Wissensanforderungen an das Personal von Akkreditierungsstellen im Bereich Informationssicherheits-Managementsysteme (ISO/IEC 27001)

(Deutsche Übersetzung des IAF Dokumentes „*IAF MD 13:2023*“)

IAF MD 13:2023 | Revision 2 | 14. Juni 2023 | Datum der Übersetzung: 06.09.2023

Die Übersetzung dieses Dokuments dient lediglich der Information und Arbeitserleichterung.

Können die deutsche Übersetzung und die englische Originalfassung unterschiedlich ausgelegt werden, gilt bei Zweifelsfällen das englische Original als verbindlich.

Gemäß § 2 i.V.m. § 3 Nr. 9 BGleiG ist § 4 Abs. 3 BGleiG nicht direkt auf die DAkkS anwendbar. In diesem Dokument wird im Interesse der Lesbarkeit für Funktionsbezeichnungen auch das generische Maskulinum verwendet, soweit eine konkrete Ansprache nach dem natürlichen Geschlecht nicht sinnvoll möglich ist und das natürliche Geschlecht unwichtig ist oder männliche und weibliche Personen gleichermaßen gemeint sind.

DAkkS-Regeln und sonstige technische Spezifikationen müssen problemlos lesbar sein und dürfen deshalb keine Schrägstriche enthalten, was eine Benutzung des Binnen-/s und Doppelbezeichnungen ausschließt (vgl. zur Zulässigkeit § 115 Handbuch der Rechtsförmlichkeit). Es gelten daneben die weiteren Anforderungen der DIN 820-2:2012-12 Normungsarbeit - Teil 2: Gestaltung von Dokumenten (ISO/IEC-Direktiven - Teil 2:2011) für die Formulierung technischer Spezifikationen.

Die International Accreditation Forum, Inc. (IAF) erleichtert den Handel und unterstützt die Industrie und Regulierungsbehörden durch eine weltweite Vereinbarung über gegenseitige Anerkennung zwischen Akkreditierungsstellen (AS), damit die Ergebnisse, die von den durch die IAF-Mitglieder akkreditierten Konformitätsbewertungsstellen (KBS) ausgegeben werden, weltweit akzeptiert werden.

Akkreditierung verringert das Risiko für Unternehmen und ihre Kunden, indem sie diesen versichert, dass die akkreditierten Konformitätsbewertungsstellen (KBS) kompetent sind, die Arbeiten auszuführen, die sie in ihrem Akkreditierungsbereich vornehmen. Von Akkreditierungsstellen (AS), die Mitglied bei IAF sind und dessen akkreditierten KBS wird gefordert, entsprechende internationale Normen und verbindliche IAF-Dokumente einzuhalten, um eine einheitliche Anwendung dieser Normen zu garantieren.

AS, die Unterzeichner der Multilateralen Anerkennungsvereinbarung (MLA) von IAF sind, führen regelmäßig gegenseitige Evaluierungen durch, um Vertrauen in die Tätigkeiten im Rahmen ihrer Akkreditierungsprogramme sicher zu stellen. Die Struktur des IAF MLA ist in *IAF PL 3 – Policies and Procedures on the IAF MLA Structure and for Expansion oft he Scope of the IAF MLA* [Richtlinien und Verfahren zur Struktur des IAF MLA und zur Erweiterung des Geltungsbereichs des IAF MLA] im Einzelnen erläutert.

Das IAF MLA ist in fünf Ebenen strukturiert: Ebene 1 spezifiziert verbindliche Kriterien, die für alle AS gelten, ISO/IEC 17011. Die Kombination aus Tätigkeiten der Ebene 2 und dem/der entsprechenden normativen Dokument(e) der Ebene 3 wird als MLA-Haupt-Scope bezeichnet, und die Kombination aus Ebene 4 (sofern anwendbar) und den entsprechenden normativen Dokumenten der Ebene 5 wird als MLA-Sub-Scope bezeichnet.

- Der MLA-Haupt-Scope beinhaltet Aktivitäten, wie z. B. die Produktzertifizierung und die dazugehörenden verbindlichen Dokumente, wie z. B. ISO/IEC 17065. Bescheinigungen/Zertifikate von KBSen auf der Ebene des Haupt-Scopes gelten als gleichermaßen vertrauenswürdig.
- Der MLA-Sub-Scope beinhaltet Anforderungen an die Konformitätsbewertungen, wie z. B. ISO 9001 und, sofern zutreffend, programmspezifische Anforderungen, z. B. die ISO TS 22003-1. Bescheinigungen/Zertifikate von KBSen auf der Ebene des Sub-Scopes gelten als äquivalent.

Das IAF MLA liefert das Vertrauen, welches für die Akzeptanz der Ergebnisse von Konformitätsbewertungen auf dem Markt erforderlich ist. Ein(e) Zertifikat/Bescheinigung im Geltungsbereich des IAF MLA, ausgestellt von einer KBS, die durch eine AS, die Unterzeichner des IAF-MLA ist, akkreditiert wurde, kann weltweit anerkannt werden. Dadurch wird der internationale Handel unterstützt.

Inhaltsverzeichnis

1 GELTUNGSBEREICH 5

2 NORMATIVE VERWEISE 5

3 BEGRIFFE UND DEFINITIONEN 6

4 WISSENSANFORDERUNGEN 6

ANHANG A (Normativ) Wissensanforderungen an das Personal von Akkreditierungsstellen, das an der Akkreditierung von ISMS-Zertifizierungsstellen beteiligt ist 7

Ausgabe 2, Version 3
Erarbeitet durch: IAF Technical Committee
Genehmigt durch: IAF-Mitglieder
Ausgabedatum: 14. Juni 2023
Datum: 22. November 2020
Anwendungsdatum: 03. Dezember 2020
Kontaktperson für Anfragen:
Elva Nilsen
Corporate Secretary IAF
Telefon: +1 613 454-8159
E-Mail: secretary@iaf.nu

Einführung in verbindliche IAF-Dokumente

Der Begriff „sollte“ wird in diesem Dokument verwendet, um anerkannte Möglichkeiten zur Einhaltung der Anforderungen der Norm aufzuzeigen. Eine Akkreditierungsstelle (AS) kann diese Anforderungen in gleichwertiger Art einhalten. Der Begriff „müssen“ wird in diesem Dokument verwendet, um diejenigen Bestimmungen aufzuzeigen, die die Anforderungen der relevanten Norm widerspiegeln und verbindlich sind.

Wissensanforderungen an das Personal von Akkreditierungsstellen im Bereich Informationssicherheitsmanagementsysteme (ISO/IEC 27001)

1 GELTUNGSBEREICH

Dieses Dokument definiert die spezifischen Wissensanforderungen an das Personal von Akkreditierungsstellen, das an der Akkreditierung von Zertifizierungsstellen, die Informationssicherheits-Managementsysteme (ISMS) nach ISO/IEC 27001 auditieren und zertifizieren, beteiligt ist.

Ziel dieses Dokuments ist es, Akkreditierungsstellen die Harmonisierung der Anwendung von Abschnitt 6.1.2.1 der Norm ISO/IEC 17011:2017 für die Akkreditierung von Stellen, die Audits und Zertifizierungen gemäß ISO/IEC 27001 durchführen, zu ermöglichen.

2 NORMATIVE VERWEISE

In Bezug auf dieses Dokument gelten die normativen Verweise aus ISO/IEC 17011 sowie die nachstehenden normativen Verweise. Bei datierten Verweisen gilt nur die angegebene Ausgabe. Bei undatierten Verweisen gilt die neueste Ausgabe des Dokuments einschließlich etwaiger Änderungen.

ISO/IEC 17011:2017 Konformitätsbewertung - Anforderungen an Akkreditierungsstellen, die Konformitätsbewertungsstellen akkreditieren.

ISO/IEC 17021-1:2015 Konformitätsbewertung - Anforderungen an Stellen, die Managementsysteme auditieren und zertifizieren - Teil 1: Anforderungen

ISO/IEC 27006 Informationstechnik - IT-Sicherheitsverfahren - Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managementsystemen anbieten

ISO/IEC 27001:2013 Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen

ISO/IEC 27000 Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Überblick und Terminologie

ISO/IEC 27007:2020 Informationssicherheit, Cybersicherheit und Datenschutz – Leitfaden für das Auditieren von Informationssicherheitsmanagementsystemen

ISO/IEC TS 27008:2019 Information technology – Security techniques – Guidelines for the assessment of information security controls (Informationstechnik - Sicherheitsverfahren - Leitfaden zur Bewertung von Informationssicherheitsmaßnahmen)

ISO/IEC 27005:2018 Information technology – Security techniques – Information security risk management (Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement)

3 BEGRIFFE UND DEFINITIONEN

In Bezug auf dieses Dokument gelten die Begriffe und Definitionen gemäß ISO/IEC 17011 und ISO/IEC 27000.

4 WISSENSANFORDERUNGEN

4.1 ISO/IEC 17011 Abschnitt 6.1.2.1 verlangt von Akkreditierungsstellen die Beschreibung der erforderlichen Kompetenzen für jede Aktivität des Akkreditierungsprozesses. Der normative Anhang A dieses Dokuments legt die Wissensgebiete fest, die die Akkreditierungsstelle für bestimmte Funktionen definieren muss, die Teil der Akkreditierung von Stellen sind, die ISMS auditieren und zertifizieren. Die in diesem Anhang aufgeführten Wissensanforderungen ergänzen die allgemeinen fachlichen Qualifikationen, die für die jeweilige Funktion innerhalb einer Akkreditierungsstelle erforderlich sind und die in ISO/IEC 17011 definiert werden.

4.2 Im Allgemeinen muss jeder Begutachter, der an der Begutachtung von ISMS beteiligt ist, jeweils über die in Anhang A unter A1 bis A5 beschriebenen Kenntnisse verfügen. Die unter A6 und A7 beschriebenen Kenntnisse stellen Anforderungen an das Team als Ganzes dar.

4.3 Zu den Prozessen und Verfahren von Kunden der Konformitätsbewertungsstelle (KBS) in Bezug auf ISMS gehören:

- typische Geschäftstätigkeiten mit Bezug auf den technischen Bereich (siehe ISO/IEC 17021-1:2015, Abschnitt 7.1.2);
- für den technischen Bereich spezifische Informations- und Kommunikationstechnik;
- für den technischen Bereich spezifische Informationssicherheitstechnologien und -praktiken, insbesondere die Ermittlung von Bedrohungen und Schwachstellen mit Bezug auf die Informationssicherheit sowie damit verbundene Maßnahmen zur Minimierung und Kontrolle;
- entsprechende rechtliche Anforderungen.

Die hier aufgeführten rechtlichen Anforderungen sind diejenigen Vorschriften, deren Erfüllung von der Organisation, die Gegenstand des Witness-Audits ist, auf dem Gebiet der Informationssicherheit, auf dem sie tätig ist, oder in dem Staat/Bundesland/Provinz, in dem/der sie tätig ist, erwartet wird.

Ende des verbindlichen IAF-Dokuments „Wissensanforderungen an das Personal von Akkreditierungsstellen, das an der Akkreditierung von Zertifizierungsstellen, die Informationssicherheits-Managementsysteme (ISMS) nach ISO/IEC 27001 auditieren und zertifizieren, beteiligt ist“.

ANHANG A
(Normativ)
Wissensanforderungen an das Personal von Akkreditierungsstellen, das an der Akkreditierung von ISMS-Zertifizierungsstellen beteiligt ist

In der nachstehenden Tabelle sind die Kenntnisbereiche festgelegt, die eine Akkreditierungsstelle für bestimmte Tätigkeiten im Rahmen der Akkreditierung von ISMS-Zertifizierungsstellen definieren muss.

Akkreditierungs-funktionen / **Thema**	**Dokumenten-prüfung**	**Begutachtung der Geschäfts-stelle**	**Witness-Begutachtung**	**Prüfung von Begutachtungsberichten und Treffen von Akkreditierungs-entscheidungen**	**Management von Akkreditierungsprogrammen**
A1. Terminologie und Grundlagen mit Bezug auf ISMS, einschließlich ISO/IEC 27000	X	X	X	X	X
A2. In ISO/IEC 27007 und ISO/IEC TS 27008 enthaltene Auditverfahren		X	X		
A3. ISO/IEC 17021-1 und ISO/IEC 27006	X	X	X	X	X
A4. ISO/IEC 27001	X	X+	X	X	X
A5. Allgemeine rechtliche und behördliche Anforderungen mit Bezug auf ISMS	X	X	X	X	
A6. Allgemeine Technologien mit	X	X	X	X	

Bezug auf ISMS, darunter - Informationssicherheitstechnologien und -praktiken - Informations- und Kommunikationstechnik - Risikobeurteilung und Risikomanagement, wie z. B. ISO/IEC 27005.					
A7. Prozesse und Verfahren von Kunden der Konformitätsbewertungsstelle (KBS) in Bezug auf ISMS			X		

Weitere Informationen:

Wenn Sie weitere Informationen zu diesem oder anderen IAF-Dokumenten benötigen, wenden Sie sich an ein Mitglied des IAF oder an das Sekretariat des IAF.

Die Kontaktdaten der IAF-Mitglieder finden sich auf der Website des IAF: http://www.iaf.nu.

Sekretariat:

Elva Nilsen
IAF Corporate Secretary
Telefon + 1 (613) 454-8159
E-Mail: secretary@iaf.nu