CIS
Prüfverfahren für
NISG §17(3)

Abläufe & Prozesse

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 Anwendungsbereich

Dieses Dokument beschreibt die Abläufe für die Prüfung nach nach dem NISG §17(3).

Die zu prüfenden Sicherheitsmaßnahmen sind in der Netz- und Informationssystemsicherheitsverordnung (NISV) näher ausgeführt. Im Weiteren wird NISV als Abkürzung verwendet, wenn die zu prüfenden Sicherheitsmaßnahmen gemeint sind.

2 Zugangsvoraussetzungen

Der Auftraggeber muss durch das Bundesministerium für Inneres (BMI) per Bescheid als Betreiber eines wesentlichen Dienstes bestimmt sein bzw. laut Gesetz zu einer Überprüfung nach dem NISG §17(3) verpflichtet sein.

3 Ablauf Prüfverfahrens

Auf Grundlage des Antrages zur Durchführung einer Prüfung nach dem NISG wird ein Angebot erstellt.

Nach Bestellung des Auftraggebers werden die weiteren Schritte des Zertifizierungsverfahrens terminlich und inhaltlich geplant.

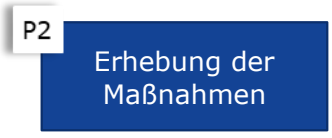
Die Beschreibung des wesentlichen Diensts (Scope) mit seinen organisatorischen und technischen Komponenten wird geprüft und allenfalls vorhanden Unklarheiten in der Scope-Beschreibung des wesentlichen Dienstes werden bereinigt.

Der vom Unternehmen bereitgestellte Netzstrukturplan des wesentlichen Dienstes wird auf Vollständigkeit und Angemessenheit geprüft.

Auf Basis der Beschreibung des wesentlichen Dienstes und des Netzstrukturplanes wird eine Liste der Systemkomponenten erstellt.

Der Prüfzeitraum für die Prüfung wird festgelegt.

Die relevanten Richtlinien und Prozessbeschreibungen zur Umsetzung der Sicherheitsvorkehrungen für den Betreiber des wesentlichen Dienstes werden ermittelt.



Gemeinsam mit dem Betreiber des wesentlichen Dienstes werden die für die NISV Prüfung relevanten Maßnahmen ermittelt und in die Prüfliste aufgenommen.

Die ermittelten Maßnahmen zur Umsetzung der Sicherheitsvorkehrungen werden auf Vollständigkeit und Angemessenheit geprüft.

Auf Basis der erhobenen Maßnahmen werden die durchzuführenden organisatorischen und technischen Prüfschritte und die Stichprobengröße festgelegt.

P3 Organisatorische Prüfung

Auf Grundlage der erhobenen Maßnahmen und festgelegten Prüfschritte wird ein Prüfplan erstellt und die organisatorische Prüfung durchgeführt und dokumentiert.

Die im Zuge der organisatorischen Prüfung gewonnenen Erkenntnisse werden genutzt, um Planung der technischen Prüfschritte zu verfeinern und zu komplementieren.

P4 Technische Prüfung

Auf Basis der erhobenen Maßnahmen und festgelegten Prüfschritte wird ein Prüfplan erstellt und die technische Prüfung durchgeführt und dokumentiert.

P5 Prüfbericht und Prüfdokumentation

Auf Grundlage der durchgeführten organisatorischen und technischen Prüfungen wird die Prüfdokumentation erstellt und die Ergebnisse der Prüfungen werden bewertet.

Gemeinsam mit dem Betreiber des wesentlichen Dienstes wird ein Prüfbericht erstellt, der sowohl die wesentlichen Erkenntnisse der durchgeführten Prüfung als auch eine Stellungnahme des Betreibers des wesentlichen Dienstes zu den Ergebnissen enthält.

Der Prüfbericht und die Prüfdokumentation werden dem Betreiber des wesentlichen Dienstes zur Weiterleitung an die Behörde übermittelt.

P6 Behördenanfragen

Wurde der Prüfbericht an die Behörde übermittelt, unterstützt der verantwortliche Prüfer das Unternehmen bei der Beantwortung von allfälligen Behördenanfragen zum Prüfbericht (optional, nach Aufwand – nicht im Angebot inkludiert)

4 Erläuterungen zur Prüfung

Antrag

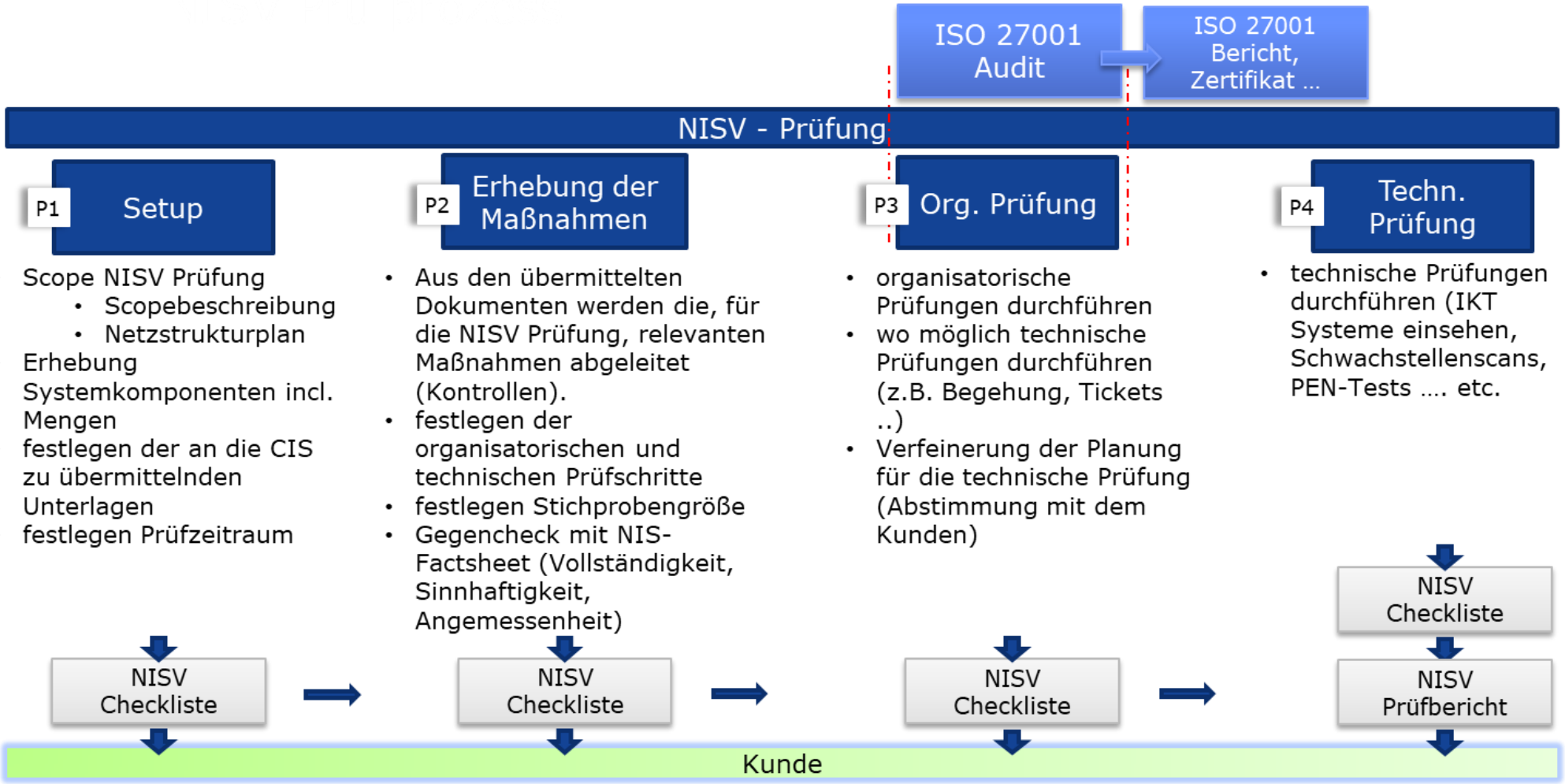
Aufgrund des Antrages wird auf Basis der Angaben ein Angebot erstellt.

(siehe Dokument Nr. d115 Angebotsanfrage für Überprüfung NISG)

Auftrag

Wird geschlossen durch Retournierung der unterfertigten Zweitschrift des Angebotes oder Bestellung.

Prüfverfahren



NISV Prüfung und ISO 27001 Audit

Die geforderten Maßnahmen zur Umsetzung der Anforderungen aus der NISV sind eine Teilmenge der Anforderungen aus der ISO 27001. Eine organisatorische NISV-Prüfung kann daher genutzt werden um auch ein Audit nach ISO/IEC 27001 durchzuführen. Voraussetzung dafür ist, dass sich der Anwendungsbereich der ISO/IEC 27001 und der Gültigkeitsbereich des wesentlichen Dienstes überschneiden. Je größer die Überschneidungen, desto größer sind die möglichen Synergien im Prüfprozess.

Zusammenhang NISV Prüfung und ISO 27001 Zertifizierung

Bereiche mit Synergien im Auditprozess

5 Mitgeltende Unterlagen

Allgemeine Bedingungen für Dienstleistungen der CIS – Certification & Information Security Services GmbH.

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

Autoren

Erich Scheiber

Robert Jamnik

Klaus Veselko