Bundesamt
für Sicherheit in der
Informationstechnik

Hinweis für Zertifizierungsstellen von sektorspezifischen Managementsystemen basierend auf ISO/IEC 27001

MS-ExternZert

Änderungshistorie

Version	Datum	Name	Beschreibung
1.01	15.07.2016	Dr. Kreutzmann	Initiale Version

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: tr-zertifizierung@bsi.bund.de
Internet: https://www.bsi.bund.de

Vorwort des Abteilungspräsidenten

Die Bedeutung der Sicherheit von informationsverarbeitenden Systemen nimmt stetig zu. Dabei führen punktuelle Ansätze durch einzelne Maßnahmen zur Absicherung von einzelnen IT-Systemen nicht zum Ziel, notwendig ist ein systematischer Ansatz, der die Informationsverarbeitung in dem Umfeld der jeweiligen Organisation betrachtet. Es wird ein Informationssicherheitsmanagementsystem (im Folgenden ISMS) benötigt, das zum einen flexibel in die jeweilige Organisation mit ggf. bereits bestehenden weiteren Managementsystemen eingepasst werden kann und zum anderen dessen Erfüllung bei Bedarf auch Dritten gegenüber durch eine Zertifizierung nachgewiesen werden kann.

Durch sein Ökosystem an unterstützenden Normen und seine faktisch weltweite Anerkennung bildet die ISO/IEC 27001 eine sehr gute Grundlage für das ISMS einer Organisation. Hierzu gehört insbesondere auch die Umsetzung der »High Level Structure« (einer identischen Struktur und gemeinsamer Text aller überarbeiteten und neuen Managementsystemnormen), die eine Integration in weitere Systeme wie z. B. die ISO 9001 deutlich erleichtert.

Der generische Ansatz erschwert es auf der anderen Seite aber auch, bestimmte Sicherheitsmaßnahmen und konkrete Sicherheitsanforderungen einer Branche als minimale (und damit verbindliche) Anforderungen zu definieren und deren Umsetzung (z. B. im Rahmen einer Zertifizierung) zu dokumentieren.

Auf internationaler Ebene wird die Erstellung eines solchen branchen- oder sektorspezifischen Standards durch die in Kürze fertiggestellte ISO/IEC 27009 beschrieben. Konkrete Umsetzungen solcher Standards werden auch durch das BSI in enger Abstimmungen mit den interessierten Kreisen als „Technische Richtlinien“ (TR) entwickelt, z. B.:

- legt die „Smart Meter Gateway Administration (BSI TR-03109-6)“ die für den sicheren, technischen Betrieb des intelligenten Messsystems benötigten einheitliche organisatorische und technische Mindestanforderungen zur Durchsetzung der Informationssicherheit fest. Für alle Marktteilnehmer, die die Aufgaben des Administrators selbst wahrnehmen oder als Dienstleister für Dritte anbieten möchten, ist damit ein vergleichbares Maß an Informationssicherheit gewährleistet. Beispielsweise werden konkrete Schutzmechanismen für private Schlüssel in Kryptomodulen, die Umsetzung von Speicher- und Löschfristen personenbezogener Daten sowie die Absicherung eines Firmware-Update-Prozesses gefordert.
- erweitert die „Secure E-Mail Transport (BSI TR-03108)“ das ISMS eines E-Mail-Diensteanbieters um spezifische fachliche Anforderungen an den Betrieb eines E-Mail-Dienstes. So wird etwa die Nutzung von DANE (DNS-based Authentication of Named Entities) zum automatisierten Austausch von kryptographischen Informationen und die Nutzung hochwertiger kryptographischer Algorithmen gefordert, um das Zustandekommen von sicheren Verbindungen innerhalb der E-Mail-Infrastruktur insgesamt zu fördern.

Das vorliegende Konzept beschreibt, wie die verschiedenen beteiligten Parteien (BSI, akkreditierte Zertifizierungsstellen) zusammenspielen, um die Umsetzung solcher branchen- oder sektorspezifischen Vorgaben in einer Organisation durch ein Zertifikat nachzuweisen.

Bernd Kowalski, Abteilungspräsident der Abteilung S des BSI

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Im Bereich der Zertifizierung von Managementsystemen bietet das BSI für einige Geltungsbereiche die Zertifizierung selbst an (z. B. für ISO 27001 auf der Basis von IT-Grundschutz), bei anderen Geltungsbereichen dagegen erstellt das BSI nur die Vorgaben (derzeit als Technische Richtlinien,zukünftig ggf.. auch in anderen Formen), ohne jedoch Zertifizierungen selbst durchzuführen[1]. In Ausnahmefällen (in der Regel bei Vorliegen eines hoheitlichen Interesses) behält sich das BSI das Recht vor, auch bei der zweiten Gruppe bei einzelnen Verfahren die Zertifizierung durchzuführen.

Für diese zweite Gruppe von Geltungsbereichen besteht damit die Möglichkeit, dass andere, akkreditierte Zertifizierungsstellen diese in ihr Zertifizierungsportofolio aufnehmen.

Dieses Dokument richtet sich an solche Zertifizierungsstellen und beschreibt die Rahmenbedingungen, die für eine derartige Zertifizierung zu beachten sind.

Weitergehende Informationen zu den Geltungsbereichen finden sich unter
https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Managementsystemzertifizierung_node.html

1 Es gibt auch Geltungsbereiche, in denen das BSI ein ISO 27001-Zertifikat auf Basis von IT-Grundschutz selber anbietet, aber parallel auch eine hier beschriebene sektorspezifische ISMS-Zertifizierung bei einer anderen Zertifizierungsstelle möglich ist.

2 Konzeptioneller Aufbau

2.1 Übersicht

In Abbildung 1 ist dargestellt, wie das System aufgebaut ist und in welcher Beziehung die Beteiligten stehen.

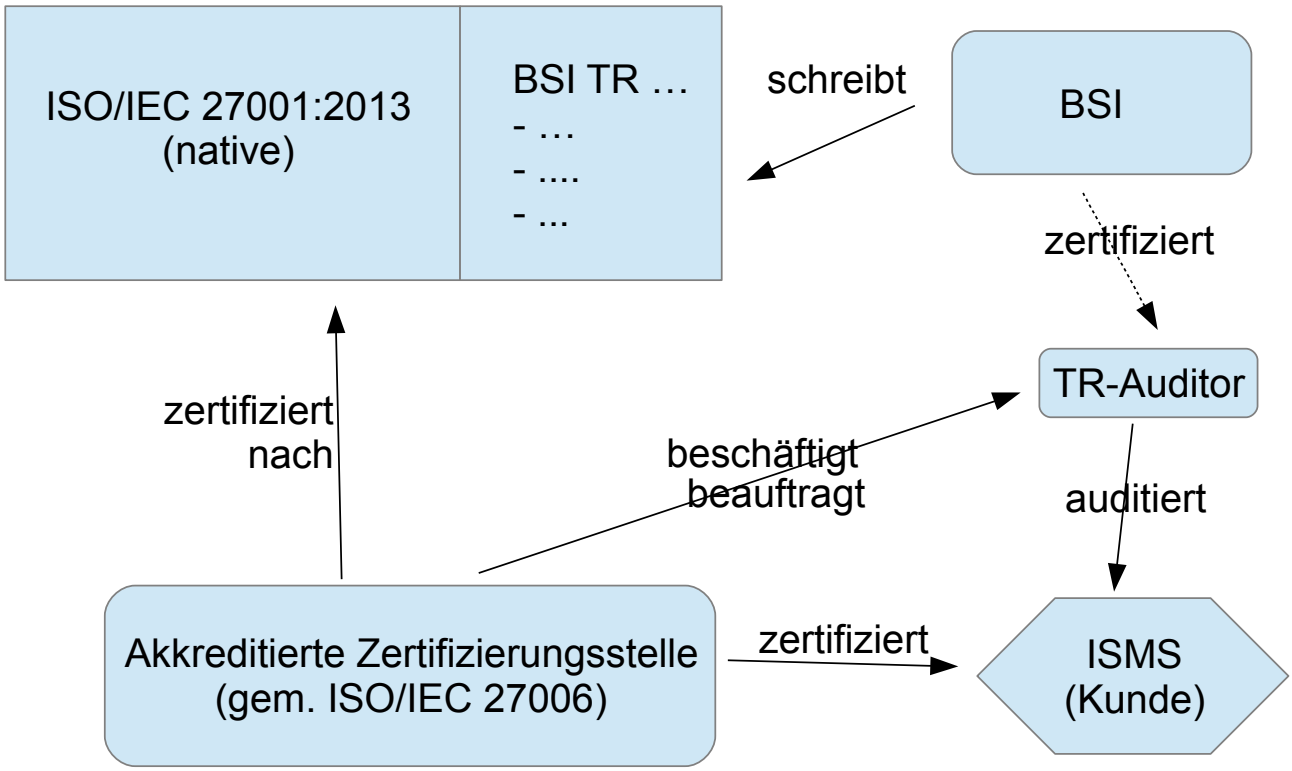

Abbildung 1: Relation der beteiligten Parteien bei der hier beschriebenen sektorspezifischen ISMS-Zertifizierung

Die Zertifizierungsgrundlage besteht aus zwei Teilen: der ISO/IEC 27001[ISO27001] sowie einer durch das BSI veröffentlichten Technischen Richtlinie (TR), die bestimmte Aspekte der ISO/IEC 27001 für einen bestimmten Geltungsbereich (Branche, Sektor, ..) konkretisiert.

Im Rahmen der Erstellung der Technischen Richtlinie werden auch die Prüfvorgaben und die Anforderungen an die Auditoren erstellt. Interessierte Auditoren können für die Prüfung einer bestimmten TR eine Personenzertifizierung beim BSI beantragen. Diese Auditoren werden im Folgenden generalisierend TR-Auditoren genannt. Diese Zertifizierung weist die Kompetenz der TR-Auditoren für die Prüfung der jeweiligen TR nach.

Die Zertifizierung des Geltungsbereichs einer Organisation erfolgt dann grundsätzlich gemäß der mit der Akkreditierungsstelle abgestimmten Vorgehensweise der Zertifizierungsstelle für ISO 27001-Zertifizierungen. Hierbei gilt u.a. die ISO/IEC 27006[ISO27006]. Ergänzend erfolgen dann durch den zertifizierten TR-Auditor die Prüfungen gemäß der jeweiligen Prüfvorgaben zu der TR (falls vorhanden) bzw. deren Umsetzung.

Im Anschluss an das Audit kann die Zertifizierungsstelle bei Erfüllen der Voraussetzungen das Zertifikat gemäß ISO/IEC 27001 ergänzt um die TR ausstellen.

Für die Überwachung des Zertifikats und die Rezertifizierung gelten dann ebenfalls die Regeln der Zertifizierungsstelle für die ISO/IEC 27001 ergänzt um die Prüfvorgaben (sofern vorhanden) für die jeweilige TR.

2.2 Zertifizierung der TR-Auditoren

Für die jeweilige TR bietet das BSI eine Personenzertifizierung an. Details hierzu sind in der jeweils gültigen Fassung vom Programm Personen[ProgPersonen] beschrieben, die über den Webauftritt des BSI verfügbar ist.

Hinweis: Aufgrund der derzeit laufenden Umstrukturierung der Dokumentation wird sich der Name des zuständigen Personenzertifizierungsdokuments in Kürze ändern.

2.3 Informationsaustausch mit dem BSI

2.3.1 Informationen vom BSI

Sofern die Zertifizierungsstelle dies wünscht, kann sie in einen Verteiler über Informationen zu der jeweiligen TR aufgenommen werden, sofern dieser existiert. Die Art und der Umfang der bereitgestellten Informationen legt das BSI nach sachlicher Notwendigkeit fest.

Unabhängig von der Teilnahme an diesem Verteiler ist allerdings die Zertifizierungsstelle dafür verantwortlich, jeweils die aktuelle Fassung der TR und der Prüfvorgabe für die TR zu verwenden.

2.3.2 Informationen an das BSI

Die Zertifizierungsstelle kann auf freiwilliger Basis dem BSI Informationen zu den Erfahrungen bei der jeweiligen TR-Zertifizierung übersenden. Sofern das BSI die Zertifizierungsstelle nach solchen Informationen fragt, ist eine Antwort stets freiwillig.

2.4 DAkkS-Akkreditierung der jeweiligen sektorspezifischen ISMS-Zertifizierung

Die Akkreditierung der jeweiligen sektorspezifischen ISMS-Zertifizierung ist prinzipiell denkbar, aber grundsätzlich nicht vorgesehen. Sofern hierzu ein Bedarf im Markt identifiziert wird, bittet das BSI hierzu um Rückmeldung, um den Bedarf prüfen zu können und ggf. ein Zertifizierungsschema für die Akkreditierung bei der DAkkS zu entwickeln. Grundsätzlich ist zudem geplant, künftig geeignete TRs gemäß den Vorgaben der ISO/IEC 27009[ISO/IEC 27009] zu entwickeln.

2.5 Zertifizierungen ohne 27001-Anteil

Für einige Geltungsbereiche kann die jeweilige TR auch die Möglichkeit vorsehen, dass die Zertifizierung auch ohne eine zugrundeliegende 27001-Zertifizierung erfolgt. In diesem Fall ist die Vorgehensweise durch die Zertifizierungsstelle entsprechend anzupassen und zu dokumentieren, sofern in der jeweiligen TR keine ergänzenden Regelungen zur Vorgehensweise sind.

Im Anschluss an das Audit kann die Zertifizierungsstelle bei Erfüllen der Voraussetzungen das Zertifikat gemäß dieser TR ausstellen.

Anhang

Anhang 1 – Nutzungsbedingungen TR-Siegel

Bei einem Verweis auf die Tatsache, dass eine Zertifizierung durch Sie nach Technischen Richtlinien (entsprechend der jeweiligen Prüfvorgaben und unter Einsatz geeigneter Auditoren) erfolgt und erfolgt ist, dürfen Sie das TR-Siegel (siehe Abbildung 2) verwenden. Das Siegel mit der Endung RGB ist optimiert für die Darstellung am Bildschirm, das Siegel mit der Endung CMYK ist optimiert für den Druck.

Das Siegel darf nur im Gesamten verwendet werden, das Herauslösen von Einzelkomponenten ist nicht erlaubt. Das Siegel darf nur in der Originalgröße verwendet werden.

Wollen Sie Links auf BSI-Inhalte setzen (z. B. auf die Liste der Technischen Richtlinien des BSI), sind Sie selbst dafür verantwortlich, dass Ihre Links dem aktuellen Stand entsprechen. Weitere Informationen über die Verlinkung auf das BSI erfahren Sie unter
https://www.bsi.bund.de/DE/Service/Benutzerhinweise/benutzerhinweise_node.html

Sollte für Messen etc. ein größeres Ausgabeformat vonnöten sein, so bitten wir um erneute Kontaktaufnahme mit dem BSI.

Abbildung 2: Muster für ein TR-Siegel

Literaturverzeichnis

[ISO27001] DIN ISO/IEC 27001:2015-03 Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Anforderungen, Beuth-Verlag

[ISO27006] ISO/IEC 27006:2015-10 Informationstechnik- IT-Sicherheitsverfahren – Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managmentsystemen anbieten, Beuth-Verlag

[ProgPersonen] Programm zur Kompetenzfeststellung und Zertifizierung von Personen, Bundesamt für Sicherheit in der Informationstechnik

[ISO/IEC 27009] ISO/IEC 27009:2016:07 Informationstechnik – IT-Sicherheitsverfahren – sektorspezifische Anwendung der ISO/IEC 27001 – Anforderungen, Beuth-Verlag

Stichwort- und Abkürzungsverzeichnis

IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ISMS	Informationssicherheitsmanagementsystem
MS	Managementsystem
TR	Technische Richtlinie (hier: des BSI)