Code of Practice for Implementing STAR Level 2

Acknowledgments

Authors:

Ashwin Chaudhary
John Di Maria
Walter Williams

Reviewers/Contributors:

Willibert Fabritius
David Forman
Ryan Mackie
Debbie Zaller

The CSA Security, Trust, Assurance and Risk (STAR) Registry documents the security and privacy controls provided by popular cloud computing offerings. This publicly accessible registry allows consumers to assess their security providers in order to make the best procurement decisions.

Table of Contents

STAR Certification

What is the CSA STAR Certification?

STAR Certification: For ISO/IEC 27001:2013

The CSA STAR Certification leverages the requirements of the ISO/IEC 27001:2013 management system standard together with the CSA Cloud Controls Matrix. Certification certificates follow normal ISO/IEC 27001 protocol and expire after three years. You must be ISO/IEC 27001 certified by an accredited Certification Body to apply for the STAR Certification, or you can get the ISO/IEC 27001 certification and STAR together. A CSA STAR certificate will have the same expiration date as the underlying ISO/IEC 27001 certificate.

Steps to Earn a STAR Level 2 Certification

Step 1: You will need to complete a Level 1 Self-Assessment submission prior to apply for a STAR Certification. For this you will need to download and fill out the Consensus Assessment Initiative Questionnaire (CAIQ). The CAIQ is the questionnaire associated with the Cloud Controls Matrix (CCM). The CAIQ provides a set of questions to determine if the CCM controls have been implemented.

Step 2: Submit your completed CAIQ to the STAR Registry.

Step 3: Next you will need to prepare for the ISO/IEC 27001 Audit against the Cloud Controls Matrix (CCM). Download the Cloud Controls Matrix (CCM) and be sure to read it and understand the content and requirements. You will have to comply with the controls to earn your certification.

Step 4: Choose a STAR Certified Auditor to conduct your audit. They will provide you with details regarding pricing, audit days required and process. After the successful conclusion the certification body you select will submit your certification to the STAR Registry for you.

Step 5: Once your STAR Certifying Body makes your submission, both your certification body and the point of contact from your organization will receive a confirmation email.

Step 6: Promote your certification to potential customers by displaying the STAR Level 2 logo on your website. Oftentimes companies will create a page to display their badges and certifications and promote their certification with a hyperlink that goes directly to their submission.

Submission materials you will need to fill out

Your organization will need to complete the following two documents in order to earn your STAR Level 2 certification. Everything else will be completed by your chosen certification body.

- CAIQ v3.1 or v4.0: This is the required self-assessment
- CCM v3.0.1 or v4.0: These are the controls that will be used to confirm your compliance during a third party audit.

Guidance for Implementing the Cloud Controls Matrix

Below are the steps you will need to take when implementing the Cloud Controls Matrix:

- Create an information security risk management capability, assess risks, create and operate the risk treatment plan.
- From this, select the controls from the CCM that are in scope to remediate your risks. Implement the controls to remediate the identified risks. You must justify any controls not in place or not applicable. Any additional controls must be part of your Statement of Applicability (SOA). Please note that this SOA should be the same SOA as you have already for your ISO/IEC 27001 ISMS.
- Establish objectives and success criteria for each control and measure the controls' performance. Create and operate a plan for when controls (e.g. procedures and technical measures) don't conform to policy.
- Constantly work to improve your ISMS and all of your controls and use the CCM to benchmark yourself

Preparing for the ISOIEC 27001 Audit against the Cloud Controls Matrix

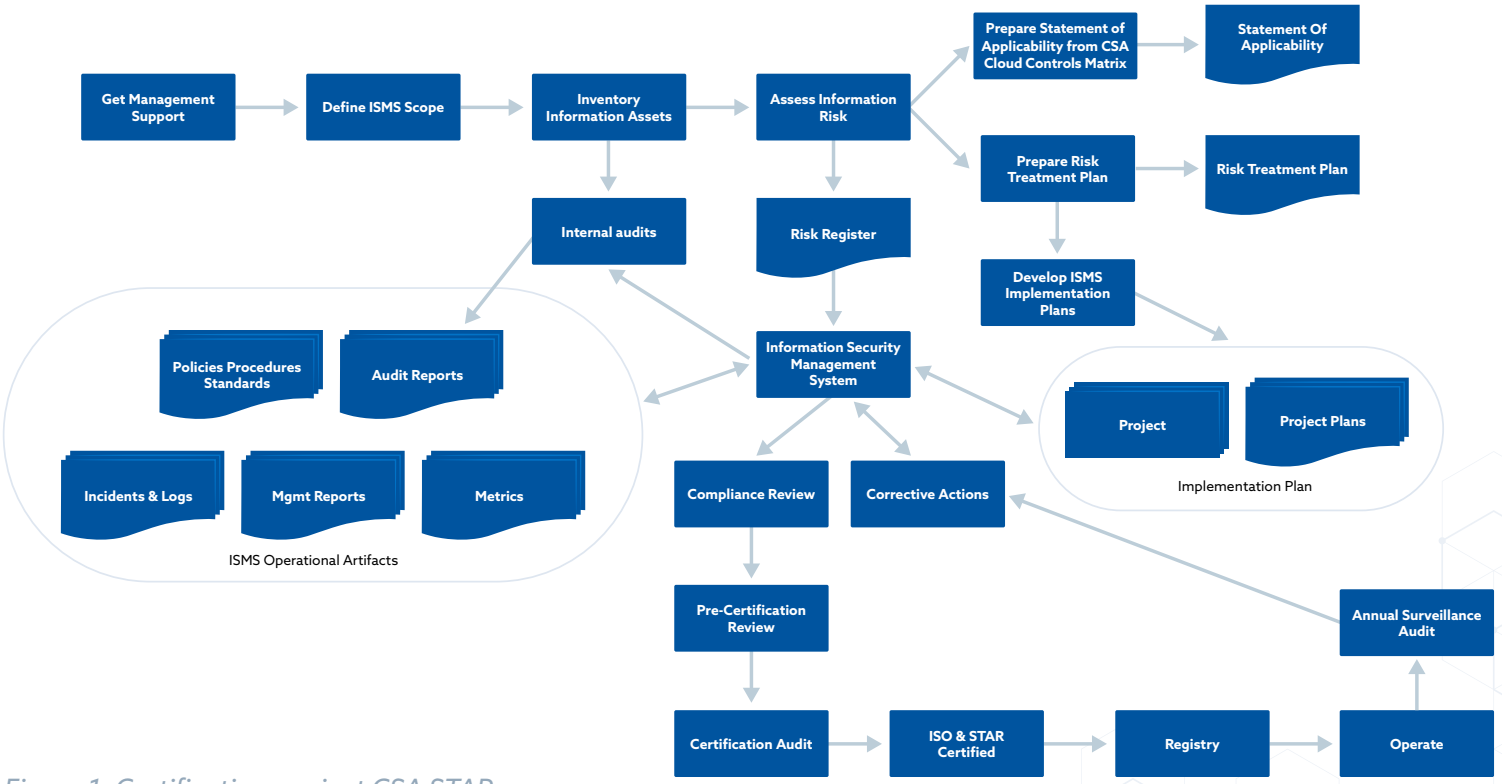

Figure 1: Certification against CSA STAR

The following are tips and recommendations when preparing for an audit against the CCM:

- Most ISO/IEC 27001 auditors will expect to audit against ISO 27002 (Annex A of ISO/IEC 27001) plus the management system requirements outlined in the ISO/IEC 27001 specification in the stage 2 audit. And this means that the process for management review, internal audits, training, and continual improvement must include STAR requirements.
- You define your controls, not your auditor.
- You must set the appropriate controls for your audit inside of a functioning Information Security Management System.
- Your Statement of Applicability (SoA) must be based on the Cloud Controls Matrix. You still can choose what is appropriate for your organization based upon both the type of service and risk to the organization. (See Figure 1)
- You also must undergo an internal audit by an informed but independent individual or team.
- Any controls in ISO 27001 Appendix A that are not mapped to the CCM must either be in scope for the audit, or you must document why you can accept the risk of not adopting those controls.
- During the audit, your organization will be measured against the CCM plus the STAR Maturity Model which measures how well the process is managed and outlines the strengths and weaknesses based on the CCM domains. This is an internal report and is used to improve your process year to year.
- Each year you will expect to have improved upon the prior year based upon your measurement of the effectiveness of your controls. This means you have to know what success looks like and can't just do check box security.
- Nonconformities (if present) will be noted and certification will be delayed or cancelled if not corrected.
- At the end of your three year certification cycle, your organization will be re-certified along with your ISO/IEC 27001 certification.
- Normal ISO/IEC 27001 protocol will be followed and a joint report will be issued.

Figure 2

Figure 3

Information Needed for the STAR Registry Listing

Note: You must have completed a Level 1 Self-Assessment submission prior to submitting a STAR Certification.

You will need to provide an adequate organization name, website, and description for your certifying body to upload to the STAR Registry along with your certification.

- **Organization Name:** This is the name of the organization you are making the submission for.
- **Organization Contact Name and Email:** You must provide a point of contact for your submission. The contact is the person who will "own" the registry entry and be contacted for any future questions concerning the entry. Their email needs to be a valid company email in order to receive a confirmation email from CSA.
- **Link to your Organization's Website:** This should be the URL of the main website.
- **Your Organization's Description:** The description should be a brief summary of your organization.
- **Cloud Service Name:** This is the name of the cloud service provided by the organization you are submitting for. The name can be the same as the company, but if the organization has a specific name for the service, we recommend using this instead.
- **Cloud Service Description:** The description should be a brief summary of the cloud service itself.

STAR Attestation

What is the CSA STAR Attestation?

The CSA STAR Attestation leverages the requirements of the AICPA governed SOC 2 Type 2 Attestation along with the CSA Cloud Controls Matrix. Assessment review periods are determined by the client but should be no less than 6 months. For STAR Attestation, the renewal period is every 12 months. You must have a SOC 2 Type 2 Attest report to apply for STAR Attestation, or you can get the SOC 2 Type 2 and STAR together.

Organizations that are applying for their first STAR Attestation over a cloud system, can provide a SOC 2 Type 1 report to the CSA to support their application. For subsequent applications of the same cloud system, only a SOC 2 Type 2 report will be accepted. In other words, a system can only complete a SOC 2 Type 1 STAR Attestation report once. If an organization has more than one system, each system can gain STAR Attestation once, using a SOC 2 Type 1 report.

A STAR Attestation obtained based on a SOC 2 Type 1 report is only valid for 6 months from the report date because this type of report addresses the suitability of design of implemented controls as of a point in time. The report date is the as-of date the controls were suitably designed and implemented. The report date

is not referring to the date of the report of the Certified Auditor for STAR Attestation, or opinion letter. An organization that received their STAR Attestation based on a SOC 2 Type 1 report is required to submit a SOC 2 Type 2 report to maintain uninterrupted STAR Attestation status within 18 months or less. A STAR Attestation based on SOC 2 Type 2 is valid for 1 year from the reporting period end date.

Steps to earn a STAR Level 2 Attestation

Step 1: You will need to complete a Level 1 Self-Assessment submission prior to submitting a STAR Attestation report for Level 2. For this you will need to download and fill out the Consensus Assessment Initiative Questionnaire (CAIQ). The CAIQ is the questionnaire associated with the Cloud Controls Matrix (CCM). The CAIQ provides a set of questions to determine if the CCM controls have been implemented.

Step 2: Submit your completed CAIQ to the STAR Registry.

Step 3: Next you will need to prepare for the SOC 2 Type 2 or Type 1 Attestation against the Cloud Controls Matrix (CCM) and the SOC 2 Trust Services Criteria. Download the Cloud Controls Matrix (CCM) and be sure to read it and understand the content and requirements. You will have to comply with the applicable controls to earn your STAR Attestation.

Step 4: Choose a Certified Auditor for STAR Attestation to conduct your engagement . They will provide you with details regarding pricing, engagement days required and process. The auditor you select will submit your Attestation to the STAR Registry for you.

Step 5: Once your Certified Auditor for STAR Attestation makes your submission, both your auditor and the point of contact from your organization will receive a confirmation email.

Step 6: Promote your STAR Attestation to potential customers by displaying the STAR Level 2 logo on your website. Oftentimes companies will create a page to display their badges and audit reports then promote their attestations with a hyperlink that goes directly to their submission.

Submission materials you will need to fill out

Your organization will need to complete the following two documents in order to earn your STAR Level 2 Attestation. Everything else will be completed by your chosen Certified Auditor for STAR Attestation.

- CAIQ v3.1 or v4.0: This is the required self-assessment
- CCM v3.0.1 or v4.0: These are the controls that will be used to confirm your compliance during the engagement.

Guidance for Implementing the Cloud Controls Matrix

Below are the steps you will need to take when implementing the Cloud Controls Matrix:

- Create an information security risk management capability, assess risks, create and operate the treatment plan.

- From this, select the controls from the CCM that are in scope to remediate your risks. Put them into place and remediate them.

Preparing for the SOC 2 Type 2 Attestation against the Cloud Controls Matrix

The following are tips and recommendations when preparing for the STAR Attestation against the CCM.

- The STAR Attestation must include the Security Category as one of the 5 AICPA Trust Services Criteria (TSC). The Security Category includes the Common Criteria as outlined in Figure 4 below
- You define your controls, not your auditor.
- You must set the appropriate controls for your environment and ensure they are suitably designed to meet the applicable criteria.
- 100% of the CCM controls will be evaluated. Any controls that are deemed not applicable must be justified within the report.
- The auditor will map the TSC to the CCM including all CCM domains.
- The STAR Attestation is a SOC 2 report that includes the CSA's CCM; therefore, the report should follow AICPA guidance for a SOC 2.

Figure 4

Information Needed for the STAR Registry Listing

Note: You must have completed a Level 1 Self-Assessment submission prior to submitting a STAR Attestation.

You will need to provide an adequate organization name, website, and description for your Certified Auditor for STAR Attestation to upload to the STAR Registry

- **Organization Name:** This is the name of the organization you are making the submission for.
- **Organization Contact Name and Email:** You must provide a point of contact for your submission. The contact is the person who will "own" the registry entry and be contacted for any future questions concerning the entry. Their email needs to be a valid company email in order to receive a confirmation email from CSA.
- **Link to your Organization's Website:** This should be the URL of the main website.
- **Your Organization's Description:** The description should be a brief summary of your organization.
- **Cloud Service Name:** This is the name of the cloud service provided by the organization you are submitting for. The name can be the same as the company, but if the organization has a specific name for the service, we recommend using this instead.
- **Cloud Service Description:** The description should be a brief summary of the cloud service itself.

Conclusion - Next Steps

After you've earned STAR Level 2 evaluate your training needs. Then be sure to re-evaluate based on any gaps you've identified during your assessment. This will help you to embed the knowledge within your organization.

In order for a STAR Certification or Attestation to be effective, it should be integrated into the larger goals of the organization. Beyond just earning the certification, take a look at how the combination of assessments, training and tools can work together to achieve better security for your organization.

Training

- Evaluate your training needs to get started
- Re-evaluate based on the gaps you've identified
- This will help embed the knowledge

Reinforced Assessment Next Generation

An integrated offering where the whole is greater than the sum of it's parts.

Figure 5

Summary - What you need to do

1. **Set up:** Set up a project team to manage the implementation
2. **Communicate:** Communicate the project across the whole organization
3. **Create:** Create an implementation plan and monitor progress
4. **Take:** Take a fresh look at your total business
5. **Highlight:** Highlight the changes as opportunities for improvement
6. **Make:** Make changes to your documentation to reflect the new structure (as necessary)
7. **Implement:** Implement the new requirements on leadership, risk and context of the organization
8. **Review:** Review the effectiveness of your current control set
9. **Carry out:** Carry out an impact assessment
10. **Start:** Start measuring ROI