Hinweise zum Fördergegenstand Basisabsicherung (Zwischenstufe)/IT-Grundschutz-Profil für Kommunen nach Nr. 2 Satz 2 Buchst. d) ISMSR vom 7. März 2022, Az. E5-1681-7-10 für Antragsteller und Dienstleister bzw. Auditoren

Überprüfung der vollständigen Implementierung

Kreis möglicher Auditoren

Die Umsetzung und Überprüfung der vollständigen Implementierung nach den Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist zwingende Voraussetzung für die Gewährung einer Zuwendung (vgl. Nr. 4 ISMS-R).

Die Überprüfung der vollständigen Implementierung hat grundsätzlich durch einen zugelassenen Grundschutzauditor zu erfolgen. Wird durch die Kommune im jeweiligen Umsetzungsprojekt auf das Testat-Verfahren verzichtet, kann die Bescheinigung der vollständigen Implementierung einer Basis-Absicherung nach IT-Grundschutz von einem für ISO/IEC27001 zertifizierten Auditor als Nachweis i.S. Nr. 6.6.1 ISMS-R anerkannt werden.

Um die Neutralität zu gewährleisten, hat die Auditierung durch einen nicht mit der Beratung und Begleitung bei der Implementierung gem. Nr. 5.2 Buchst. a ISMSR für die geförderte Maßnahme betrauten Auditor zu erfolgen.

Prüfschema „IT-Grundschutz-Profil für Kommunalverwaltungen“

Für die Erteilung eines Testats bzw. die Überprüfung der vollständigen Implementierung prüft der Auditor die übermittelten Referenzdokumente und auditiert in einer Vor Ort Prüfung die Erfüllung der Basis-Anforderungen.

Jeder Prüfung muss ein dokumentierter Prüfplan zugrunde liegen. Eine komplette Prüfung des gesamten Informationsverbundes ist in der Regel nicht mit wirtschaftlich vertretbarem Aufwand möglich. Daher muss der Prüfer eine angemessene Stichprobenauswahl im Prüfplan nach Maßgabe des BSI-Prüfschemas festlegen.

Für die praktische Durchführung hat das BSI am 11.04.2022 die Version 2.0 des Prüfschemas für die Erteilung eines Testats nach der Basis-Absicherung gemäß IT-Grundschutz (Anlage 1) veröffentlicht und darin folgende Rahmenbedingungen für die Vor-Ort-Prüfung festgelegt:

•Es werden ca. 10% der modellierten Bausteine (aber mindestens 6 Bausteine) auditiert, darunter zwingend der Baustein ISMS.1 Sicherheitsmanagement.

•Der Auditor wählt die Bausteine und die Zielobjekte risikoorientiert aus und begründet die Auswahl kurz. Hierbei sollten aus allen modellierten Schichten jeweils mindestens ein Baustein überprüft werden.

•Der Auditor kann die Stichprobe erweitern.

•Die Basis-Absicherung fordert keine Durchführung einer Risikoanalyse. Daher wird in der Regel bei der Testat-Prüfung eine ggf. vorhandene Risikoanalyse nicht betrachtet oder geprüft.

Weitere Konkretisierungen zur Prüftiefe ergeben sich aus den im Prüfschema aufgeführten Referenzdokumenten (vgl. Seite 2 – letzter Absatz – Prüfungsgrundlagen), insbesondere dem Leitfaden zur Basis-Absicherung nach IT-Grundschutz (Anlage 2).

Die Prüftiefe für die Erteilung eines Testats nach der Basis-Absicherung gemäß IT-Grundschutz ist durch obige Dokumente verbindlich definiert.

Angebotserstellung „Audit für eine Basis-Absicherung“

Für eine Angebotserstellung durch den IT-Dienstleister hat das BSI in seinem Prüfschema folgendes Berechnungsbeispiel (anhand von Aufwandsschätzungen) zur Orientierung aufgenommen:

Ein kleiner Zulieferer mit 30 Mitarbeitern, der Bauteile für die Produktion von Gütern produziert, könnte mit folgen Prüfaufwand rechnen:

Aufgaben	**Umfang**
Dokumentenprüfung und Erstellung des Prüfplans	ca. 0,5 bis 1 PT
Vor-Ort-Prüfung und Abschlussbesprechung	1 PT
Erstellung des Prüfberichtes und Ausstellung des Testats nach Basis-Absicherung	ca. 0,5 PT
Summe	**2 – 2,5 PT**

Dieses Rechenbeispiel sollte sich auf kleine und mittlere Kommunen übertragen lassen. Selbst bei großen Kommunen oder Kommunalunternehmen sollten die Aufwände maximal 5 Personentage betragen. Mit einer Förderung von Audits (Leistungen nach Nr. 5.2.1 Buchst. c) bis maximal 6.000 Euro (brutto) (vgl. Nr. 5.2.4 ISMS-R) stehen hier - auch für größere ISMS-Projekte - ausreichend Fördermittel zur Verfügung.