CSA cloud security alliance℠

STAR™ CERTIFICATION

Guidance Document

Auditing the Cloud Controls Matrix

Release 1: 08/08/2013

Contents

1. Introduction

The purpose of this document is to provide guidance to certified bodies and associated organizations that are performing audits or supporting certification activities related to STAR certification.

STAR certification and the associated management capability model:

1. Give a prospective customer of the certified organization a greater understanding of the level of control that the organization has in place
2. Highlight areas where an organization might wish to improve
3. Ensure that the Cloud Controls Matrix (CCM) does not become the minimum requirement, but through the model also characterizes best-in-class performance

Therefore, there are both internal (business improvement) and external (customer reassurance and transparency) reasons for auditing to a management capability model.

One of the key objectives of the scheme is to ensure that the scope of the cloud service provider fits for the consumer's needs and is service-level agreement (SLA) driven.

2. How does this process provide reassurance to a client of the certified organization?

- ISO 27001 requires the organization to evaluate their customers' requirements and expectations, as well as contractual requirements. As a result, it requires that the organization has implemented a system to achieve this evaluation.
- ISO 27001 requires the organization to conduct a risk analysis that identifies the risks to meeting their customers' expectations.
- The CCM requires the organization to address the specific issues that are critical to cloud security.
- The Maturity Model assesses how well managed activities in the control areas are.

No certification can ever guarantee information is 100% secure; however, ISO 27001 certification and STAR certification ensure that an organization has an appropriate system for the type of information it is dealing with, that it is well managed, and that it is focused on cloud-specific concerns.

3. Assigning a score to an organization

An organization must demonstrate that it has all of the controls in place and is operating effectively before an assessment of the management capability around the controls can occur. If the organization has a major nonconformity against any of the controls in the control area, the maximum score achievable for that control area is 6.

When an organization is audited, a Management Capability Score will be assigned to each of the control areas in the CCM. This will indicate the capability of the management to ensure that the control is operating effectively in this area. The 11 control areas in CCM version 1.4 are listed below.

CONTROL AREAS
1. Compliance
2. Data Governance
3. Facility Security
4. Human Resources
5. Information Security
6. Legal
7. Operations Management
8. Release Management
9. Resiliency
10. Risk Management
11. Security Architecture

The management capability of the controls will be scored on a scale of 1-15. These scores have been divided into five different categories that describe the type of approach characteristic of each group of scores.

SCORE	DESCRIPTOR
1-3	No Formal Approach
4-6	Reactive Approach
7-9	Proactive Approach
10-12	Improvement-Based Approach
13-15	Optimising Approach

When assigning a score to a control area, the five factors below will be considered. The lowest score against any one of those five factors will be the score awarded for the control area.

FACTORS
1. Communication and Stakeholder Engagement
2. Policies, Plans and Procedures, and a Systematic Approach
3. Skills and Expertise
4. Ownership, Leadership, and Management
5. Monitoring and Measuring

In summary, there are a number of control areas on the CCM that will each be awarded a management capability score on a scale of 1-15. To decide what the score is, each control area will be considered against five capability factors.

4. The assessor’s grid

In order to make it possible for an assessor to consistently apply a score to the control area, the grid below outlines what would be required of an organization to achieve each score.

Score		1 to 3	4 to 6	7 to 9	10 to 12	12 to 15
Factors		No formal approach	Reactive	Proactive	Improving	Innovating
Communication and Stakeholder Engagement	Evidence / Definition	1. There is no evidence that stakeholders have been identified.	4. Some evidence that stakeholders are identified and some communication takes place.	7. Stakeholders are systematically identified.	10. Stakeholders are actively engaged in improving measures in the control.	13. Control area owners actively share best practice to support development in other areas of the business.
	Managed	2. Some stakeholders have been identified but communication does not take place.	5. Key communications are disseminated to relevent stakeholders.	8. Stakeholders are consulted over proposed changes.	11. Stakeholders have a clear understanding of how changes in the control area affect their area of responsibility.	14. Control area owners actively share best practice to support development in other areas of the business.
	Followed / Effective	3. Communication takes place but there is no evidence that it is effective.	6. There evidence that most communication is effective.	9. The effectiveness of the communication process is monitored and reviewed.	12. Methods of communications are reviewed to ensure they are effective.	15. Stakeholders understand how the control area will need to develop to meet the organisations strategic objectives.
Policies, Plans, Processes and Procedures, and a systematic approach	Evidence / Definition	1. There is little evidence that plans, processes, policies or procedures are in place.	4. There is evidence that some staff are aware of processes for core areas of the control.	7. Comprehensive plans, policies, processes and procedures cover most areas of operation in the control.	10. Plans, policies, processes and procedures cover contingency operations as well as routine operations.	13. There is strong leadership to align all the plans, policies processes and procedures within the control area to drive coherent changes in the system they form part of.
	Managed	2. A limited number of processes are in place.	5. Most plans, processes, policies and procedures are up to date.	8. Plans processes and procedures are routinely reviewed.	11. Plans, Policies, Processes and Procedures are reviewed against the risks and opportunities associated with the context of the organisations activities.	14. Plans policies and procedures are compared with best practice within and outside the organisation.
	Followed / Effective	3. Processess are followed in some key areas.	6. There is evidence that these plans, polices, processes and procedures are usually followed.	9. Staff know or can find out how to access relevant plans, policies, processes and procedures.	12. Staff are actively involved in risk management and mitigation.	15. Changes to plans, policies, processes and procedures are made with an appreciation of how they align with the vision of the organisation.
Skills and Expertise	Evidence / Definition	1. The skills and expertise to opperate in the control area are poorly understood	4. The competencies required to perform key tasks in the control area are defined.	7. The competencies required to perform all key activities in the control area are defined and where appropriate documented.	10. Staff training includes a full range of business continuity plans.	13. Succession planning is in place to ensure the continuity of skills.
	Managed	2. There is some evidence that staff competency is reviewed.	5. There is some evidence that staff competence is recorded or monitored.	8. Staff competency for all key areas of the control is monitored and where appropriate recorded.	11. Staff competence is continually monitored to identify any weaknesses and improved where weaknesses are found.	14. Resources are managed to ensure the competent staff are always available to react to issues in an appropriate time scale.
	Followed / Effective	3. There is little evidence that staff have the skills to conduct the tasks associated with the control area effectively.	6. There is evidence that staff are competent to operate the core activities in the control area.	9. There is evidence that staff have competence to perform all key activities within the control area.	12. Staff can demonstrate knowledge of business continuity planning.	15. Best practice in training is considered across the organisation.
Ownership, Leadership and Management	Evidence / Definition	1. Ownership of the control area can not be identified.	4. The control area owner understands the key activities within the control area.	7. The control area owner actively reviews the control area to ensure they alligned with customer requements.	10. Risk analyses are regularly review by people empowered to take action.	13. Issues in the control area can be rapidly escalated and can result in action.
	Managed	2. The control area owner recognises their responsibility.	5. The control area owner understands the broader implication of actions within the control area.	8. There clear leadership in addressing issues identified in the review.	11. There is clear leadership in driving improvements in the control area to manage risk.	14. There is clear succession planning in place for leadership positions.
	Followed / Effective	3. The control area owner understands the scope of the control area.	6. The control area owner is empowered to provide the resources required to fix issues in the control area.	9. The control area owner is empowered to provide the resources required to take preventive action where it is justified.	12. The resources are made available to make proactive improvements to prevent potential risks posing a threat.	15. There is clear leadership in aligning activities within the control area with the overall business strategy.
Monitoring and Measuring	Evidence / Definition	1. There is little evidence that the control area is monitored or measured.	4. Formal monitoring covers key areas of operation.	7. Tools and automated techniques are employed or have been evaluated to improve reliability of the monitoring and measuring processes.	10. Monitoring information is analysed using statistical techniques to identify anomalies.	13. The capability of monitoring procedures to detect issues are regularly tested.
	Managed	2. There some evidence that monitoring or measuring information is reviewed.	5. Monitoring information is reviewed in a timely manner.	8. Monitoring information is formally analysed.	11. Anomalies are investigates and where appropriate action is taken.	14. Monitoring processes are reviewed every time significant changes in the control area occur.
	Followed / Effective	3. There is limited evidence that monitoring and measurments are routinely carried out.	6. Monitoring is likely to pick up key risks identified by the organisation.	9. Monitoring is capable of detecting a comprehensive range of issues in the control area.	12. Monitoring processes are reviewed regularly in line with a thorough risk analysis.	15. Approaches to monitoring are routinely benchmarked with industry best practice.

5. How will an assessor use this grid?

This grid should be used to assign an overall score to each of the control areas in the CCM (e.g., data governance or facilities security). The Maturity Model aims to assess the maturity of the management processes in place around the controls. In most cases, an organization will apply a common management approach across all of the controls in a control area. Therefore, one maturity score will be applicable to the whole control area. In cases where multiple management approaches are taken, different controls in the same control area could be awarded different scores. In this circumstance the lowest score should be taken. When a maturity score is applied to the whole control area it is easier to justify the maturity level, as described in the scenario below:

Individual controls are too specific to make it possible to assign a level to them in isolation. Consider, for example, DG-06 – "*Production data shall not be replicated or used in non-production environments."* This control would not require much in the way of "*skills or training*" or "*leadership.*" However, if you look across the full range of data governance controls, there is scope to assess the majority of the factors on this matrix. Take, for example, DG-01 – "*All data shall be designated with stewardship with assigned responsibilities defined, documented and communicated."* This control would allow an assessor the opportunity to evaluate the capability of a number of factors that could not be ascertained just by looking at DG-06.

6. How does an assessor approach scoring a control area?

1. The assessor will look at all of the controls in the control area to ensure that, based on the risk assessment, the organization had implemented the appropriate controls. If a control was not directly addressed, the client would need to demonstrate why it was not covered through their risk assessment or statement of applicability, or through compensating controls.
2. The assessor will decide which of the five factors could be applied to the controls in the control area (all factors are applicable to most control areas in most organizations, but in some circumstances only some of the factors should be considered).
3. The assessor will look for evidence of the organization's capability to manage these factors.
    a. It is expected that similar management structures will span all of the individual controls within a control area. However, if there are significantly different management approaches in the control area, the organization will be awarded the score for the weakest management approach. There are more likely to be multiple management approaches in place in the information security control area.
4. In order to achieve a certain score, all of the lower levels must be achieved first. For example, if an organization misses a vital element at the lower levels of the model, they will receive a low score even if they have some of the higher level attributes in place.
5. The client will be awarded the lowest score they achieved for any of the factors assessed against the control area (e.g., if they score 11 for leadership, 9 for communication and 4 for skills, the score for the control area is 4).

6. If a client has a major NCR[1] in the area, the maximum possible score will be 6.
7. The assessor will then move onto the next control area.
8. Once the assessor has assessed all of the control areas, there will be 11 scores (if assessed using v1.4 of the CCM).
9. The average score will be used to assign the overall level for the client.
10. The organization's report will highlight what level of maturity their system has achieved.

Notes – Due to the way the controls are structured, an organization that has all of the controls properly in place in the control area will score fairly highly on the controls matrix. For example, in the risk management control area, RI-01 states – *"Organizations shall develop and maintain an enterprise risk management framework to manage risk to an acceptable level*." This can be assessed against most of the factors of the maturity model and could be a sophisticated (high-scoring) implementation, or it could be poorly managed, achieving a low score. However, as you look at the other controls in this control area, they are more specific and more detailed about what is required. Consider, for example, *"Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and executive approval."* This is characteristic of the higher management capability levels of the model. Therefore, it would be difficult for a client to have all of the CCM controls in place and not score relatively well.

7. What type of certificate will a client get?

A client will be awarded a certificate following the assessment.[2] Depending on the capability level they achieved, they may get:

1. No award
2. A bronze award
3. A silver award
4. A gold award

The award is based on the average score received across the 11 control areas.

- If the organization has an average score of less than 3, it will receive a certificate with no award
- If the organization has an average score between 3 and 6, it will receive a bronze award
- If the organization has an average score between 6 and 9, it will receive a silver award
- If the organization has an average score greater than 9, it will receive a gold award

[1] NCR – Non-Conformance Report

[2] In jurisdictions where the issuing of additional certificates is difficult STAR certification may be included in the scope of the ISO 27001 certificate and it can be endorsed appropriately.

ISO 27001 is a management systems standard and, by definition, requires a systematic approach to managing an organization. Therefore if an organization is certified to ISO 27001, it is very unlikely that they would not achieve at least a bronze certificate.

8. Example of how an assessor might audit a control area?

The facilities security control area is used here as an illustration because it is a relatively tangible example (there are actually eight controls in this area in v1.4. Only the first four are examined here).

The description below is a simplified example of how an assessor might audit the control. It is not supposed to describe in detail what an assessor would do. The approach would vary considerably depending on the type of organization being auditing. The approach would be framed by the organization's analysis of its customers' expectations and contractual requirements that comes from ISO 27001, and the organization's overall information security risk analysis that comes from ISO 27001.

Control	ID	Description
Facility Security - User Access	FS-01	Policies and procedures shall be established for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas.
Facility Security - User Access	FS-02	Physical access to information assets and functions by users and support personnel shall be restricted.
Facility Security - Controlled Access Points	FS-03	Physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) shall be implemented to safeguard sensitive data and information systems.
Facility Security - Secure Area Authorization	FS-04	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.

1. The assessor would identify which person or people were responsible for facilities security and establish whether they were responsible for the all controls listed in the section.
2. They would assess if, in the context of the organization, the five factors on the grid were applicable – (communication, procedures, skills and expertise, leadership, and measurement). In most cases they would be.
3. The assessor would then review the first control in the control area, which tends to be a general description of the control area.
    1. The first factor on the matrix was "Communication and Stakeholder Engagement."
        i. No formal approach – Stakeholders are identified and include all obvious people accessing the facility.

ii. Reactive approach – There is evidence of communication about changes in procedures (e.g., requirements to display and update badges or not hold doors open for unidentified people). E-mails, staff notices, meeting minutes, and other material might establish this. This would be characteristic of a reactive approach.

iii. Proactive approach – There is evaluation of programs aimed at stakeholders. The assessor might then ask for formal stakeholder analysis that listed people who accessed the facility and what level of access they required. The assessor would also establish how the organization has determined the approach and look for evidence that the communication was effective, possibly by asking people if they knew about changes. The assessor might then ask for evidence of a measurable change in behavior (e.g., Are id badges displayed? Are there people in the building who swiped out without swiping in?). This would begin to suggest a proactive approach.

iv. Improving approach – There is evidence of stakeholder input in decisions (or a reason why stakeholders weren't consulted). There would probably be evidence, discussion boards, or meetings with documentation to prove action was taken or there were obvious changes on the ground. Evidence could be a process for reporting observed weaknesses in the system, but also an appreciation of how restrictions might hamper other operations (e.g., Can the engineering team get through the turnstiles with all the equipment? Was this discussed with them?). This should link back to the risk assessment.

v. Optimizing approach – There is a justification for who was involved in decision making and how they were informed of all the relevant facts. This would probably be in meetings. The assessor would expect to see how performance was benchmarked inside and outside of the organization. Participation in trade events and industry committees might be evidence.

The assessor would then consider if this level of management extended across the other controls in the area FS-02, FS-03, and FS-04. If the same management processes extended, then a score could be given. However, if management processes did not extend, the assessor would have to repeat the process to ensure the level of management across the control area at least at this level.

2. The second factor is "Policies, Plans, Procedures, and a Systematic Approach." This is actually the key focus of the facilities security control area, so a high score would be expected in order for the organization to conform to ISO 27001. The levels for this factor are:

   i. No formal approach – There is evidence of procedures in operation to manage access to the site, identify who should get access to where, and determine how access should be withdrawn and granted.

   ii. Reactive approach – Security staff are operating in line with any documented procedures and these procedures are documented and reviewed when operational changes are made.

   iii. Proactive approach – Documented plans cover the whole control area (e.g., all the points of access, all people, all the operations, and all the situations the site was exposed to).
   iv. Improving approach – There is risk analysis of business continuity issues and plans in place for the possible events (e.g., if power is cut and disables door locks).
   v. Optimizing approach – Plans, policies and procedures align with business strategy. The assessor might expect the control owner to show what changes in the business they were expecting and that the policies and procedures could cope with these changes (e.g., if the strategy included expanding the site, when would policies change? What would need changing?).

   Again, the assessor would then check that the same management regime was applicable across all controls in the area.

3. The third factor is "Skills and Expertise." This factor evaluates whether the personnel are able to run the control. The levels for this factor are:
   i. No Formal Approach – Staff have basic skills (e.g., an appreciation of how to decide if someone can access a certain part of the building and how to grant access).
   ii. Reactive Approach – Staff are able to identify breaches (e.g., they can and do look at access logs to secure areas, operate CCTV cameras, raise alarms, and do routine maintenance).
   iii. Proactive Approach – The organization monitors staff competency. They have tests to ensure that staff understand issues and results are recorded. Only qualified people are assigned to tasks.
   iv. Improving Approach – Staff competency is tested (e.g., simulations of breaches or power cuts) to ensure that staff respond effectively. Where weaknesses are found, training is put in place.
   v. Optimizing Approach - Succession planning system is in place to ensure that there is adequate coverage of skilled people.

   Again, the full breadth of the control area should be considered to ensure the same standard of management is maintained throughout.

4. The fourth factor is "Ownership and Leadership." This factor evaluates whether there is a capacity to co-ordinate action through a responsible person in charge. The levels for this factor are:
   i. No Formal Approach – Staff in charge can identify the key issues in physical security.
   ii. Reactive Approach – The control owner knows how the facility's security links to the overall security of the organization, as well as the organization's risk analysis. They should be able to demonstrate that they can access appropriate resources to fix problems.

iii. Proactive Approach – The control area owner is able to outline how preventive actions are considered and implemented, and justify the resources dedicated to it based on an analysis that considers customer requirements (e.g., making changes to barrier timing after people were found to follow a colleague into secure areas).

iv. Improving Approach - The control owner should able to outline how they improve the control area based on data and risk analysis to make proactive improvements to the system (e.g., internal audits highlighted a theoretical but plausible risk that someone could force a window open with limited tools, so locks were added).

v. Optimizing approach - The control owner is able to demonstrate how plans are made to deal with future changes in the organization (e.g., examining lead times to upgrade facilities to handle higher security data).

Again, it should be checked that the same leadership attention is paid across the control area.

5. The fifth factor is "Monitoring and Measuring." This factor evaluates whether issues are detected and if personnel have the facts to improve the system. The levels for this factor are:

    i. No Formal Approach – The organization has some way of monitoring security. The assessor might expect a security guard at the prime entrance, but only occasional patrols to cover the back entrance.

    ii. Reactive Approach – Organization has formal monitoring that is considered in line with the risk analysis. There will be some data available to check that monitoring has taken place, but the data might not be analyzed (e.g., the security guard records that they checked the doors and the system would flag if someone tried to gain unauthorized access, but patterns are not analyzed).

    iii. Proactive Approach – The organization collects data for all security areas identified on the risk register.

    iv. Improving Approach – Security data is routinely analyzed to detect anomalies in security access. It would be easy to flag if one person suddenly increased access to a particular area. Records could be produced for the assessor.

    v. Optimizing Approach – Monitoring processes are routinely tested for effectiveness (e.g., using simulated security breaches and intentional unusual access patterns). Results of tests could be shown to assessors.