Checkliste zum Review eines ISO/IEC 27001 Zertifikats

Zertifizierungsstelle

Wurde die Zertifizierung von einer akkreditierten Zertifizierungsstelle ausgestellt? Für Österreich siehe https://akkreditierung-austria.gv.at/ (Suche nach 27001), für andere Länder siehe https://www.iaf.nu/

Verifizierung der Zertifizierung

Ist das Zertifikat über die Zertifizierungsstelle verifizierbar? In Österreich:

- CIS - Certification & Information Security Services GmbH
- TÜV AUSTRIA CERT GMBH
- Österreichische Computer Gesellschaft (OCG)

Sind Name und Adresse der zertifizierten Firma ident mit dem Dienstleister?

Wann erfolgte die Zertifizierung (je älter, desto weniger Aussagekraft)?

Ist das Zertifikat aktuell und zeitlich gültig (gültig bis)?

Wurde ein Zertifizierungs- oder ein Rezertifizierungsaudit durchgeführt? D.h. es wurden alle Anforderungen der Norm stichprobenartig überprüft.

Wurde ein Überwachungsaudit durchgeführt. Überprüfen Sie, welche Schwerpunkte im Rahmen des Audits gesetzt wurden?

Wurde die Zertifizierung unter Auflagen erteilt? Überprüfen Sie, ob die Mängel zwischenzeitlich beseitigt wurden bzw. Pläne zur Beseitigung der Mängel vorliegen.

Zertifizierte Norm

Welche Norm wurde verifiziert (z.B. ISO/IEC 27001 Informationssicherheit, ISO/IEC 27018 Datenschutz in der Cloud, ISO/IEC 27701:2019 Datenschutz)?

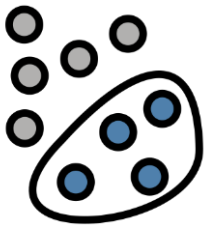
Umfang der Zertifizierung

Sind alle relevanten Organisationseinheiten, Geschäftsprozesse und Standorte des Dienstleisters von der Zertifizierung erfasst (Scope)?

Sind die von ihrem Institut bezogenen Services vom Scope der Zertifizierung abgedeckt?

Umfasst der Scope die ganze Organisation des Dienstleisters oder nur Teile?

Review der Erklärung zur Anwendbarkeit (Statement of Applicability):



- Wurden alle Kontrollen der jeweiligen Norm abgedeckt (vgl. z.B. ISO 27001:2013 Annex A). Welche Lücken bestehen im Hinblick auf die Sicherheitsanforderungen ihres Instituts?
- Welche Kontrollen wurden nicht implementiert und warum? Entspricht die Vorgehensweise den Sicherheitsanforderungen ihrer Organisation?

Wurden im Rahmen der Zertifizierung Nichtkonformitäten identifiziert? Sind diese relevant für ihr Institut?