ePrivacycert

Programm
der ePrivacycert GmbH
zur Zertifizierung nach DIN ISO/IEC 27001:2017-06

Inhalt

Einleitung

Informationssicherheitsmanagementsysteme (ISMS) wahren die Vertraulichkeit, Integrität und Verfügbarkeit von Information in Organisationen, indem sie Risikomanagementprozesse etablieren. Die DIN ISO/IEC 27001 legt Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung von Informationssicherheitsmanagementsystemen fest.

Das vorliegende Dokument beschreibt das Standardvorgehen der Zertifizierungsstelle der ePrivacycert GmbH bei der Prüfung von ISMS im Zertifizierverfahren. Für weiterführende Stadien und Sonderfälle sowie ergänzend zum Verfahren gelten die Bestimmungen des Verfahrenshandbuchs 17021 der ePrivacycert GmbH.

1. Allgemeines; Beginn des Zertifizierverfahrens

1.1. Informelle Vorprüfung

Auf Anfrage der zertifizierungswilligen Organisation übersendet ihr die Zertifizierungsstelle (im folgenden: ZS) einen Fragebogen, mit dem sie folgende Pflichtangaben erhebt:

a) der gewünschte Geltungsbereich der Zertifizierung;
b) Name des Antragstellers,
c) Anschriften der Standorte
d) Prozesse und Tätigkeiten
e) ob und ggfs von wem der Antragsteller bezüglich des zu zertifizierenden ISMS bereits beraten wurde.

Dabei stellt die ZS sicher,

- dass für jeden Geltungsbereich der Zertifizierung mindestens eine Erklärung zur Anwendbarkeit vorliegt

- dass Schnittstellen zu Diensten oder Tätigkeiten, die nicht vollständig innerhalb des ISMS-Anwendungsbereiches liegen, einbezogen werden

- dass der Antragsteller angegeben hat, ob er bei mehreren Standorten eine Gemeinschafts- oder eine Verbundzertifizierung wünscht.

Sind vertrauliche, sensible Informationen involviert, dann entscheidet die ZS, ob das ISMS ggfs. auch ohne die betreffenden Informationen in angemessener Weise auditiert werden kann.

Bei dem ISMS müssen **vorab** mindestens eine Managementbewertung und ein internes ISMS-Audit durchgeführt worden sein, die den Geltungsbereich der Zertifizierung abdecken.

Ggfs. fordert die ZS weitere Unterlagen an, um ein Angebot kalkulieren zu können.

1.2. Antrag

Auf Basis dieses Angebots stellt die zertifizierungswillige Organisation einen formellen Antrag auf Durchführung des Zertifizierungsverfahrens.

1.3. Ermittlung der erforderlichen Kompetenzen

Die ZS ermittelt, welche Kompetenzen sie für das Auditteam sowie für die Zertifizierungsentscheidung benötigt. Stehen ihr die erforderlichen Kompetenzen nicht zur Verfügung, lehnt sie den Zertifizierungsantrag ab.

1.4. Auditprogramm

Die ZS entwickelt ein Auditprogramm für den Zertifizierungszyklus. Dabei berücksichtigt sie die Größe des Kunden, den Geltungsbereich und die Komplexität seines ISMS, seiner Produkte und Prozesse sowie die Wirksamkeit des ISMS und die Ergebnisse früherer Audits. Die ZS kann weitere relevante Umstände berücksichtigen, etwa Beschwerden über den Kunden oder Änderungen der Akkreditierungsanforderungen.

Für eine erstmalige Zertifizierung ist ein zweistufiges Erstaudit durchzuführen. Im ersten und zweiten Jahr nach der Zertifizierungsentscheidung finden Überwachungsaudits statt und im dritten Jahr unmittelbar vor Ablauf der Zertifizierung ein Re-Zertifizierungsaudit. Das Datum des ersten Überwachungsaudits, das der Erstzertifizierung folgt, darf nicht mehr als 12 Monate nach dem Datum der Zertifizierungsentscheidung liegen. Der erste dreijährige Zyklus der Zertifizierung beginnt mit der Zertifizierungsentscheidung, nachfolgende Zyklen mit der Re-Zertifizierungsentscheidung.

Beruft sich der Kunde auf Zertifizierungen oder Audits einer anderen ZS, so verlangt die ZS der ePrivacycert ausreichende Nachweise dafür, dass die Anforderungen der ISO 17021 und der IAF MD 2:2017 erfüllt sind.

1.5. Ermittlung des Auditzeitaufwands

Die ZS ermittelt den Zeitaufwand der Auditoren für die Planung und Durchführung des ISMS-Audit gemäß der Richtlinie Auditzeiten der ePrivacycert. Sie dokumentiert und begründet die Dauer. Der Zeitaufwand von Teammitgliedern, die nicht als Auditor eingesetzt sind (d. h. Fachexperten, Übersetzer, Dolmetscher, Beobachter und Auditoren in Ausbildung), wird bei der Bestimmung des Auditzeitaufwands nicht mitgerechnet.

1.6. Mehrere Standorte

Sind mehrere Standorte zu auditieren, dann kann die Zertifizierungsstelle einen stichprobenbasierten Ansatz wählen, sofern alle Standorte unter demselben ISMS betrieben werden und das ISMS zentral verwaltet und intern auditiert wird und das ISMS einer zentralen Managementbewertung unterliegt. In diesem Fall stellt sie sicher, dass die Stichprobenahme bei einer repräsentativen Auswahl von Standorten erfolgt.

Das Auditprogramm deckt repräsentative Stichproben aus dem Geltungsbereich der ISMS-Zertifizierung innerhalb des Zeitraums von drei Jahren ab. Das Audit muss die Tätigkeiten am Stammsitz des Kunden behandeln, um sicherzustellen, dass ein einzelnes ISMS alle Standorte abdeckt und auf betrieblicher Ebene ein zentrales Management bietet.

Bei Mehrfachzertifizierungen muss die Auditplanung ein angemessenes Vor-Ort-Audit vorsehen.

Bei der Vorbereitung und Durchführung der Audits orientiert sich die ZS an der ISO 19011.

2. Planen von Audits

Die Planung von Audits umfasst die Festlegung der Auditziele, des Auditumfangs und der Auditkriterien. Die Auditziele, etwa die Feststellung der Konformität mit den Auditkriterien oder ggfs Verbesserungsmöglichkeiten des ISMS, legt die ZS fest. Der Auditumfang ist mit dem Kunden abzustimmen. Er bezieht sich etwa darauf, welche Standorte, Organisationseinheiten, Tätigkeiten und Prozesse abgedeckt werden. Die Auditkriterien stimmt die ZS mit dem Kunden ab.

2.1 Auswahl des Auditteams

Abhängig vom Zertifizierungsgegenstand legt die ZS fest, welche **Kompetenzen** im Auditteam zur Erreichung der Auditziele erforderlich sind. Auf dieser Grundlage wählt sie die beteiligten Auditoren aus, bestimmt einen Auditteamleiter und zieht bei Bedarf Fachexperten hinzu. Sie berücksichtigt dabei die Anforderungen an die Unparteilichkeit.

Das erforderliche Wissen und die erforderlichen Fertigkeiten des Auditteams dürfen durch Fachexperten, Übersetzer und Dolmetscher ergänzt werden, die unter der Anleitung eines Auditors arbeiten müssen. Hinzuziehung und Betätigung von Fachexperten sind mit dem Kunden abzustimmen.

Jeder Auditor wird von einem Betreuer begleitet, es sei denn, Auditteamleiter und Kunde haben etwas anderes vereinbart.

2.2 Auditplan

Für jedes Audit ist ein Auditplan zu erstellen. Er berücksichtigt die festgelegten Informationssicherheitsmaßnahmen. Er muss mindestens Folgendes enthalten oder Bezug darauf nehmen:
a) die Auditziele;
b) die Auditkriterien;
c) den Auditumfang, einschließlich der Festlegung der zu auditierenden Organisations- und Funktionseinheiten oder Prozesse;
d) die Termine und Standorte, an denen Audittätigkeiten vor Ort durchgeführt werden, gegebenenfalls einschließlich der Besuche von temporären Standorten und Audittätigkeiten aus der Ferne. Gebieten es wesentliche Umstände, die dem Einfluss der Parteien entzogen sind, so kann in besonders zu begründenden Ausnahmefällen von einer Auditierung vor Ort abgesehen werden;
e) die vorgesehene Dauer der Audittätigkeiten vor Ort;
f) die Rollen und Verantwortlichkeiten der Mitglieder des Auditteams und der Begleitpersonen, wie z. B. Beobachter und Dolmetscher.

Der Auditplan bestimmt, welche netzwerkgestützten Auditverfahren angewandt werden. Darunter fallen etwa Telefonkonferenzen, Webmeetings, interaktive webbasierte Kommunikation und elektronischer Fernzugriff auf die ISMS-Dokumentationen oder -Verfahren.

Der Auditplan wird dem Kunden mitgeteilt, die Daten sind mit dem Kunden abzustimmen.

Die Aufgaben des Auditteams werden dem Team mitgeteilt. Sie bestehen darin,
a) Struktur, grundsätzliche Regelungen, Prozesse, Verfahren, Aufzeichnungen und zugehörige Dokumente des Kunden bezüglich der ISMS-Norm zu prüfen und zu verifizieren;
b) festzustellen, dass diese alle relevanten Anforderungen bezüglich des beabsichtigten Geltungsbereichs der Zertifizierung erfüllen;
c) festzustellen, dass die Prozesse und Verfahren wirksam eingeführt, umgesetzt und aufrechterhalten werden;
d) dem Kunden zu verdeutlichen, wenn Widersprüche zwischen seiner Politik, seinen Zielen und seinen Vorgaben auftreten sollten.

Die ZS stellt den Namen und auf Nachfrage Hintergrundinformationen zu jedem Mitglied des Auditteams zur Verfügung. Erhebt der Kunde Einspruch gegen die Benennung eines bestimmten Mitglieds des Auditteams und ist dieser begründet, dann muss die ZS das Team neu zusammenstellen.

3. Erstzertifizierung

Das Erstzertifizierungs-Audit wird in zwei Stufen durchgeführt.

3.1 Stufe 1

In Stufe 1 des Audits lässt sich die Zertifizierungsstelle die erforderliche Dokumentation zur Gestaltung des ISMS vorlegen.
Die Ziele der Stufe 1 sind mindestens:
a) die dokumentierten Informationen zum ISMS des Kunden zu bewerten;
b) die standortspezifischen Bedingungen des Kunden zu beurteilen sowie Diskussionen mit dem Personal des Kunden zu führen, um zu ermitteln, ob der Kunde auf Stufe 2 vorbereitet ist;
c) den Vorbereitungsstand sowie das Verständnis des Kunden bezüglich der Anforderungen der Norm zu bewerten, insbesondere im Hinblick auf die Identifizierung von Schlüsselleistungen bzw. bedeutsamen Aspekten, Prozessen, Zielen und das Betreiben des ISMS;
d) notwendige Informationen zu erlangen bezüglich des Geltungsbereichs des ISMS einschließlich:
- Standort(e) des Kunden,
- Prozesse und eingesetzte Arbeitsmittel,
- festgelegte Lenkungsebenen (insbesondere bei Kunden mit mehreren Standorten),
- anzuwendende gesetzliche und behördliche Anforderungen;
e) die Zuteilung der Ressourcen für Stufe 2 zu bewerten sowie die Einzelheiten von Stufe 2 mit dem Kunden abzustimmen;
f) zu beurteilen, ob
- die internen Audits und Managementbewertungen geplant und durchgeführt werden und
- der Kunde für Stufe 2 bereit ist.

Die Ergebnisse von Stufe 1 werden in einem schriftlichen Bericht aufgezeichnet, der der ZS vorzulegen ist. Die Zertifizierungsstelle prüft den Auditbericht der Stufe 1, bevor sie entscheidet, mit Stufe 2 fortzufahren. Sie bestätigt, dass die Auditoren für Stufe 2 über die notwendigen Kompetenzen verfügen.

Bei der Ermittlung des zeitlichen Abstands zwischen Stufe 1 und Stufe 2 ist der Aufwand zu berücksichtigen, den der Kunde voraussichtlich betreiben muss, um Lösungen zu Schwachstellen zu finden, die während Stufe 1 identifiziert wurden. Treten bedeutende Änderungen beim Kunden auf, etwa im ISMS, am Geltungsbereich oder an der Dokumentation, ordnet die ZS nach pflichtgemäßem Ermessen an, die gesamte Stufe 1 oder Teile derselben zu wiederholen.

Die Schlussfolgerungen und die Bereitschaft für Stufe 2 werden dem Kunden mitgeteilt. Dabei ist auf Schwachstellen hinzuweisen, die in Stufe 2 als Nichtkonformität eingestuft werden könnten.

3.2 Stufe 2

In Stufe 2 werden Umsetzung und Wirksamkeit des ISMS des Kunden bewertet. Das Audit richtet sich schwerpunktmäßig auf:
- Führung durch die oberste Leitung;
- die in ISO 27001aufgelisteten Dokumentationsanforderungen;
- mit der Informationssicherheit zusammenhängende Risiken;
- Bestimmung der Maßnahmen;
- Informationssicherheitsleistung und die Wirksamkeit des ISMS;
- Umsetzung der Maßnahmen (siehe ISO 27006, Anhang D);
- Programme, Prozesse, Verfahren, Aufzeichnungen, interne Audits und Bewertung der ISMS-Wirksamkeit.

Auf Grundlage der im Auditbericht dokumentierten Ergebnisse entwickelt die Zertifizierungsstelle einen Auditplan für Stufe 2.

4. Durchführen von Audits

Die ZS
a) fordert vom Kunden den Nachweis, dass die Bewertung der mit der Informationssicherheit zusammenhängenden Risiken für den ISMS-Betrieb relevant und angemessen ist;
b) legt fest, ob die Verfahren des Kunden zur Bestimmung, Untersuchung und Bewertung der Risiken und die Umsetzung mit der Politik und den Zielen des Kunden in Einklang stehen.
c) stellt fest, ob die eingesetzten Verfahren gründlich und angemessen umgesetzt wurden.

4.1 Vor-Ort-Audits

Vor-Ort-Audits beginnt die ZS mit einer Eröffnungsbesprechung. Diese umfasst
a) Vorstellung der Teilnehmer einschließlich einer Kurzdarstellung ihrer Rollen;
b) Bestätigung des Geltungsbereichs der Zertifizierung;
c) Bestätigung des Auditplans sowie aller Änderungen und sonstigen relevanten Vereinbarungen mit dem Kunden;
d) Bestätigung der offiziellen Kommunikationskanäle zwischen Auditteam und Kunde;
e) Bestätigung, dass die vom Auditteam benötigten Ressourcen und Einrichtungen zur Verfügung stehen;
f) Bestätigung von Angelegenheiten, die sich auf Vertraulichkeit beziehen;
g) Bestätigung der für das Auditteam zutreffenden Arbeitsschutz-, Notfall- und Sicherheitsverfahren;
h) Bestätigung der Verfügbarkeit, Rollen und Identitäten von etwaigen Betreuern und Beobachtern;
i) Methoden der Berichterstattung;
j) Umstände, die zum vorzeitigen Abbruch des Audits führen können;
k) Bestätigung, dass der Auditteamleiter und das Auditteam in Vertretung der ZS die Verantwortung für das Audit tragen und die Leitungsfunktion für die Ausführung des Auditplans innehaben müssen;
l) Bestätigung des Status von Auditfeststellungen aus der vorangegangenen Überprüfung bzw. aus dem vorangegangenen Audit, falls zutreffend;

m) Methoden und Verfahren, die bei der Durchführung von Audits anzuwenden sind, die auf Stichproben basieren;
n) Bestätigung der während des Audits zu verwendenden Sprache;
o) Bestätigung, dass der Kunde während des Audits über dessen Fortschritt und alle auftretenden Probleme auf dem Laufenden gehalten wird;
p) Möglichkeit für den Kunden, Fragen zu stellen.

Der Auditteamleiter bespricht mit dem Kunden jeglichen Änderungsbedarf am Auditumfang, der sich im Verlauf der Audittätigkeiten vor Ort herausstellt, und berichtet der ZS darüber.

4.2 Informationserlangung

Es sind mindestens folgende Methoden der Informationserlangung einzusetzen:
a) Befragungen;
b) Beobachtung von Prozessen und Tätigkeiten;
c) Auswertung von Dokumentationen und Aufzeichnungen.

Um als Auditnachweise verwendet werden zu können, sind die Informationen durch angemessene Stichproben zu erfassen und zu verifizieren.

4.3 Aufzeichnung von Auditfeststellungen

Auditfeststellungen sind aufzuzeichnen. Verbesserungsmöglichkeiten dürfen ermittelt werden, sofern dies nicht nach den Anforderungen des Zertifizierungsprogramms verboten ist.

4.4 Erarbeiten der Auditschlussfolgerungen

Falls die Auditnachweise anzeigen, dass die Auditziele nicht erreicht werden können oder ein unmittelbares und erhebliches Risiko bestehen kann, muss der Auditteamleiter dem Kunden und, falls möglich, der ZS darüber Bericht erstatten, um die entsprechenden Maßnahmen zu ermitteln.

Jede Nichtkonformität muss einer bestimmten Anforderung zugeordnet werden. Die objektiven Nachweise für die Nichtkonformität sind im Einzelnen zu beschreiben. Nichtkonformitäten sind mit dem Kunden zu erörtern.

Das Auditteam
a) bewertet die Auditfeststellungen und alle sonstigen im Verlauf des Audits erlangten geeigneten Informationen und teilt die Nichtkonformitäten ein;
b) zieht gemeinsam die Auditschlussfolgerungen unter Berücksichtigung von Ungewissheiten bezüglich des Auditprozesses;
c) beschließt über erforderliche Folgemaßnahmen;
d) bestätigt die Eignung des Auditprogramms ermittelt die erforderlichen Änderunge für zukünftige Audits (z. B. Geltungsbereich der Zertifizierung, Auditzeitaufwand oä).

4.5 Abschlussbesprechung

Die Abschlussbesprechung wird mit dem Management des Kunden und gegebenenfalls mit den Personen, die die Verantwortung für die zu auditierenden Funktionen oder Prozesse tragen, durchgeführt. Die aus dem Audit gezogenen Schlussfolgerungen einschließlich der Empfehlung hinsichtlich der Zertifizierung werden vorgestellt. Die Besprechung umfasst:
a) Hinweis an den Kunden, dass die Auditnachweise auf einer Stichprobe basieren und daher ein gewisses Unsicherheitselement beinhalten;
b) Methode und Zeitraum der Berichterstattung einschließlich Einstufung der Auditfeststellungen;
c) Prozess der ZS für die Behandlung von Nichtkonformitäten;
d) Zeitrahmen, innerhalb dessen der Kunde einen Plan für Korrekturmaßnahmen in Bezug auf die ermittelten Nichtkonformitäten vorlegen muss;
e) nach dem Audit erfolgende Tätigkeiten der ZS;
f) Informationen zu den Prozessen für die Behandlung von Beschwerden und Einsprüchen.

4.6 Auditbericht

Die ZS erstellt für jedes Audit einen schriftlichen Bericht für den Kunden. Er enthält oder bezieht sich auf
a) die Nennung der ZS;
b) Name und Anschrift des Kunden und des Beauftragten des Kunden;
c) Audittyp (z. B. Erst-, Überwachungs- oder Re-Zertifizierungsaudit oder Audits aus besonderem Anlass);
d) Auditkriterien;
e) Auditziele;
f) Auditumfang und besonders die Angabe der auditierten Organisations- oder Funktionseinheiten oder -prozesse und den Auditzeitaufwand;
g) jede Abweichung vom Auditplan und die Gründe dafür;
h) jeden bedeutenden Aspekt, der einen Einfluss auf das Auditprogramm besitzt;
i) Benennung des Auditteamleiters, der Mitglieder des Auditteams und aller Begleitpersonen;
j) Termine und Orte, an denen die Audittätigkeiten (vor Ort oder nicht vor Ort, dauerhafte oder vorübergehende Standorte) durchgeführt wurden;
k) Auditfeststellungen, Verweis auf Auditnachweise und Auditschlussfolgerungen in Übereinstimmung mit den Anforderungen des betreffenden Audittyps;
l) bedeutende Änderungen gegenüber dem vorangegangenen Audit, die das ISMS des Kunden beeinflussen;
m) alle ungelösten Aspekte, falls solche festgestellt wurden;
n) ob es sich um ein kombiniertes, gemeinschaftliches oder integriertes Audit handelt;
o) einen Haftungsausschluss, der angibt, dass die Auditierung auf einem Stichprobenahmeverfahren der verfügbaren Informationen basiert;
p) Empfehlung des Auditteams;
q) der auditierte Kunde kontrolliert wirksam die Verwendung von Zertifizierungsdokumenten und -zeichen, sofern zutreffend;
r) Verifizierung der Wirksamkeit von ergriffenen Korrekturmaßnahmen bezüglich vorangegangener identifizierter Nichtkonformitäten;
s) eine Darstellung des Zertifizierungsaudits der Informationssicherheitsrisikoanalyse des Kunden;

t) den ISMS-Anwendungsbereich.

Aus dem Bericht muss hervorgehen:

a) eine Aussage über die Konformität und über die Wirksamkeit des ISMS
b) eine Feststellung zur Eignung des Geltungsbereichs der Zertifizierung;
c) die Bestätigung, dass die Auditziele erfüllt worden sind.

4.7 Analyse der Ursachen von Nichtkonformitäten

Die ZS fordert vom Kunden, die Ursachen von Nichtkonformitäten zu analysieren und die Korrekturmaßnahmen zu beschreiben, die er innerhalb eines festgelegten Zeitraums zu ergreifen hat.

4.8 Wirksamkeit von Korrekturen und Korrekturmaßnahmen

Die ZS bewertet die vom Kunden vorgelegten Korrekturmaßnahmen und verifiziert deren Wirksamkeit. Nachweise über die Behebung von Nichtkonformitäten sind aufzuzeichnen.

Der Kunde ist über das Ergebnis der Überprüfung und Verifizierung zu informieren. Er ist auch zu informieren, wenn weitere Schritte durch die ZS erforderlich sind, um die Wirksamkeit von Korrekturen zu überprüfen.

5. Zertifizierungsentscheidung

5.1 Voraussetzungen für die Zertifizierentscheidung

Bevor sie die Zertifizierentscheidung trifft, stellt die ZS sicher, dass:

a) die durch das Auditteam bereitgestellten Informationen im Hinblick auf die Zertifizierungsanforderungen und den Geltungsbereich ausreichend sind;
b) sie für alle wesentlichen Nichtkonformitäten die Korrekturen und Korrekturmaßnahmen bewertet, angenommen und verifiziert hat;
c) sie für alle untergeordneten Nichtkonformitäten den Plan des Kunden in Bezug auf Korrekturen und Korrekturmaßnahmen bewertet und angenommen hat.

Wer an der Entscheidung über die Erteilung oder Verweigerung der Zertifizierung, Erweiterung oder Einschränkung des Geltungsbereichs der Zertifizierung, Aussetzung oder Wiederherstellung der Zertifizierung, Zurückziehung der Zertifizierung oder Erneuerung der Zertifizierung mitwirkt, darf nicht an den Audits mitgewirkt haben.

Die Zertifizierungsentscheidung wird auf Grundlage der Zertifizierungsempfehlung des Auditteams sowie auf den Anforderungen in ISO 17021 getroffen. Die ZS zeichnet jede Zertifizierungsentscheidung einschließlich zusätzlicher Informationen oder Klarstellungen, die vom Auditteam oder von anderen Quellen erfragt wurden, auf.

Die Zertifizierungsentscheidung darf dem Kunden erst erteilt werden, wenn er nachweist, dass Vorkehrungen für Managementbewertungen und interne ISMS-Audits wirksam sind und aufrechterhalten werden.

Die Zertifizierung wird für drei Jahre erteilt. Die Gültigkeitsbedingungen des Zertifikates ergeben sich aus der Zertifizierordnung, die als Anlage zur Zertifiziervereinbarung rechtsverbindlich mit dem Kunden vereinbart ist. Die Zertifizierordnung regelt sämtliche Rechte und Pflichten des Antragstellers, insbesondere im Hinblick auf die Nutzung des Zertifikates.

Das Zertifikat wird auf der Webseite der ePrivacycert GmbH veröffentlicht.

5.2 Information über Erteilung der Erstzertifizierung

Das Auditteam stellt der ZS für die Zertifizierungsentscheidung mindestens bereit:
a) den Auditbericht;
b) Anmerkungen zu den Nichtkonformitäten und Korrekturmaßnahmen;
c) Bestätigung der Angaben aus der Antragstellung;
d) Bestätigung, dass die Auditziele erreicht worden sind;
e) eine Empfehlung, ob die Zertifizierung gewährt werden soll oder nicht, zusammen mit Bedingungen bzw. Beobachtungen.

Wesentliche Nichtkonformitäten sind innerhalb von 6 Monaten nach dem letzten Tag der Stufe 2 zu korrigieren. Andernfalls muss die ZS vor der Empfehlung zur Zertifizierung eine erneute Stufe 2 durchführen.

5.3 Informationen zur Erteilung der Re-Zertifizierung

Die ZS entscheidet über die Erneuerung der Zertifizierung auf der Grundlage der Ergebnisse des Re-Zertifizierungsaudits sowie der Ergebnisse aus der Bewertung des Systems über den Zeitraum der Zertifizierung und der von den Nutzern der Zertifizierung erhaltenen Beschwerden.

6. Aufrechterhaltung der Zertifizierung

Ist dargelegt, dass der Kunde die Normanforderungen weiterhin erfüllt, wird die Zertifizierung aufrechterhalten.

Die ZS darf die Zertifizierung eines Kunden auf der Grundlage einer positiven Schlussfolgerung des Auditteamleiters ohne weitere unabhängige Bewertung und Entscheidung aufrechterhalten. Etwas anderes gilt, wenn eine Nichtkonformität oder eine andere Situation eintritt, die zu einer Aussetzung oder Zurückziehung der Zertifizierung führen könnte. In diesem Fall berichtet der Auditteamleiter der ZS, dass eine Bewertung durch kompetentes Personal (siehe Ziffer 7.2.8 ISO 17021) notwendig ist. Dieses Personal muss sich von dem unterscheiden, das das Audit durchgeführt hat. Es führt eine Bewertung durch und ermittelt, ob die Zertifizierung aufrechterhalten werden kann.

Die ZS stellt durch ihre Prozesse sicher, dass ihre Überwachungstätigkeiten durch kompetentes Personal überprüft werden ihre Zertifizierungstätigkeiten in wirksamer Weise durchgeführt werden.

6.1 Überwachungstätigkeiten

Die ZS überwacht regelmäßig maßgebliche Bereiche und Tätigkeiten, die vom Geltungsbereich des ISMS erfasst werden. Änderungen sind zu berücksichtigen. Weitere Überwachungstätigkeiten können sein:
a) Anfragen der ZS an den Kunden;
b) Bewertung der Angaben des Kunden im Hinblick auf seine Tätigkeiten (z. B. Werbematerial, Webseiten);
c) Aufforderungen an den Kunden zur Bereitstellung von Informationen (auf Papier oder elektronischen Medien);
d) andere Mittel zur Überwachung der Leistungsfähigkeit des Kunden.

Jede Überwachung umfasst die Prüfung und Bewertung von:
a) internen Audits und Managementbewertung;
b) Maßnahmen zu Nichtkonformitäten, die während des vorhergehenden Audits festgestellt wurden;
c) Umgang mit Beschwerden;
d) Wirksamkeit des ISMS im Hinblick auf das Erreichen der Ziele insbesondere hinsichtlich der Informationssicherheitspolitik des Kunden und der beabsichtigten Ergebnisse der entsprechenden ISMS;
e) Fortschritt bei Tätigkeiten, die auf eine ständige Verbesserung zielen;
f) anhaltende operative Lenkung;
g) Änderungen;
h) Nutzung von Zeichen und/oder anderen Verweisen auf die Zertifizierung;
i) die Funktionsweise der Verfahren zur regelmäßigen Bewertung und Prüfung der Einhaltung relevanter Gesetze und Vorschriften zur Informationssicherheit;
j) Änderungen an den festgelegten Maßnahmen und daraus resultierende Änderungen an der SoA.

Im Rahmen von Überwachungsaudits sind der Zertifizierungsstelle vorgelegte Einsprüche und Beschwerden zu prüfen. Bei Nichtkonformitäten oder nicht erfüllten Anforderungen der Zertifizierung prüft die ZS, ob der Kunde sein eigenes ISMS und Verfahren untersucht und angemessene Korrekturmaßnahmen ergriffen hat.
Ein Überwachungsauditbericht muss insbesondere Angaben zur Behebung von Nichtkonformitäten, die Version der SoA und wichtige Änderungen seit dem letzten Audit enthalten.

6.2 Re-Zertifizierung

Tätigkeiten zu Re-Zertifizierungsaudits können ein Stufe 1-Audit erfordern, wenn es signifikante Änderungen im ISMS, bei der Organisation oder im Zusammenhang mit der Arbeitsweise des ISMS gibt (z. B. Veränderungen in der Gesetzgebung). Das Re-Zertifizierungsaudit muss ein Vor-Ort-Audit beinhalten.

Für jede wesentliche Nichtkonformität legt die ZS Fristen für Korrekturen fest. Die Korrekturen müssen vor Ablauf der Zertifizierung umgesetzt und verifiziert werden. Das Ausgabedatum des neuen Zertifikats muss dem Tag der Re-Zertifizierungsentscheidung oder einem späteren entsprechen.
Hat die ZS vor Ablauf des Zertifizierungsdatums das Re-Zertifizierungsaudit nicht abgeschlossen oder die Umsetzung von Korrekturen für eine wesentliche Nichtkonformität nicht verifiziert, dann darf keine Empfehlung für die Re-Zertifizierung ausgesprochen und die Gültigkeit der Zertifizierung nicht verlängert werden. Der Kunde ist darüber zu unterrichten, die Konsequenzen sind ihm zu erläutern.
Sind die ausstehenden Re-Zertifizierungstätigkeiten abgeschlossen worden, kann die ZS innerhalb von 6 Monaten nach Ablauf der Zertifizierung die Zertifizierung wiederherstellen; andernfalls ist mindestens die Stufe 2 durchzuführen. Das Gültigkeitsdatum des Zertifikats muss dem Tag der Re-Zertifizierungsentscheidung oder einem späteren entsprechen; das Ablaufdatum muss auf dem vorangegangenen Zertifizierungszyklus basieren.