Requirements for Bodies Providing Star Certification
# Table of Contents

Introduction ......................................................................................................................................... 3  
1. General ....................................................................................................................................... 3  
Part 1 - Requirements ........................................................................................................................... 4  
2. Normative References ................................................................................................................ 4  
3. Terms and Definitions .................................................................................................................... 4  
4. Requirements for a Certification Body ....................................................................................... 4  
5. Scope of Certification .................................................................................................................... 5  
6. Audit Duration ............................................................................................................................... 5  
7. Assessing the ISO/IEC 27001 and the CCM together .................................................................. 5  
8. Audit and Certification .................................................................................................................. 6  
9. Control establishment .................................................................................................................... 6  
10. Control selection .......................................................................................................................... 6  
Part 2 Submitting Data to the CSA ....................................................................................................... 7  
11. Capability model .......................................................................................................................... 7  
12. Submitting Certification Data ..................................................................................................... 7  
13. Issuing Certification ..................................................................................................................... 7  
14. Appendix 1 ............................................................................................................................... 8
Introduction

The Security Trust Assurance and Risk (STAR) certification scheme is designed to comply with the following international standards:

- ISO/IEC 17021-1:2015, Conformity assessment – Requirements for bodies providing audit and certification of management systems
- ISO 19011:2018, Guidelines for auditing management systems

The STAR certification process is not meant to be a replacement for any ISO/IEC 27001 certification processes but as a supplement or extension of those processes. All Certifying Bodies (CB) shall continue to follow their internal accredited ISO/IEC 27001 schemes to establish confidence that the organization's ISMS is functioning adequately and to confirm that the ISMS can achieve continued compliance.

Where references to other standards have been included it is to highlight where comparable requirements can be found.

1. General

1.1 This document outlines the requirements CBs must meet in order to conduct a STAR certification assessment to the Cloud Controls Matrix (CCM) as part of an ISO/IEC 27001 assessment, incorporating additional requirements. Appendix 1 documents requirements where the two assessments are not conducted by the same CB.
1.2 The controls set out in the CCM can be considered additional controls in ISO/IEC 27001. Ref clause 6.1.3 in ISO/IEC 27001:2013.
1.3 This document should be considered as supplementary to ISO/IEC 27006 and serves to outline the additional requirements for the assessment of the CCM.
1.4 Part 1 lists Requirements for CBs. Part 2 is informative, and provides a description of how to submit data and certifications to the Cloud Security Alliance (CSA).
Part 1 - Requirements

2. Normative References

2.1 The following documents are indispensable in the application of this document:
- ISO/IEC 27006:2015, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 17021-1:2015, Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements
- ISO 19011:2018, Guidelines for auditing management systems
- Auditing the Cloud Control Matrix
- Any references to specific clauses in the above listed or other documents are not normative, and solely to help highlight relationships between documents.

3. Terms and Definitions

3.1 Cloud computing – A paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand (ISO/IEC 17788).

3.2 Cloud Service Provider – An organization providing cloud services to a Cloud Service Consumer. The term Client is used within this document when applying for CSA STAR L2 certification.

3.3 STAR Registry – A database managed by the CSA which stores the results of CCM assessments, including STAR certification assessments

4. Requirements for a Certification Body

4.1 A CB must be a CSA Corporate Member in good standing.
4.2 A CB conducting STAR certification assessments shall be ISO/IEC 17021-1 accredited by an IAF member accreditation body for issuing ISO/IEC 27001 certification.
4.3 A CB shall comply with all the requirements of this document, and where not specified herein, as well as both ISO/IEC 17021 and ISO/IEC 27006, when conducting a STAR certification assessment.
4.4 This document adds greater clarity concerning CCM specific audit areas. Competency requirements.
4.5 All assessors must be documented as registered as an ISO/IEC 27001 assessor for an IAF member accredited ISO/IEC 27001 certification body. Ref 7.2.1 in ISO/IEC 27006.

4.6 All assessors must demonstrate knowledge of the Cloud Services business sector. Ref 7.1.2.1.5 in ISO/IEC 27006:2015.

4.7 All assessors must have technical knowledge of the activity to be audited. Ref 7.2.1.1 b in 27006:2

4.8 The requirements of clause 5.2 may be met by achieving a passing mark to earn the most recent version of:
   • CSA’s Certificate in Cloud Security Knowledge (CCSK), or
   • Certified CSA STAR Auditor¹
   • CSA’s Certificate of Cloud Auditing Knowledge (CCAK), or other equivalent certificate that gives a similar level of grounding in cloud computing or information security applications.

5. Scope of Certification

5.1 An organization’s context shall clearly define what functions are within the scope of certification.

5.2 A scope that could be misleading to a client shall not be allowed. Certification bodies shall ensure that the client’s information security risk assessment and risk treatment properly reflects its activities and extends to the boundaries of its activities as defined in the scope of certification. Certification bodies shall confirm that this is reflected in the client’s scope of their ISMS and Statement of Applicability. Ref clause 9.1.3.5 in ISO/IEC 27006.

5.3 The scope of the ISO/IEC 27001 certification must not be less than that of the scope of the STAR certification.

5.4 Scopes shall be written to reflect as closely as possible the full chain of critical activities that have implications for the client’s data, their users’ data, or the service they provide.

6. Audit Duration

6.1 An Initial CCM audit shall be planned (at minimum) as an additional 50% of total audit time compared to the underlying calculation for the ISO/IEC 27001 Initial audit and adjusted for surveillance audit as appropriate. Ref B.3.3 and B.4 in ISO/IEC 27006.

6.1 Sampling is permitted in line with ISO/IEC 27006.

7. Assessing the ISO/IEC 27001 and the CCM together

7.1 There will be no reduction in the time that would usually be allocated to the assessment of ISO/IEC 27001 when conducting a combined ISO/IEC 27001 and STAR certification assessment. However, where there is overlap in the auditing requirements of ISO/IEC

¹ https://bsi.learncentral.com/shop/Course.aspx?id=23192&name=Certified%2BCSA%2BSTAR%2BAuditor
27001 and the CCM, duplication of effort should be avoided.

7.2 To make the identification of duplicative areas easier, the overlapping objectives of ISO/IEC 27001 have been referenced in the CCM.

8. Audit and Certification

8.1 A CCM assessment cycle will follow the assessment cycle for ISO/IEC 27001. Ref clause 9.6 in ISO/IEC 27006.

NOTE: It is a mandatory requirement (ref: GTB NO. 12082019-001) that a Consensus Assessments Initiative Questionnaire (CAIQ) self-assessment under the current version is submitted to the CSA and added to the STAR database by the applicant organization prior to any audit activity to facilitate planning and to serve as evidence of preparedness.

8.2 For an organization obtaining both ISO/IEC 27001 and STAR certification for the first time in parallel, there will be a 2-part initial assessment comprising the requirements of both ISO/IEC 27001 and the CCM followed by surveillance visits. Over a 3-year period, the surveillance visits will cover the full range of ISO/IEC 27001 and the CCM. A recertification assessment will be conducted at the end of the cycle.

8.3 For an organization adding STAR certification to an existing ISO/IEC 27001 certification, the full applicable control set will be audited on the first visit. This can be done on any type of visit provided that additional time allocated to audit the CCM is applied per clause 7.1.

8.4 When there is a request to transfer an existing CSA STAR certificate, the requirements of IAF MD 2 should be applied. The accepting CB should verify that the requirements of clause 4 of this document have been met by the issuing certification body at the time of issuance for the certificate to be transferred.

9. Control establishment

9.1 There must be evidence that a control has been in place and is effective.

NOTE: This would usually mean a control of some description would have been in place for 3 months. However, if evidence could be collected to demonstrate that the control was effective over a shorter period of time, this could be considered.

10. Control selection

10.1 In some cases a control may not be applicable. Any exclusion of a control area must be properly justified as described in ISO/IEC 27001. Ref clause 6.1.3 d in ISO/IEC 27001.

10.2 Compensating controls are acceptable where there is sufficient evidence that the replacement control provides the same control coverage as the original control.

NOTE: A compensating control, also called an alternative control, is a mechanism that is put in place to satisfy the requirement for a security measure that is deemed too difficult or impractical to implement at the present time.
Part 2 Submitting Data to the CSA

11. Capability model

11.1 The CCM shall be audited against a management capability model. Guidance on how to audit this model can be found in the CSA’s document ‘Auditing the Cloud Controls Matrix’.

11.2 All STAR certification assessments must be audited using the cloud control matrix and the maturity model grid as defined in the document ‘Auditing the Cloud Control Matrix’.

12. Submitting Certification Data

12.1 Following an assessment, an organization can choose to make their certification public on the STAR registry. Normally, maturity scores are not made public on the certificate or registry and reports are for internal use only. If reports are shared or made public, they shall be shared in their entirety.

12.2 The certification body shall submit all required certification registration information using the CSA STAR Registry Submission webpage.

13. Issuing Certification

A STAR certification shall not be issued unless the applicant organization has obtained, and maintains, a valid IAF accredited ISO/IEC 27001 certification.
14. Appendix 1

Providing STAR certification for Organizations that have been certified to ISO/IEC 27001 by another CB.

Introduction

There are times when an organization holds an ISO/IEC 27001 certification with a CB that is not accredited by CSA and wishes to obtain CSA STAR certification. It is recommended that the CB obtains accreditation by CSA or the organization transfers their ISO/IEC 27001 certification to an CSA accredited CB. However, there are cases that, for whatever reason, they may not wish (or cannot) change CBs or the CB cannot obtain accreditation.

In those cases, CSA allows CSA accredited CBs to carry out a STAR certification but there will be additional due diligence and audit time required. This appendix specifies those requirements.

A.1 The CB shall conduct validation of the risk assessment, as well as the Statement Of Applicability, as these are two critical areas where the organization would be addressing conformity with the CCM controls:

The review shall cover the following aspects as a minimum and the review and its findings shall be documented:

i. confirmation that the applicant organization's ISO/IEC ISO 27001 certification falls within the accredited scope of the issuing and accepting certification body and includes the scope related to the cloud service;
ii. confirmation that the issuing certification body is accredited to ISO/IEC 27001 by an IAF member;
iii. the reasons for seeking a CSA STAR certification from a separate CB;
iv. that the site or sites wishing to be certified are within the scope of the valid accredited ISO/IEC 27001 certification;
v. the initial certification or most recent recertification audit reports, and the latest surveillance report; the status of all outstanding nonconformities that may arise from them and any other available, relevant documentation regarding the ISO/IEC 27001 certification process.
vi. If these audit reports are not made available or if the surveillance audit or recertification audit has not been completed as required by the ISO/IEC 27001 issuing certification body's audit programme, then certification to CSA STAR will be denied;
vi. complaints received and action taken;
viii. considerations relevant to establishing an audit plan and an audit programme. The audit programme established by the issuing ISO/IEC 27001 certification body shall be reviewed if available.
ix. The accepting certification body should plan for additional audit time of the CCM when these conditions apply to allow for adequate inspections of these criteria.
A.2 Because of the above due diligence that must be carried out in addition to the maturity assessment it is expected that a CSA STAR audit would be no less than the number of days required for a full ISO/IEC 27001 initial audit.

A.3 All CSA STAR certificates shall reference the ISO/IEC 27001 unique identification code. Ref: 8.2.2d in ISO/IEC 17021.