

Erläuterungen:

Sicherheitserklärung:	Die Sicherheitserklärung für die Stufe „geheim“ muss vollständig ausgefüllt und entsprechend handschriftlich oder qualifiziert elektronisch (z.B. mittels ID-Austria) unterfertigt (siehe hierzu Punkt 10 und 11 in der Sicherheitserklärung) sein.
Identitätsnachweis:	z. B. Kopie des Führerscheins, Reisepasses oder Personalausweises
Begründung der Notwendigkeit:	Warum haben Mitarbeiter bzw. Prüfer Zugang zu vertraulichen Informationen, durch deren missbräuchliche Verwendung diese kritische Infrastrukturen bzw. Betreiber wesentlicher Dienste schädigen könnten? (siehe § 55a SPG)
Rechnungsanschrift:	des Unternehmens (nach Möglichkeit elektronisch)
UID- und Firmenbuchnummer:	Zur besseren Identifizierung und Abwicklung sind die entsprechende Umsatzsteuer-Identifikationsnummer (UID-Nummer) sowie – falls vorhanden – die entsprechende Firmenbuchnummer des Unternehmens anzugeben.
Erledigungsadresse:	Stelle bzw. Person im Unternehmen, zu deren Handen das Ergebnis der Sicherheitsüberprüfung übermittelt werden soll (nach Möglichkeit elektronisch). Das Ergebnis der Sicherheitsüberprüfung kann dabei nicht an eine Person übermittelt werden, die selbst Gegenstand der Überprüfung ist!

6 Versionshistorie

Bei diesem Dokument handelt es sich um die Version 3 vom 07. Februar 2024.

Folgende relevanten Änderungen und Anpassungen gegenüber der Version 2 wurden vorgenommen:

- Aktualisierung der Kommunikationskanäle mit und der Kontaktdaten der zuständigen Organisationseinheit
- Streichung des Kapitels 2.2 Erhalt einer Kennung
- Zur Präzisierung neue Kapitel 4.1 Durchgeführte Überprüfungen und 4.2 Weiterbildungsmaßnahmen eingeführt
- Kapitel 5 Exkurs Sicherheitsüberprüfungen: Änderung der Kontaktdaten und Präzisierung der Form (insb. Angabe von UID- und Firmenbuchnummer sowie entsprechende Unterschriften bei ausgefüllter Sicherheitserklärung)

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundeskanzleramt, Ballhausplatz 2, 1010 Wien
Autoren: Bundeskanzleramt Abteilung I/8 (Technologie- und Datenmanagement, Cybersicherheit und Krisenrechenzentrum) und BMI/IV/S/2 (Netz- und Informationssystemsicherheit)
Wien, 2024. Stand: 7. Februar 2024

Abschließende Anmerkungen:
Es wird darauf hingewiesen, dass Änderungen vorbehalten sind.
Alle in diesem NIS Fact Sheet verwendeten personenbezogenen Bezeichnungen gelten gleichermaßen für alle Geschlechter.

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an nis@bka.gv.at und post@nis.gv.at .