ISO/IEC 27001
Certificate Review Checklist

Certification Authority

Was the certification issued by an accredited certification authority? For Austria see https://akkreditierung-austria.gv.at/ (search for 27001), for other countries see https://www.iaf.nu/

Verification of the Certification

Is the certificate verifiable via the certification authority? For Austria:

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

Are name and address of the certified company identical to the service organization?

When was the certification issued (the older, the less meaningful)?

Is the certificate current and valid in time (valid until)?

Has a certification audit or recertification audit been performed? I.e. all requirements of the standard were checked on a random basis.

Has a surveillance audit been performed? Check which focus was set within the scope of the audit.

Was the certification granted subject to conditions? Check whether the deficiencies have been eliminated in the meantime or whether there are plans to eliminate the deficiencies.

Certified Standard

Which standard was verified (e.g. ISO/IEC 27001 information security, ISO/IEC 27018 data security in the Cloud, ISO/IEC 27701:2019 data security)?

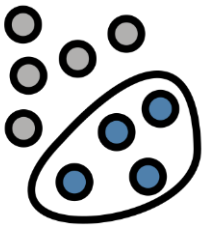
Scope of Certification

Are all relevant organizational units, business processes and locations of the service organization within the scope of the certification?

Are all of the services used by your institution covered by the scope of the certification?

Does the scope include the entire service organization or only parts of it?

Review of the Statement of Applicability:



- Have all controls of the respective standard been covered (e.g. ISO 27001:2013 Annex A). What gaps are there with regard to the security requirements of your institute?
- Which controls have not been implemented and why? Does the approach meet the security requirements of your organization?

Were non-conformities identified during the certification process? Are these relevant to your institution?