



Bundesamt  
für Sicherheit in der  
Informationstechnik

## **Vertrag zur Zertifizierung als Auditteamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz**

zwischen der

**Bundesrepublik Deutschland,**

vertreten durch das  
Bundesministerium des Innern,

vertreten durch das  
Bundesamt für Sicherheit in der Informationstechnik,

Godesberger Allee 185 - 189  
53 175 Bonn

- im folgenden BSI -

und dem Auditteamleiter

**Knud Brandis**

wohnhaft in

Puschkinallee 17

14469 Potsdam

- im folgenden Auditteamleiter -

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63

53133 Bonn

Tel.: +49 22899 9582-0

E-Mail: [auditor@bsi.bund.de](mailto:auditor@bsi.bund.de)

Internet: <https://www.bsi.bund.de>

© Bundesamt für Sicherheit in der Informationstechnik 2013

## § 1 Geltungsbereich des Vertrags

Der Auditteamleiter hat ausreichende Fachkunde und Erfahrung im Bereich Informationssicherheit und IT-Grundschutz sowie Kenntnisse der Vorgehensweise zur Durchführung von ISO 27001-Audits auf der Basis von IT-Grundschutz nachgewiesen.

Er ist berechtigt, unter der Zertifikatsnummer **BSI-ZIG-0093-2018** die Bezeichnung

„Zertifizierter Auditteamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz“

zu führen und damit ISO 27001-Auditberichte auf der Basis von IT-Grundschutz zu erstellen.

Zur Sicherstellung der Qualität und Vergleichbarkeit der Prüfverfahren und Prüfergebnisse wird Folgendes vereinbart:

## § 2 Einhaltung von Regelungen, Mitteilungspflicht

- (1) Der Auditteamleiter verpflichtet sich, die Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen nebst dem Programm zur Kompetenzfeststellung und Zertifizierung von Personen, die Verfahrensbeschreibung „Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Zertifizierungsschema“ sowie die Verfahrensbeschreibung „Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Auditierungsschema“, welche als Anlagen 1 bis 3 zum Bestandteil dieses Vertrages gemacht werden, in der jeweils gültigen, auf der Internetseite des BSI veröffentlichten Fassung, einzuhalten und anzuwenden. Da sich die Verpflichtung auf die jeweils gültige Fassung bezieht und diese sich während der Vertragslaufzeit ändern kann, ist der Auditteamleiter verpflichtet, sich regelmäßig auf der Internetseite des BSI darüber zu informieren, ob Änderungen vorgenommen wurden. Er ist verpflichtet, das BSI unverzüglich schriftlich zu unterrichten, sobald die Einhaltung der Pflichten aus Satz 1 und 2 nicht mehr gewährleistet werden kann.
- (2) Der Auditteamleiter verpflichtet sich, keine Audits für Stellen durchzuführen, bei denen er beratend tätig geworden ist oder werden wird. Jegliche frühere, derzeitige oder geplante Beziehung zu dieser Stelle außerhalb der Audittätigkeit ist dem BSI frühestmöglich mitzuteilen.
- (3) Dem Auditteamleiter wird ein Zertifikat zur Verfügung gestellt. Der Auditteamleiter darf mit Zertifikat nur für seine Tätigkeit als Auditteamleiter werben. Er verpflichtet sich, das Zertifikat nicht zur Werbung für Produkte oder zur Werbung für Dienstleistungen Dritter einzusetzen. Jedoch kann er seinem Arbeitgeber gestatten, das Zertifikat zu verwenden, aber ausschließlich in Verbindung mit seinem Namen, da das Zertifikat personenbezogen ist. Das Zertifikat darf nur unverändert wiedergegeben werden. § 7 Abs. 1 Satz 3 und § 7 Abs. 4 dieser Vereinbarung bleiben unberührt.



## § 3 Tätigkeit als Auditteamleiter

- (1) Bei seiner Tätigkeit stellt der Auditteamleiter sicher, dass er dem BSI jederzeit umfassend Auskunft über Ablauf und Inhalte von Audits gibt, die er für das BSI durchführt.
- (2) Das BSI überwacht den laufenden Auditbetrieb für das BSI. Zu diesem Zweck ist es berechtigt,
  - (a) abweichende Entscheidungen von den Bewertungen in Auditberichten, die vom Auditteamleiter verfasst wurden, zu treffen, insbesondere wenn Gründe der Vergleichbarkeit der Ergebnisse anderer Audits dies erfordern,
  - (b) im Zertifikat nach eigenem Ermessen Auszüge aus dem vom Auditteamleiter vorgelegten Auditbericht ohne Quellenangabe zu verwenden,
  - (c) ein (Teil eines) Vor-Ort-Audits des Auditteamleiters zu begleiten - dies geschieht grundsätzlich einmal für einen Tag pro Vertragslaufzeit sowie bei begründeten Problemen; der Auditteamleiter hat dabei die Kosten des BSIs zu tragen.
- (3) In jedem ISO 27001-Zertifikat auf der Basis von IT-Grundschutz wird der Auditteamleiter, der das Audit durchgeführt hat, genannt.

## § 4 Auditteamleitertreffen/-Erfahrungsaustausch

Das BSI wird im Einvernehmen mit zertifizierten Auditteamleitern Arbeitstreffen zur Klärung von Grundsatz- oder Kriterienfragen durchführen. Der Auditteamleiter ist verpflichtet, an diesen Arbeitstreffen teilzunehmen. Eine unverschuldete Nicht-Teilnahme (z.B. wegen Krankheit, höherer Gewalt) ist dem BSI zeitnah mitzuteilen.

## § 5 Vertraulichkeit

- (1) Der Auditteamleiter gewährleistet die streng vertrauliche Behandlung der Interna von Audit- und Zertifizierungsverfahren, der beim Audit gewonnenen Betriebsgeheimnisse Dritter sowie aller vertraulichen Informationen und Unterlagen des BSI-Zertifizierungssystems und der hieraus gewonnenen vertraulichen Erkenntnisse. Hierzu hat er notwendige Sicherungsmaßnahmen zu treffen und diese auf Anfrage dem BSI mitzuteilen.
- (2) Er wird Beschäftigten und Dritten Informationen nur geben, soweit ihre Kenntnis notwendig („Kenntnis-nur-wenn-nötig-Prinzip“) und dies zulässig ist.

## § 6 Veröffentlichung von Daten

Das Bundesamt veröffentlicht mindestens vierteljährlich im Internet oder in anderen Medien Gesamtlisten oder seit der letzten Veröffentlichung geänderte oder hinzugefügte Listeneinträge der zertifizierten Personen mit deren Adresse, mit den technischen Geltungsbereichen der Zertifizierung und mit der Geltungsdauer der Zertifizierung.

Das Bundesamt sieht von der Veröffentlichung ab, soweit durch die Veröffentlichung die öffentliche Sicherheit beeinträchtigt werden könnte. Das Bundesamt kann von der Veröffentlichung ganz oder teilweise absehen, wenn durch die Veröffentlichung öffentliche oder private Interessen beeinträchtigt würden.

Der Auditteamleiter erklärt sich – wie beantragt – mit der Veröffentlichung der Tatsache der Zertifizierung unter Angabe der Zertifizierungsnummer und des Gültigkeitszeitraums des Zertifikats und eventueller Einschränkungen, des Namens und der Anschrift sowie des Entzugs des Zertifikats im Internet und in der Publikation „KES“ einverstanden. Änderungen dieser Daten teilt der Auditteamleiter dem BSI zeitnah mit.

Der Inhaber eines Zertifikats kann der Veröffentlichung widersprechen.

## § 7 Kündigung

- (1) Stellt das BSI fest, dass der zertifizierte Auditteamleiter
  - (a) gegen die Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen nebst dem Programm zur Kompetenzfeststellung und Zertifizierung von Personen oder
  - (b) gegen die Verfahrensbeschreibung „Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz - Zertifizierungsschema“ oder
  - (c) gegen die Verfahrensbeschreibung „Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Auditierungsschema“ oder
  - (d) gegen die vereinbarte Vertraulichkeit der Ergebnisse verstößt oder
  - (e) im Rahmen der Auditteamleiter-Überwachung Kompetenzmängel aufweist oder
  - (f) das Vertrauensverhältnis zwischen BSI und Auditteamleiter nachhaltig gestört hat oder
  - (g) verschuldet nicht am Erfahrungsaustausch und den Auditteamleitertreffen nach § 4 teilgenommen hat oder
  - (h) Zertifizierungsantrag oder Fachkundenachweise vorlegte, die unrichtig waren oder Inkorrektheiten enthielten,

wird der zertifizierte Auditteamleiter vom BSI schriftlich gemahnt. In der Mahnung wird der Grund der Mahnung mitgeteilt und eine angemessene Frist zur Beseitigung beziehungsweise Stellungnahme gesetzt. Der Auditteamleiter erhält somit Gelegenheit, sich zum Grund für die Mahnung zu äußern sowie diesen ggf. zu korrigieren und Maßnahmen zur zukünftigen Vermeidung zu ergreifen. Durchgeführte Maßnahmen sind der Personenzertifizierungsstelle des BSI schriftlich mitzuteilen und nachzuweisen.

Das BSI kann bis zur Entkräftung beziehungsweise Beseitigung des Mahnungsgrundes eine Aussetzung der Zertifizierung aussprechen, wenn dies wegen Gefahr im Verzug oder im öffentlichen Interesse notwendig erscheint. In diesem Fall ist dem zertifizierten Auditteamleiter eine Verwendung des Zertifikats und Werbung mit dem Zertifikat untersagt. Neue Projekte dürfen während der Frist zur Beseitigung beziehungsweise Stellungnahme nicht begonnen und laufende nur mit ausdrücklicher Zustimmung des BSI fortgeführt werden.

Der Auditteamleiter muss die an laufenden Projekten beteiligten Kunden schriftlich über die *Aussetzung* benachrichtigen. Kopien dieser Schreiben müssen der Personenzertifizierungsstelle des BSI spätestens 10 Kalendertage nach der Aussetzung vorliegen.

Die Aussetzung wird aufgehoben, wenn der Mahnungsgrund, der zur Aussetzung geführt hat, beseitigt wurde.

Können die Gründe, die zur Mahnung bzw. Aussetzung geführt haben, nicht fristgerecht entkräftet oder beseitigt werden, wird die Aufhebung der Zertifizierung für den Geltungsbereich ausgesprochen.

- (2) Der Auditteamleiter muss die an laufenden Projekten beteiligten Kunden schriftlich über die *Aufhebung* benachrichtigen. Kopien dieser Schreiben müssen der Personenzertifizierungsstelle des BSI spätestens 10 Kalendertage nach der Aufhebung vorliegen.
- (3) In schwerwiegenden Fällen ist auch eine sofortige Aufhebung der Zertifizierung möglich.
- (4) Bei Entzug des Zertifikats ist die Zertifikatsurkunde unverzüglich an das BSI zurückzugeben und die Bezeichnung als zertifizierter Auditteamleiter unverzüglich einzustellen.

## § 8 Gültigkeitsdauer des Zertifikats

Die Zertifizierung erfolgt für einen Zeitraum von 3 Jahren.  
Sie beginnt am 01.10.2018 und endet am 30.09.2021.

## § 9 Haftung

- (1) Schadensersatzansprüche gegenüber dem BSI sind, außer bei Vorsatz und grober Fahrlässigkeit, ausgeschlossen.
- (2) Für die wirtschaftliche Verwertbarkeit der Zertifizierung wird keine Gewähr übernommen.
- (3) Der zertifizierte Auditteamleiter verantwortet die Qualität seiner Prüfungen, Evaluierungen, Zertifizierungen und Dienstleistungen gegenüber seinen Auftragnehmern selbst.



## § 10 Sprache

Alle Unterlagen (Auditbericht, Protokolle, etc.) zu laufenden Audits mit dem Ziel eines ISO 27001-Zertifikats auf der Basis von IT-Grundschutz sind grundsätzlich in deutscher Sprache zu verfassen. Ausnahmen bedürfen der vorherigen schriftlichen Zustimmung des BSI. Auslagen für notwendige Übersetzungen sind zu erstatten.

## § 11 Auslegung

Lücken oder Widersprüche der Vereinbarung sind so auszulegen, dass die Durchführung des Verfahrens gewährleistet ist. Eine etwaige Ungültigkeit einzelner Bestimmungen berührt die Wirksamkeit im Übrigen nicht, wenn dadurch der Zweck weiterhin erreicht werden kann.

## § 12 Schriftform

Außerhalb dieser Vereinbarung und ihrer Anlagen bestehen keine weiteren Abreden. Mündliche Nebenabreden sind nicht zulässig. Künftige Änderungen oder Ergänzungen bedürfen der Schriftform, wobei diese Klausel nur schriftlich geändert werden kann.

## § 13 Abtretung

Die Abtretung der aus diesem Vertrag bestehenden Rechte und Verpflichtungen an Dritte ist nicht zulässig.

## § 14 Gerichtsstand und geltendes Recht

- (1) Ausschließlicher Gerichtsstand und Erfüllungsort für diese Vereinbarung ist Bonn.
- (2) Es gilt deutsches Recht.

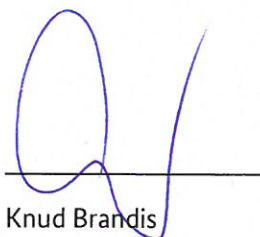
Bonn,

18.09.18



Bernd Kowalski  
Abteilungspräsident

Potsdam,



Knud Brandis

Anlagen:

1. Verfahrensbeschreibung zur Kompetenzfeststellung und Zertifizierung von Personen  
[https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Personenzertifizierung/personen\\_node.html](https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Personenzertifizierung/personen_node.html)
2. Programm zur Kompetenzfeststellung und Zertifizierung von Personen  
[https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Personenzertifizierung/Auditteamleiter/auditteamleiter\\_node.html](https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Personenzertifizierung/Auditteamleiter/auditteamleiter_node.html)
3. Verfahrensbeschreibung „Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Zertifizierungsschema“  
<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Zertifizierungsschema.html>
4. Verfahrensbeschreibung „Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Auditierungsschema“  
<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Auditierungsschema.html>

Diese Anlagen werden diesem Vertrag nicht in Papierform beigelegt. Sie sind auf der Webseite des BSI abrufbar.