



Comgroup GmbH, Certification Center Security

Zertifizierungsstelle für Informationssicherheit nach ISO/IEC 27001

Zertifizierungsregeln

**Allgemeine Bedingungen und Regeln für die Zertifizierung von
Informationssicherheitsmanagementsystemen (ISMS) nach ISO/IEC 27001**

Stand: 30.01.2012

Version 1.3

Inhaltsverzeichnis

1. Allgemeines	3
2. Geltungsbereich.....	3
3. Zertifizierungsverfahren	3
3.1 Voraussetzungen.....	3
3.2 Ablauf	4
3.3 Modulare Zertifizierung	7
4. Zertifikatsnutzung	8
5. Pflichten von CCSEC.....	9
6. Pflichten des Klienten	9
7. Einspruchsverfahren.....	10
8. Witness-Audits durch die Akkreditierungsstelle.....	10
9. Inkrafttreten.....	11



1. Allgemeines

Das Certification Center Security der Comgroup GmbH (CCSEC) wurde nach DIN EN ISO/IEC 17021 und ISO 27006:2007 unter der DAR-Registrierungsnummer TGA-ZM-10-99-20 durch die Trärgemeinschaft für Akkreditierung GmbH (TGA) akkreditiert. CCSEC bietet interessierten Unternehmen ihre Dienste zur Zertifizierung ihrer ISMS nach ISO/IEC 27001 an.

2. Geltungsbereich

Diese Prüf- und Zertifizierungsordnung regelt die Zertifizierung von ISMS nach ISO/IEC 27001 durch CCSEC.

3. Zertifizierungsverfahren

3.1 Voraussetzungen

Durch die schriftliche Annahme des Angebotes, dem dieses Dokument im Normalfall als Anlage beigefügt ist,

- schließt der Auftraggeber, nachfolgend Klient genannt, einen Zertifizierungsvertrag mit CCSEC
- erteilt er gleichzeitig damit einen Zertifizierungsauftrag
- erklärt er, dass keine weitere Zertifizierungsstelle mit der Durchführung des gleichen Verfahrens beauftragt wurde
- erkennt er diese Zertifizierungsbedingungen an.

3.2 Ablauf

Das Zertifizierungsverfahren auf Basis der DIN EN 45012 unterteilt sich in

6 Phasen:

Phase 1: Workshop

Der Workshop hat die Aufgabe, den Zertifizierungsverantwortlichen des Klienten über die Anforderungen der ISO/IEC 27001 zu unterrichten, den Auditoren Informationen über das Unternehmen zu vermitteln und die Interpretation der Norm aus Sicht der Zertifizierungsstelle darzustellen. Dabei erlangt der Klient Kenntnis über die Erwartungshaltung der Zertifizierungsstelle und somit auch eine Entscheidungsgrundlage für die Fortführung des Verfahrens. Nach dem Workshop hat der Klient die Möglichkeit des Ausstiegs aus dem Verfahren ohne dass ihm zusätzliche Kosten entstehen. In diesem Fall würden dem Klienten lediglich die Kosten für den Workshop berechnet.

Phase 2: Entwicklung und Einführung des ISMS

Der Klient führt eine strukturierte Risikoanalyse durch. Bei dieser werden seine materiellen und ideellen Werte erfasst und auf Schwachstellen hin analysiert. In einem weiteren Schritt zieht er daraus seine Schlussfolgerungen und setzt diese in entsprechende Maßnahmen um. Diese Maßnahmen werden unter Berücksichtigung der ISO/IEC 27001 eingeführt und entsprechend dokumentiert.

Die Dokumentation muss mindestens folgende Punkte umfassen:

- Allgemeine Dokumente zum ISMS-Rahmen
 - Die Aussagen des Managements in der Informationssicherheitspolitik
 - Die Definition des Anwendungsbereiches
- Dokumente zur Risikoanalyse
 - Die Beschreibung der angewandten Methodik bei der Risikoanalyse
 - Die Ergebnisse aus der Risikoanalyse
 - Der Plan zur Behandlung von Risiken

- Dokumente zum IS-Prozess
 - Die Beschreibung des Prozesses zur Einführung und Aufrechterhaltung des ISMS
 - Sicherheitsrelevante Aufzeichnungen
 - Die Verfahren und Regelungen des ISMS-Handbuchs
 - Erklärung zur Anwendbarkeit der in der Norm geforderten Regelungen (Annex A)

Phase 3: Desktop Review

Der Klient übergibt die Dokumentation des ISMS an CCSEC. Der leitende Auditor prüft daraufhin die Unterlagen auf Konformität mit der ISO/IEC 27001. Die Abweichungen werden in einem Abweichungsbericht erfasst, der dann an den Klienten zurückgesandt wird. Wurden keine Abweichungen festgestellt oder handelt es sich bei den festgestellten Abweichungen lediglich um geringfügige, also um Abweichungen, die eine Zertifizierung nicht unmöglich machen würden, kann das Audit stattfinden. Die Vorlage der überarbeiteten Dokumente vor dem Audit ist nicht erforderlich. Bei erheblichen Abweichungen hat der Klient 8 Wochen Zeit, um diese zu beseitigen, die Dokumentation entsprechend zu überarbeiten und die geänderte Fassung der Zertifizierungsstelle vorzulegen. Erst wenn die Zertifizierungsstelle keine erheblichen Abweichungen mehr feststellt, darf das Audit durchgeführt werden. Wird die 8-Wochen-Frist überschritten, so wird das Zertifizierungsverfahren durch CCSEC vorübergehend geschlossen und der bis dahin entstandene Aufwand mit dem Klienten abgerechnet. Eine Wiederaufnahme des Verfahrens kann innerhalb eines halben Jahres ab dem Datum des Abweichungsberichts durch den Klienten beantragt werden, wenn er gleichzeitig die erforderlichen Dokumente vorlegt. In diesem Fall wird das Desktop Review erneut in vollem Umfang durchgeführt. Nach Verstreichen der Halbjahresfrist ab dem Datum des Abweichungsberichts wird das Verfahren endgültig geschlossen. Im Bedarfsfall wäre dann ein neues Verfahren zu beantragen.

Phase 4: Zertifizierungsaudit

Der leitende Auditor versendet ca. 2 Wochen vor Beginn des Zertifizierungsaudits einen Auditplan. Dieser enthält Informationen über durchzuführende Tätigkeiten und den zeitlichen Ablauf. Der Klient prüft daraufhin die Machbarkeit und kann dann evtl. Änderungswünsche einbringen, die dann je nach Möglichkeit und Machbarkeit berücksichtigt werden.

Während des Audits ist es Aufgabe des Klienten, die praktische Anwendung seiner dokumentierten Verfahren zu demonstrieren und die Wirksamkeit seiner Maßnahmen unter Beweis zu stellen. Zum Abschluss des Audits wird der Klient im Rahmen eines Abschlussgesprächs über die Ergebnisse des Audits unterrichtet.

Phase 5: Berichterstellung und Zertifikatserteilung

Im Anschluss an das Audit werden die Abweichungen in einem Abweichungsbericht erfasst, der dann innerhalb von 2 Wochen an den Klienten gesandt wird. Alle erkannten Abweichungen müssen klientenseitig auf Ihre Ursachen hin analysiert werden (Ursachenanalyse). Die Ergebnisse sind zu dokumentieren und der Zertifizierungsstelle mitzuteilen.

Wurden keine Abweichungen festgestellt oder handelt es sich bei den festgestellten Abweichungen lediglich um geringfügige, also um Abweichungen, die eine Zertifizierung nicht unmöglich machen würden, teilt der Klient dem leitenden Auditor innerhalb weiterer 2 Wochen schriftlich mit, welche Maßnahmen er treffen wird oder bereits getroffen hat um die Abweichungen zu beseitigen. Daraufhin empfiehlt der leitende Auditor die Erteilung des Zertifikats. Ein Nachaudit ist in diesem Fall nicht erforderlich.

Bei erheblichen Abweichungen hat der Klient 8 Wochen Zeit, diese zu beseitigen, die Dokumentation entsprechend zu überarbeiten und die geänderte Fassung der Zertifizierungsstelle vorzulegen. Nach Ablauf dieser Zeit wird innerhalb weiterer 4 Wochen ein Nachaudit durchgeführt, das sich auf die Bereiche beschränkt, in denen die erheblichen Abweichungen festgestellt wurden. Erst wenn die Auditoren keine erheblichen Abweichungen mehr feststellen, darf die Erteilung des Zertifikats vorgeschlagen werden.

Wird die 2- (bei geringfügigen) bzw. 8-Wochen-Frist (bei erheblichen) vom Klienten überschritten, so wird das Zertifizierungsverfahren durch CCSEC vorübergehend geschlossen und der bis dahin entstandene Aufwand mit dem Klienten abgerechnet. Eine Wiederaufnahme des Verfahrens kann innerhalb eines halben Jahres ab dem Datum des Abweichungsberichts durch den Klienten beantragt werden, wenn er gleichzeitig die erforderlichen Dokumente vorlegt. In diesem Fall wird das Zertifizierungsaudit erneut in vollem Umfang durchgeführt. Nach Verstreichen der Halbjahresfrist ab dem Datum des Abweichungsberichts wird das Verfahren endgültig geschlossen. Im Bedarfsfall wäre dann ein neues Verfahren zu beantragen.

Nach positiver Prüfung der Dokumentation des Zertifizierungsverfahrens wird das Zertifikat

durch den Leiter der Zertifizierungsstelle erteilt. Das Zertifikat wird nur erteilt, wenn alle erheblichen Abweichungen behoben sind.

Phase 6: Überwachung

Die Gültigkeitsdauer des Zertifikates beträgt drei Jahre, wenn jährlich eine Überwachungsmaßnahme beim Klienten durchgeführt wird. Die Überwachungsmaßnahme kann sowohl in Form eines Desktop-Reviews als auch durch ein Audit erfolgen. Die Entscheidung hierfür trifft der Leiter der Zertifizierungsstelle auf Basis der bislang vorliegenden Projektdokumentation. Nach Ablauf des Zertifikats wird ein Rezertifizierungsaudit durchgeführt. In dem Jahr, in dem das Rezertifizierungsaudit durchgeführt wird, ist keine weitere Überwachungsmaßnahme erforderlich. Für die Aufrechterhaltung des Zertifikats gelten die Regeln für die Erstzertifizierung analog.

3.3 Modulare Zertifizierung

Um dem Klienten zwischenzeitlich zu ermöglichen, das bereits Erarbeitete nachzuweisen, auch wenn der Prozess der Gesamtzertifizierung sich verzögert, wurde durch CCSEC die Möglichkeit der modularen Zertifizierung geschaffen. Hierbei kann bereits nach der Phase 1 und einer erfolgten strukturierten Risikoanalyse, die durch CCSEC begutachtet ist, ein Zwischenzertifikat (**Level 1**) ausgestellt werden. Dieses dient als Nachweis für den Klienten, dass er eine Risikoanalyse normenkonform durchgeführt hat und sich somit seiner Risiken bewusst ist. An dieser Stelle müssen dementsprechend bereits die in Punkt 3.2 unter Phase 2 beschriebenen „Dokumente zum ISMS-Rahmen“ und die „Dokumente zur Risikoanalyse“ vorliegen.

Ein weiteres Zwischenzertifikat (**Level 2**) kann erteilt werden, wenn die Phase 3 abgeschlossen ist. Durch dieses Zertifikat wird nachgewiesen, dass der Klient (nach Dokumentenlage) ein normenkonformes ISMS dokumentiert hat.

Das 3. Zertifikat (**Level 3**) kann erteilt werden, wenn alle Anforderungen der ISO/IEC 27001 erfüllt sind (also i.d.R. nach Phase 4 + 5). Dieses Zertifikat entspricht dem akkreditierten Zertifikat und weist nach, dass der Klient ein normenkonformes ISMS eingeführt und umgesetzt hat.

Die Zwischenzertifikate für Level 1 und 2 unterliegen keiner Akkreditierung, sind nicht konform mit DIN EN 45012 und enthalten somit auch nicht die üblichen Akkreditierungsmerkmale. Die Fristen zur Beseitigung von Abweichungen in den einzelnen Phasen sowie die Notwendigkeit von

Überwachungsmaßnahmen zur Aufrechterhaltung der Zertifikate gelten für die modulare Vorgehensweise analog. Solange die Zertifikate für Level 1 oder 2 (durch Überwachungsmaßnahmen) aufrechterhalten werden, gelten keinerlei zusätzliche zeitliche Anforderungen für die Durchführung weiterer Schritte. Die Fortführung des Gesamtzertifizierungsprozesses kann in diesem Fall jederzeit erfolgen.

4. Zertifikatsnutzung

Die Berechtigung zur Nutzung des Zertifikates durch den Klienten, beispielsweise für Marketingzwecke, beschränkt sich auf den im Zertifikat benannten Geltungsbereich.

Ein Zertifikat erlischt, wenn

- die im Zertifikat genannte Gültigkeitsdauer überschritten ist
- der Klient auf das Zertifikat vor Ablauf der im Zertifikat genannten Gültigkeitsdauer verzichtet
- der Vertrag über die Zertifizierung durch den Klienten gekündigt wird
- die dem Zertifikat zugrunde gelegten Bestimmungen geändert wurden oder andere Bestimmungen, z.B. aufgrund geänderter Nutzung, anzuwenden sind.

Ein Zertifikat kann von der Zertifizierungsstelle zurückgezogen werden, wenn

- schwerwiegende Abweichungen festgestellt werden
- der Klient die vereinbarten Überprüfungen seines ISMS durch die Zertifizierungsstelle oder deren beauftragte prüfende Stelle nicht zulässt oder behindert
- in Zusammenhang mit dem Zertifikat irreführende oder anderweitig unzulässige Werbung betrieben wird
- aufgrund von Tatsachen, die einer Zertifizierung entgegenstehen würden, welche zum Zeitpunkt der Zertifikatserteilung nicht zu erkennen waren.

Die Zertifizierungsstelle kann das Erlöschen oder die Zurückziehung nach eigener Wahl veröffentlichen.

Die Zertifizierungsstelle ist berechtigt, die Aufsichtsbehörden, die Akkreditierungsstellen, andere Zertifizierungsstellen und die Zulassungsbehörden über das Erlöschen oder die Zurückziehung von Zertifikaten zu informieren.

Die Zertifizierungsstelle haftet nicht für Nachteile, die dem Klienten aus der Nichterteilung, dem Erlöschen oder der Zurückziehung eines Zertifikats erwachsen.

5. Pflichten von CCSEC

CCSEC verpflichtet sich, alle ihm zugänglich gemachten Informationen über das Unternehmen des Auftraggebers vertraulich zu behandeln und nur für den vereinbarten Zweck auszuwerten. Zugänglich gemachte Unterlagen werden nicht an Dritte weitergegeben. Hiervon ausgeschlossen ist die ausführliche Berichterstattung an die Schiedsstelle in Streitfällen. Der Kunde kann die Zertifizierungsstelle aus bestimmten Gründen von ihrer Schweigepflicht entbinden.

Ergänzend zu unseren allgemeinen Geschäftsbedingungen und als notwendige Vertragsbedingung, beschränkt sich die Haftung von CCSEC gegenüber dem Klienten oder Dritten auf die gesetzliche Mindestforderung im Falle eines Vorsatzes oder grober Fahrlässigkeit. Weitergehende Ansprüche sind ausgeschlossen. Dies gilt insbesondere für die Durchführung von Netzwerkanalysemaßnahmen.

6. Pflichten des Klienten

Folgende Pflichten sind vom Klienten vor, während und nach dem Zertifizierungsverfahren zu erfüllen:

- Bereitstellung geeigneter Arbeitsplätze für die Auditoren während der Audits
- Bereitstellung geeigneter Netzzugänge für die Durchführung von Netzwerkanalysen
- Bereitstellung kompetenter Interviewpartner während den Interviews
- Bereitstellung der erforderlichen Dokumentation

7. Einspruchsverfahren

Der Klient kann vor dem Audit Einspruch gegen die Auditoren einlegen, die während des Audits eingesetzt werden sollen. Diese werden ihm ca. 2 Wochen vor dem Audit von CCSEC mitgeteilt. Im Falle eines Einspruchs des Klienten gegen einen oder mehrere Auditoren prüft der LZ, ob Alternativen möglich sind bzw. das Audit dennoch durchführbar ist. Danach bespricht er die weitere Vorgehensweise mit dem Klienten. Für vertragsrechtliche Folgen gelten die gesetzlichen Bestimmungen.

Der Klient kann auch Einspruch bzw. Beschwerde gegen sonstige nicht zufriedenstellende Entscheidungen der Zertifizierungsstelle im Rahmen des durchgeführten Zertifizierungsverfahrens bei der Zertifizierungsstelle erheben. Die Zertifizierungsstelle begründet daraufhin dem Klienten die Entscheidung, soweit noch nicht erfolgt, nochmals ausführlich, ggf. mit Verweisen auf die relevanten Stellen in der Projektdokumentation.

Ist die Begründung der Zertifizierungsstelle für den Klienten nicht nachvollziehbar oder akzeptiert er diese nicht, so kann er eine Beschwerde beim Lenkungsausschuss der Zertifizierungsstelle einlegen. Der Lenkungsausschuss trifft dann die endgültige Entscheidung.

8. Witness-Audits durch die Akkreditierungsstelle

Der Klient duldet im Bedarfsfall die Begleitung der CCSEC-Auditoren durch Begutachter der Trägergemeinschaft für Akkreditierung GmbH (TGA) im Rahmen von Witness-Audits.

9. Inkrafttreten

Diese Zertifizierungsregeln treten am 01.01.2006 in Kraft und unterliegen einem Änderungsdienst. Das Datum und die Versionsnummer sind der ersten Seite dieses Dokuments zu entnehmen. Der jeweils aktuelle Stand ist zum Zeitpunkt des Vertragsschlusses maßgeblich. Die Zertifizierungsregeln gelten grundsätzlich für alle Verfahren, die im Zeitraum ihrer Gültigkeit durch CCSEC begonnen werden. Zukünftige Änderungen können auf bestehende Zertifikate oder bereits laufende Verfahren nur nach schriftlichem Einverständnis mit dem Klienten angewandt werden.

A handwritten signature in black ink, appearing to read "M. Tomas".

Michael Tomas, LL.M.

Leiter der Zertifizierungsstelle