Secure Your Business

CIS – Certification &
Information Security Services GmbH

Information

CIS-Zertifizierungsverfahren

nach ISO 27001 (inkl. 27018),

ISO 20000 (inkl. 20000-9)

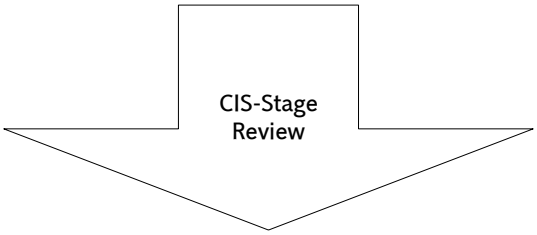
und ISO 22301

1. Zugangsvoraussetzungen:

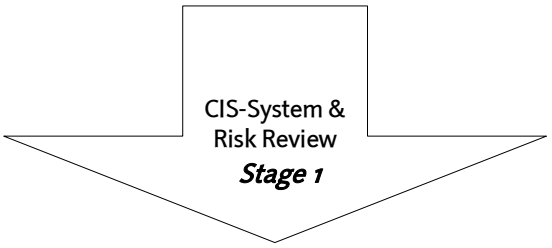
Der Auftraggeber muss ein dokumentiertes Informations-/Service-/Business-Continuity-/ Management-System unterhalten.

2. Ablauf des Zertifizierungsverfahrens

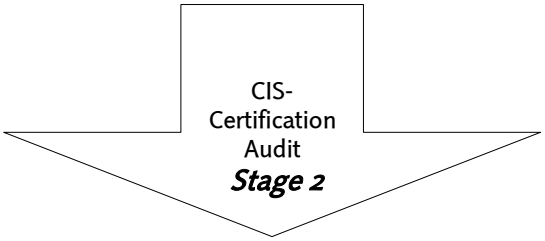
Auf Grundlage des CIS-Antrages auf Zertifizierung werden die weiteren Schritte des Zertifizierungsverfahrens terminlich und inhaltlich geplant und der Geltungsbereich der Zertifizierung bestimmt. Mit dem „Initial Registration & Planning Stage" steht Ihre Organisation formal im CIS-Zertifizierungsverfahren und wird daher auch in der CIS-Registrationlist gelistet.



Organisationen können während der Etablierung oder bei Anpassung bzw. Verbesserung des Management-Systems die Angemessenheit und Zweckmäßigkeit der getroffenen Vorkehrungen und Maßnahmen durch den CIS-Stage Review im Sinne der Normforderungen beurteilen lassen. Der CIS-Stage Review kann daher auch als unabhängige und schrittweise Projektfortschrittsüberwachung eingesetzt werden.

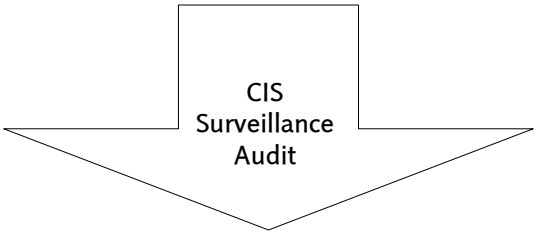


Das System Review hat zum Ziel, die unternehmensbezogene Interpretation der Normforderungen auf Grundlage durchgeführter konkreter Maßnahmen und Vorkehrungen zu beurteilen. Weiters wird die existierende Management-System Dokumentation geprüft und beurteilt. Die erkannten Schwachstellen werden erläutert und der weitere Handlungsbedarf vor dem CIS-Certification Audit wird in einem schriftlichen Bericht festgehalten.

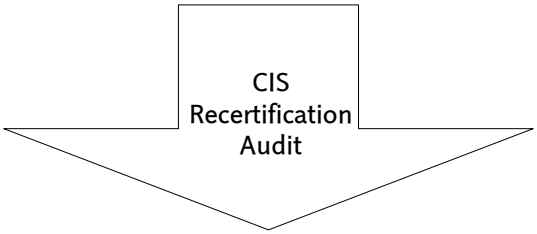


Das CIS-Certification Audit hat die praktischen Maßnahmen zum lückenlosen Nachweis der Normforderungen zum Umfang. Dabei wird besonders der Schwerpunkt darauf gelegt, dass durch multiple Stichproben in allen Ebenen der Organisation, die systematische Vorgehensweise nachvollziehbar wird. Die eingesetzte Technologie spielt dabei soweit eine Rolle als diese den Organisations- und Managementbedarf maßgeblich beeinflusst.

Mit der Certificate Issuance & Right to Use Licence erwirbt die zertifizierte Organisation das Recht zur Führung eines CIS-Konformitätsnachweises. Der CIS-Konformitätsnachweis wird mit einer 3-jährigen Gültigkeit ausgestellt und darf als vertrauensbildender Nachweis gegenüber Dritten verwendet werden. Weiters werden CIS Kunde für ISO 20000-1 auf der Homepage von APMG gelistet, falls dies gewünscht wird.



Jedes Management-System unterliegt einer ständigen und schnell fortschreitenden organisatorischen, technologischen Umfeld Änderung, wodurch Anpassungen und Verbesserungen nötig werden. Im Rahmen des CIS-Surveillance Audits werden daher der Umgang mit diesen Veränderungen sowie die Wirksamkeit des gesamten Management-Systems festgestellt. Wird das CIS-Surveillance Audit erfolgreich abgeschlossen, so wird die Weiterverwendung des bestehenden Zertifikates beantragt. Bis zum Ablauf der dreijährigen Zertifikatsgültigkeit werden zwei CIS-Surveillance Audits im Abstand von jeweils 12 Monaten durchgeführt.



Nach 3 Jahren muss die Zertifikatsgültigkeit erneuert werden. Es ist daher ein vollumfängliches Recertification Audit im Umfang eines STAGE 2 Audits erforderlich. Nach einer erfolgreichen Recertification kann erneut das 3-jährige Recht zur Führung des CIS-Zertifikates und des CIS-Konformitätszeichens erworben werden.

3. Erläuterungen zum Zertifizierungsablauf

Antrag (siehe Dokument Nr. d012 bzw. d013 bzw.d066)

Aufgrund des Antrages wird auf Basis der Angaben ein Angebot erstellt.

3.1. Auftrag

Wird geschlossen durch Retournierung der unterfertigten Zweitschrift des Angebotes oder Bestellung.

3.2. Audit Stage 1

Das Audit Stage 1 findet bei Ihnen vor Ort statt.

Zweck dieses Audits ist eine **praktische Auseinandersetzung mit den Normforderungen**. Schwerpunkt dabei ist es den Status einer bereits durchgeführten Risikoanalyse festzustellen oder Anhaltspunkte und Ansätze für die Durchführung einer entsprechenden Risikoanalyse im Unternehmen zu liefern. Der „CIS-System & Risk Review" wird gemeinsam mit jenen Mitarbeitern durchgeführt, welche Koordinations- und Steueraufgaben in Bezug auf die Informationssicherheit / Servicemanagement / Business Continuity des Unternehmens übernehmen oder dafür Verantwortung tragen. Das System & Risk Review hat zum Ziel unternehmensbezogene Interpretation der Normforderungen auf Grundlage durchgeführter Risikoanalysen, -bewertungen sowie konkreter Maßnahmen und Vorkehrungen zu beurteilen.

Das CIS–Office gibt Ihnen schriftlich die CIS-Mitarbeiter bekannt, die Stage 1 durchführen. Der (die) Mitarbeiter nehmen mit Ihnen Kontakt zwecks Terminvereinbarung auf.

Über das Ergebnis des Stage 1 wird ein schriftlicher Bericht verfasst und Ihnen zur Kenntnis gebracht.

3.3. Audit Stage 2

Nach positivem Abschluss des Stage 1 erfolgt Audit Stage 2.
Das CIS-Office gibt Ihnen schriftlich die Namen des Auditoren Teams bekannt, wogegen Sie in begründeten Fällen Einwände (gegen einzelne Teammitglieder) vorbringen können.

Sofern Sie dem Auditoren Team zustimmen, wird der leitende Auditor einen Audittermin mit Ihnen vereinbaren.

Das CIS-Certification Audit hat die **praktischen Maßnahmen** zum lückenlosen Nachweis der Normforderungen zum Umfang. Dabei wird besonders der Schwerpunkt darauf gelegt, dass durch multiple Stichproben **in allen Ebenen der Organisation** die systematische Vorgehensweise nachvollziehbar wird. Die eingesetzte Technologie spielt dabei soweit eine Rolle als diese den Organisations- und Managementbedarf maßgeblich beeinflusst.

Über das Ergebnis des Stage 2 wird ein schriftlicher Bericht verfasst und zur Kenntnis gebracht.

Sofern darin Abweichungen dargelegt sind, sind diese zu beheben und die durchgeführten Maßnahmen zu berichten.
Sofern Abweichungen festgestellt wurden, die nicht durch die Nachreichung von Unterlagen erledigt werden können, wird das Stage 2 wiederholt.

Nach positivem Abschluss des Stage 2 wird vom Audit-Teamleiter die Empfehlung auf Zertifikatserteilung an die CIS GmbH gestellt.

3.4. Zertifikatsausstellung

Nach positiver Bewertung des Berichtes bzw. allfälliger Erledigungen von Abweichungen erfolgt die Zertifikatsausstellung durch die CIS GmbH. Die Gültigkeit des Zertifikates wird ab dem Zeitpunkt der Entscheidung der CIS Geschäftsführung berechnet.

3.5. Jährliche Überwachung (Bedingungen für die Aufrechterhaltung)

Der Termin der Überwachung ist immer Termin des Audits Stage 2. Das CIS-Office gibt Ihnen 3 Monate vor dem Termin des Überwachungsaudits, der mit der Überwachung beauftragten Auditor bekannt. Dieser nimmt mit Ihnen Kontakt auf und vereinbart einen Termin.

Im Rahmen der Überwachung wird der Umgang mit Veränderungen sowie die Wirksamkeit des gesamten Management-Systems festgestellt.

Über das Ergebnis wird ein Bericht verfasst. Sofern Abweichungen festgestellt wurden, sind diese von Ihnen zu beheben und in geeigneter Weise den CIS-Auditoren die durchgeführten Maßnahmen nachzuweisen. Im Falle von Abweichungen die nicht durch die Nachreichung von Unterlagen erledigt werden können, wird ein Nachaudit vor Ort durchgeführt. Nach positivem Abschluss des Überwachungsaudits wird vom Auditor die Empfehlung auf Weiterführung des Zertifikates an die CIS GmbH gestellt. Sofern Abweichungen nicht termingerecht behoben wurden, führt dies zum Entzug des Zertifikates.

3.6. Re-Zertifizierung

Nach Ablauf von 3 Jahren wird ein Re-Zertifizierungsaudit im Umfang eines Stage 2 durchgeführt (siehe Beschreibung Pkt. 3.4. Stage 2)

3.7. Änderungen in Bezug auf den Geltungsbereich der zertifizierten Systeme:

Änderungen werden wie Neuzertifizierungen abgehandelt. Rückmeldungen von Auftraggebern bezüglich organisatorischer Veränderungen werden von

Seiten der Geschäftsführung beurteilt. Sie trifft die Entscheidung über die weitere Vorgangsweise.

3.8. Änderungen bezüglich der Anforderungen an die Zertifizierung :

Änderungen bezüglich der Anforderungen an die Zertifizierung wie z.B. Änderung der Normen nach denen die Zertifizierung erteilt wurde, werden allen zertifizierten Kunden per E-Mail zur Kenntnis gebracht. Sofern weiterführende erläuternde Hinweise erforderlich sein sollten, werden diese auf der Homepage oder per Newsletter veröffentlicht.

4. Mitgeltende Unterlagen

4.1. Allgemeine Bedingungen für Dienstleistungen der CIS – Certification & Information Security Services GmbH.

Anmerkung 1:
Im CIS-Zertifizierungsverfahren ist keine Aussetzung der Zertifizierung vorgesehen.