cloud security alliance℠

Requirements for Bodies Providing STAR Certification

Release 1: 07/16/2013

Contents

Introduction

To be consistent with international standards, the STAR certification scheme is designed to comply with:

- ISO/IEC 17021:2011, Conformity assessment – Requirements for bodies providing audit and certification of management systems
- ISO/IEC 27006:2011, Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
- ISO 19011, Guidelines for auditing management systems

This manual is not meant to be a replacement for any ISO/IEC 27001 certification process. Rather, it is a supplement or extension of those processes. All certifying bodies shall continue follow their internal accredited ISO/IEC 27001 scheme manuals to establish confidence that the organization's ISMS is functioning adequately and to confirm that the ISMS is capable of achieving 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 how to conduct a STAR certification assessment of the Cloud Controls Matrix (CCM) as part of an ISO 27001 assessment.

1.2 The controls set out in the CCM can be considered additional controls in ISO 27001. *Ref clause 4.2.1 g in ISO/IEC 27001:2006.*

1.3 No certificate for a CCM assessment is valid without an accompanying ISO 27001 certificate with a scope that is equal to, or greater than, that of the STAR certification.

1.4 A certification body conducting a CCM assessment must comply with ISO 27006.

1.5 This document should be considered as supplemental to ISO 27006 and serves to outline the additional requirements for the assessment of the CCM.

1.6 Certification bodies must comply with parts 1 and 2 of this document. Part 2 provides a description of how the certification scheme will operate.

1.7 In order to conduct the STAR certification assessment, a certification body must comply with this document to the satisfaction of the Cloud Security Alliance (CSA).

Part 1 – Requirements

2. Normative References

2.1 The following documents are necessary for the application of this document:

- BS ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems – Requirements
- ISO/IEC 27006:2011**,** Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems
- ISO 19011, Guidelines for auditing management systems

2.1.1 Any references to specific clauses in other documents are to help highlight correspondences between documents.

3. Terms and Definitions

3.1 Cloud computing – Computing resources delivered over a network

3.2 Cloud Service Provider – An organization providing cloud services

3.3 STAR Database – A database run by the CSA which stores the results of assessments of the CCM

4. Requirements of a Certification Body

A certification body conducting CCM assessments shall be accredited to ISO 27006 by an International Accreditation Forum (IAF) member accreditation body for delivery of ISO 27001 assessments.

4.1 A certification body shall comply with all the requirements of ISO 27006 as well as this document's requirements when conducting a CCM assessment.

4.2 This document adds greater clarity for areas specific to auditing the CCM, but does not relieve a certification body of its obligation to comply with ISO 27006 when conducting an assessment.

4.3 This document adds greater clarity for areas specific to auditing the CCM, but does not relieve a certification body of its obligation to comply with ISO 27006 when conducting an assessment.

5. Competency Requirements

5.1 All assessors must be able to present evidence of passing an accredited lead auditor course for ISO 27001 or be a qualified and experienced ISO 27001 assessor for an IAF member accredited ISO 27001 certification body. *Ref 7.2.1.3.1 c in ISO 27006.*

5.2 All assessors must have completed a BSI/CSA CCM course. *Ref 7.2.1.3.1 c* in 27006.

5.3 All assessors must have a minimum of two years of experience working in information security. *Ref 7.2.1.3.1 e in 27006.*

5.4 The requirements of clause 5.3 are not necessary if the assessor has earned the CSA's Certificate in Cloud Security Knowledge (CCSK) or completed an alternative course that gives a similar level of knowledge in cloud computing or information security applications.

6. Scope of Certification

6.1 An organization's scope shall clearly define what functions are within the scope of certification.

6.2 A scope that could be misleading to a client or a scope that excludes an area of an organization that a client might assume is covered in the scope of registration shall not be allowed. *Ref clause 9.1.2 in ISO 27006*.

6.3 The scope of the ISO 27001 certification must not be less than the scope of the STAR certification.

6.4 Scopes will be written to reflect as closely as possible the full chain of critical activities that have implications for the clients' data or the service they receive. It will cover the core service-level agreements that the organization has with its clients.

7. Audit Time

7.1 Audit durations for conducting an ISO 27001 assessment combined with a CCM assessment will be a minimum of 1.5 times the duration required for an ISO 27001 assessment as defined in ISO 27006. *Ref clause 9.1.3/9.1.4 ad Annex C in ISO 27006.*

7.2 Sampling will be permitted in accordance with ISO 27001.

8. Assessing the ISO 27001 and the CCM Together

8.1 There will be no reduction in the time that would usually be allocated to the assessment of ISO 27001 when conducting a combined ISO 27001 and CCM assessment. However, where there is overlap in the auditing requirements of ISO 27001 and the CCM, duplication of effort should be avoided. To make identifying areas of potential duplication easier, the corresponding areas of ISO 27001 have been referenced in the CCM.

9. Audit and Certification

9.1 An assessment cycle will follow the assessment cycle for ISO 27001. *Ref clause 9.2 /9.3 /9.4 in ISO 27006.*

9.2 For an organization simultaneously getting both ISO 27001 and STAR certification for the first time, there will be a two-part initial assessment covering all of the requirements of ISO 27001 and the CCM followed by surveillance visits. Over a three-year period, the surveillance visits will cover the full range of ISO 27001 and the CCM. A recertification assessment will be conducted at the end of the cycle.

9.3 For an organization adding STAR certification to an existing ISO 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 the time allocated to audit the CCM is an additional 50% of the time that would be required to conduct a recertification visit.

10. Control Establishment

10.1 There must be reasonable evidence that a control has been in place and is effective. This would usually mean a control of some description would have been in place for three months. However if evidence could be collected to demonstrate that the control was effective over a shorter period of time, this could be considered.

11. Control Selection

11.1 In some cases a control may not be applicable. Any exclusion of a control area must be properly justified as described in ISO 27001. *Ref clause 4.2.1 g in ISO 27001*.

11.2 Compensating controls are acceptable where one control in the CCM is rendered redundant by measures taken in other control areas.

Part 2 – Submitting Data to the CSA

12. Capability Model

12.1 The CCM will be audited against a management capability model. Guidance on how to audit to this model can be found in the CSA's document 'Auditing the Cloud Controls Matrix'.

12.2 All STAR certification assessments must be audited following the guidelines in the document 'Auditing the Cloud Control Matrix'.

13. Submitting Scores

13.1 Following an assessment, an organization can choose to make their certification public on the STAR register. They can choose one of the following options:

- Disclose that they have been assessed against the CCM, but chose not to disclose any score
- Disclose a summary score, but not disclose the score for individual controls areas in the CCM
- Full disclosure of the scores for each control area

13.2 It will be the responsibility of the certification body to ascertain what level of disclosure the organization is prepared to make.

13.3 Following the client's consent, certification bodies shall submit the scores to the CSA for listing on the CSA's STAR database through a mutually agreed data exchange program.

14. Issuing Certification

14.1 A STAR certification certificate cannot be issued unless the organization has passed their ISO 27001 assessment.