CMMI Audit Guide

ISACA®

CMMI Performance Solutions

Purpose

The guide is intended to present a general approach for the various types of CMMI audits which are tailored to the depth or degree of coverage as determined by the Auditor and ISACA Quality Management.

This Audit Guide is for use in Audits conducted by ISACA CMMI Authorized Auditors. An ISACA CMMI Authorized Auditor is an individual who has been vetted and trained by ISACA to conduct audits on behalf of ISACA for the purposes of verifying that CMMI Product Suite requirements have been fully and adequately met and are being interpreted and applied correctly with the fidelity and level of quality specified by ISACA.

The guide serves as a tool in assisting the auditor to assure the review of CMMI appraisal/course-related evidence and its operations comply with policies, program rules, and generally accepted auditing standards. Please refer below for auditing standards:

I. Auditing Standards

The general standards of audit conduct approved by ISACA include:

1. The Auditor possesses all appropriate and current CMMI certifications as listed under the ISACA Authorized CMMI Auditor section of this guide
2. The Auditor has adequate observation, auditing, and technical training and experience
3. The Auditor must remain current with all upgrades to the certifications relevant to the audit
4. The Auditor exercises professional care in the performance of the audit and preparation of the audit report to ensure audits are carried out in accordance with the standards set in the appraisal method and comply with ISACA policies, CMMI models, and Partner and Certification Agreements
5. The Auditor obtains sufficient and appropriate evidence through inspections, observations, inquiries, and affirmations to acquire an objective basis for audit findings

II. Auditor Requirements

ISACA CMMI Authorized Auditors must meet the following requirements and conditions:

- Must possess the appropriate CMMI certifications as identified below.
- Must be in good standing as defined by ISACA (i.e., having no quality issues or unpaid invoices)
- Must complete any required ISACA CMMI Auditor training
- Must be either an ISACA employee or have an active independent service provider (ISP) agreement with ISACA
- Must have an executed ISACA non-disclosure (NDA), non-compete, and confidentiality agreement, legally binding the Auditor from disclosing or sharing information about the audit activities or results, and prohibiting them from soliciting the customers of the audited individual or CMMI Partner
- Must have been interviewed, vetted, and approved for audit conduct by the ISACA Quality Management team and ISACA CMMI Subject Matter Experts (SMEs)

For Auditing ISACA CMMI course deliveries:

- Must meet all general ISACA CMMI Authorized Auditor requirements cited above
- Must be a Certified CMMI Instructor in the domain of the course being audited, e.g., CMMI for Services (SVC), CMMI for Development (DEV) or an ISACA employee who possesses training and instructional experience and is knowledgeable of ISACA CMMI courses, materials, and policies
- For CMMI High Maturity (HM) Courses, the Auditor must be a Certified CMMI High Maturity Lead Appraiser (CHMLA) as well as a Certified CMMI Instructor
- Must possess a minimum of 10 years of experience as a Certified CMMI Instructor or possess equivalent process and performance improvement experience

For Quality Improvement Checkups (QICs) on ISACA CMMI course deliveries, QIC Auditors must:

- Possess a current CMMI Practitioner certification
- Complete QIC Auditor Training
- Be approved by Quality Management

For auditing CMMI appraisals of any type (e.g., Benchmark, Sustainment, Evaluation, Medical Device Discovery Appraisal Program (MDDAP), Action Plan Reappraisal (APR)), Auditors:

- Must meet all general ISACA CMMI Authorized Auditor requirements cited above
- Must be a CMMI Certified Lead Appraiser in the domain of the appraisal being audited, e.g., CMMI-SVC, CMMI-DEV
- For HM appraisals (Maturity or Capability Levels 4 and 5), must be a CMMI Certified High Maturity Lead Appraiser (CHMLA)
- Must possess a minimum of 10 years of experience as a Certified CMMI Lead Appraiser or possess equivalent process and performance improvement experience

III. Responsibilities of the Auditor

The Auditor assigned by ISACA has the authority, on behalf of ISACA, to review objective evidence, interview and/or meet with the appraisal team lead (ATL) and members (ATMs), Appraisal Sponsor, interviewees, and participants for the appraisal or course being audited. The Auditor has the responsibility to plan and perform an audit to obtain reasonable assurance that the auditee (in this case, either LA or Instructor) demonstrates mastery of the skills expected of ISACA Certified CMMI Lead Appraisers and Instructors.

I. Appraisal Audits

Lead Appraisers (LAs) may be assessed on all or some of the areas below depending on the scope and length of the audit:

- Achieving and managing agreements
- Decision making and problem solving
- Project planning and management
- Interpersonal communication and facilitation (i.e., working with interpreters)
- Integration, articulation, and expression of information

- Understanding and adapting to organizational context
- Model understanding and interpretation
- Appraisal method understanding, interpretation, tailoring, adaptation, and application
- Appropriate and accurate reporting of appraisal information in the CMMI Appraisal System (CAS)
- Professionalism
- Adherence to the ISACA CMMI Code of Professional Conduct (COPC), ISACA CMMI policies, CMMI Appraisal Method Definition Document (MDD), agreements, and guidelines
- Quality of virtual appraisal activities (if applicable) e.g., following Appendix A of the MDD while maintaining quality and integrity of MDD requirements, adhering to the virtual delivery toolkit and Lead Appraiser Checklist

The Auditor is also responsible for assessing the ability of the auditee (in this case, the LA) to evaluate evidence for the characteristics of fraud and to detect misstatements by appraisal participants. The LA is responsible for presenting the Organizational Unit's conformity to CMMI in a fair and accurate manner; the Auditor's knowledge of an organization is acquired solely through the audit. The Auditor evaluates the LA's ability to judge the effectiveness of an organization's processes, and whether it meets the intent of the reference model for the targeted maturity level.

II. Course Audits

Instructors may be assessed on all or some of the areas below, depending on the scope and length of the audit:

- Use of student-centered teaching techniques, activities, and assessments that support Learner Objectives
- Employment of strategies that require students to analyze the relationship between the course Learner Objectives and solutions relevant to real organizations
- Development and usage of class activities that require students to engage with course materials (content), the Instructor(s), and each other
- Proper application of different formative and summative assessment techniques with a clear purpose
- Effective usage of course materials and the CMMI model to teach the course, including applying appropriate and accurate model content knowledge and reinforcing correct answers
- Understanding and communication of the student lifecycle (i.e., material and exam access, course survey access)
- Demonstration of a range of instructional techniques to meet the same Learner Objective
- Use of tailoring within the ISACA course tailoring guidelines (if applicable)
- Effective planning of course delivery, preparation of course materials, and planning strategies for mitigating risks
- Usage of effective instructional strategies in their delivery method and effectively uses platform/materials during delivery
- Appropriate and accurate reporting of course information in the CMMI Course Management System (CMS)
- Professionalism
- Adherence to the CMMI Code of Professional Conduct (COPC), ISACA CMMI policies, agreements, and guidelines

- Quality of virtual course activities (if applicable) e.g., adhering to the virtual delivery toolkit and Instructor Checklist

The Auditor is responsible for assessing the ability of the auditee (in this case, the Instructor) to accurately deliver course content with a student-centered focus to support the course Learner Objectives. The Auditor will evaluate the Instructor's ability to effectively convey accurate CMMI model knowledge and application and use of effective instructional strategies to do so.

For QICs - The Auditor's primary role is observing, and not participating. The Auditor should not be available for any participation in questions, nor should they interject opinions or judgements to the event participants, e.g., students. The Instructor must always remain the focal point for all communication with the students/organization for which the course is being delivered.

III. Adherence to the ISACA CMMI Code of Professional Conduct and Certification Agreement

ISACA Authorized CMMI Auditors have a responsibility to comply with the standards accepted by their fellow LAs and Instructors. Those standards are agreed to through and enforceable by the CMMI COPC and CMMI Certification Agreement.

Background

Audits of CMMI appraisals may be opened for a variety of reasons, including (but not limited to) inconsistencies identified during standard review, formal complaints submitted to ISACA, random selection, or product performance management. The goals of an audit are (1.) to verify the validity of the appraisal's results, and (2.) to identify any potential improvement opportunities for either the Appraisal Team Leader (ATL) or the CMMI Product suite.

Scope

The scope includes identifying the type of audit being conducted, timeframe and location.

I. Audit Types

ISACA defines four main audit types. Given the unique circumstances of the audit, ISACA may utilize one or a combination of the below approaches or adapt elements of one or more audit types in defining the scope of the audit.

- **Directed Interview Audit (DIA):** A new approach to appraisal audits, aimed at resolving unique and complex quality concerns that arise during standard appraisal reviews. A DIA consists of an interview of an LA by an auditor, during which the key concern is discussed in depth.
- **Desktop Audit (DA):** A desktop (or document review) audit is a high-level review of artifacts that were provided as objective evidence during an appraisal. It is designed to verify that the characterizations and ratings assigned during the appraisal were arrived at correctly.
- **Intensive Audit (IA): An** intensive audit is performed during delivery of a course or appraisal through live observation by the auditor or retrospectively after the delivery of a

course or appraisal to ensure compliance to requirements. An intensive audit can be performed either in-person or virtually and, if performed live, requires the auditor to be present for the entirety of the appraisal or course delivery.

- **Quality Improvement Checkups (QICs):** Quality Improvement Checkups (QICs) are real-time audits of randomly selected CMMI courses. The purpose of Quality Improvement Checkups (QICs) on CMMI course deliveries is to reinforce quality standards and collect feedback about techniques and best practices being employed by CMMI Partners. The scope of QICs aims to randomly select and observe an upcoming course scheduled to be delivered by a CMMI Partner.

II. Duration of an Audit

The Auditor will review the appraisal or course plan provided by the auditee to determine the scope and duration of the audit.

III. Location of the Audit

An audit can be conducted either onsite or virtually and may include telecons and email exchanges. If an audit includes an onsite component, the auditee must provide organizational location and entry details and secure all necessary clearance requirements and NDAs as deemed appropriate.

Policy

Please refer to the CMMI Quality - Audit Policy for more information.

Auditing Compliance and Program Requirements

I. Appraisal Sponsor

An Appraisal Sponsor is an individual who champions the planning and delivery of an appraisal for an organization and provides financial or other resources to carry it out. Appraisal Sponsors, whether internal or external to the organization being appraised, are the organizational contact that ISACA will notify regarding appraisal activities, which may include audits.

It is important that the Appraisal Sponsor understands the responsibilities related to this role if their organization's appraisal has been selected for an audit by ISACA. The selected individual must have the authority to make decisions and accept the responsibilities outlined in this document. This role cannot be delegated to another individual. The Appraisal Sponsor must be available to the LA for all communications related to the planning and conduct of the audited appraisal.

The audit is intended to be constructive and provide as little disruption to the appraisal delivery as possible. Audits are focused on helping the organization achieve responsible and effective CMMI adoption. Audits also help ISACA to determine if certified LAs are following the appraisal method, appropriately interpreting CMMI models, and complying with ISACA's COPC, Partner and Certification Agreements, policies, and guidelines.

II. Cost of an Audit

Audits are conducted at ISACA’s expense unless an audit is requested by the Appraisal Sponsor in which case the audit expenses must be covered by the Appraisal Sponsor’s organization.

III. Appraisal Sponsor Responsibilities During an Audit

1. Be familiar with the requirements outlined in *CMMI* *Appraisal – Sponsor Role and Responsibilities Policy*, which is provided to the Appraisal Sponsor at the time of the appraisal’s registration in ISACA’s CAS. Appraisal Sponsors and LAs are required to sign the document to confirm that each understands the Appraisal Sponsor’s responsibilities. It is the responsibility of the LA to ensure that the Appraisal Sponsor understands the policy considering their native language
2. Provide organizational address and physical site access information (if applicable)
3. Allow access to organizational documents necessary to conduct a valid CMMI appraisal audit
4. Provide a safe environment to allow the Auditor to observe any portion of the appraisal delivery
5. Allow the Auditor to interact with all appraisal participants or organizational employees who perform the work being appraised. Participants must feel comfortable being open and honest about their organization without concern for retribution
6. Provide or allow virtual technology (e.g., Zoom or the equivalent) if virtual meetings are required
7. Validate that the appraisal is conducted in accordance with all policies implemented by ISACA
8. Attend the opening briefing and final findings and any subsequent audit presentations
9. Ensure that there are no real or perceived COIs that may result in ISACA having a lack of confidence in the appraisal results
10. Validate that the appraisal was conducted in accordance with agreements between the LA, the CMMI Partner, and ISACA
11. Ensure that the appraisal evidence is appropriately archived and protected for the duration of the appraisal’s validity
12. Understand that if the appraisal is rescheduled, the audit will also be rescheduled
13. Recognize that ISACA determines, at its sole discretion, that if a delivery does not meet the quality standards for the relevant product, the appraisal will be rejected. Further, if an organization is determined to have misrepresented itself during an appraisal, ISACA may not recognize further CMMI appraisal attempts

Review Implementation

ISACA Audit Process

This audit process describes the high-level steps of an audit. A full outline of the steps of an audit can be found in the Appendix section of this document. The Auditor may tailor the audit process to fit the unique circumstances of the audit being performed. If this occurs, the Auditor will obtain approval from ISACA to proceed with the tailoring, and (if approved) will then identify and communicate the specific tailoring to the auditee. All emails related to the audit should be directed to quality@cmmiinstitute.com.

The audit work is broken down into three phases, each of which has a bearing on how and to what extent the audit is conducted. The phases are defined as follows:

Phase 1
Identification of an Audit
Phase 2
Notification of an Audit
Audit Participants
Steps of the Audit Process
Audit Findings
Audit Report
Appraisal Submission and Quality Review
Unethical Behavior
Phase 3
Communicating Audit Results
Remediation or Additional Training
Unsatisfactory Performance on Additional Training or Remediation

PHASE 1

I. Identification of an Audit

Audits may be conducted at any phase of an appraisal: Plan and Prepare for Appraisal (Phase 1), Conduct Appraisal (Phase 2), Report Results (Phase 3) and/or Conduct Action Plan Reappraisal (Phase 4), or after the standard appraisal quality review has been completed. Audits may be conducted during the planning, conduct, and reporting aspects of a course, or after the course has been completed. ISACA reserves the right to audit at any time. ISACA determines if the audit is to be conducted onsite, via virtual technologies, by telecon, a combination, or by other medium. There are various reasons why an appraisal or course delivery may be identified for audit, but most are selected due to:

- Random selection (which takes schedule and Auditor availability into consideration)
- Mentoring LAs or Instructors
- Ethics and compliance reports
- Patterns or trends indicating issues with appraisal or course delivery understanding or implementation
- Conflicting data in appraisal or course record submissions
- Requests for audit
- Observation of new product releases

ISACA informs the auditee (and the BPOC) that their appraisal or course delivery has been selected for audit. In the case of an appraisal, it is the LA's responsibility to inform the Appraisal Sponsor of the audit. Once the Appraisal Sponsor has been notified, the LA must then work with the Appraisal Sponsor, Auditor, and Quality Management to plan and perform the audit.

If an appraisal or course is identified for audit, and the appraisal or course is delayed, the audit will also be delayed until the appraisal or course resumes. Refusal to permit an audit will result in rejection of the appraisal or course results. ISACA reviews each audit report submitted for compliance with CMMI models, methods, policies, and guidelines. If ISACA determines, at its sole discretion, that the quality of delivery does not meet the standards for the relevant product, the appraisal or course results are rejected.

PHASE 2

II. Notification of an Audit

ISACA can announce an audit at any time (see Identification of an Audit).

- ISACA notifies an auditee that their appraisal or course is selected for audit
  - The CMMI Partner's BPOC is copied on the audit notification
- Within three days of the notification, the auditee must respond to ISACA acknowledging the audit and (in case of an appraisal audit) inform the Appraisal Sponsor that an audit has been announced. Failure to do so within the required timeframe may result in corrective action at ISACA's discretion
  - Exceptions may apply if ISACA announces a live audit of an appraisal that has an immediate Phase 2 start date

III. Audit Participants

- **ISACA Authorized CMMI Auditor** – Performs the audit on the CMMI appraisal or course
- **Auditee** – ISACA certified CMMI LA or Instructor who delivers the audited appraisal or course
- **Quality Management leadership** – Coordinates, monitors, and reviews results of the audit; reviews and approves the audit entry and exit criteria; and assigns any corrective actions that may result from the audit
- **CMMI Subject Matter Expert (SME)** – Consults throughout the audit process, reviews Auditor's report and recommendations, and offers input on any potential corrective actions

IV. Audit Findings

Several types of findings can be noted in the audit report:

1. Strength - Identifies a best practice or good behavior exhibited by the auditee during the appraisal conduct or course delivery
2. Issue - Identifies a situation where the appraisal method, COPC, policies, etc. have not been followed correctly, or the auditee has misinterpreted one or more CMMI model practices
3. Improvement - Identifies a situation where the appraisal method, COPC, policies, etc. are being followed, but the Auditor recommends a better way to perform that process
4. Remediation – Identifies serious weaknesses exhibited by the auditee that can be addressed through remediation activities
5. Ethics Violations – Identifies unethical behavior which may pertain to mishandling of the appraisal or course delivery, inappropriately mitigated conflicts of interest (COIs), acceptance of fraudulent documents or statements, selling of maturity levels, acceptance of bribes, violation of Partner or Certification Agreements or the COPC, etc.
6. Lessons Learned - Feedback on the audit process and its conduct

V. Audit Report

The ISACA Authorized CMMI Auditor is responsible for submitting a standard audit report to ISACA within two to five business days of the completion of an audit. The audit report is reviewed by at least one additional ISACA Authorized CMMI Auditor, or CMMI SME, and Quality Management senior leadership. General standards of reporting include:

1. Compliance with the standard audit report template provided by Quality Management

2. The report shall state if the appraisal or course delivery was conducted in accordance with the CMMI COPC, CMMI policies, CMMI training guidelines, Partner and Certification Agreements, CMMI Models, and the CMMI Appraisal Method

3. The report shall identify instances where standards have not been observed. These include:

   a. CMMI appraisal method violations
   b. Policy violations
   c. Ethics and compliance issues or reports
   d. Misinterpretation or misapplication of the CMMI model

4. The report shall contain an overall opinion regarding the performance of the auditee

5. The report shall contain a recommendation for remedial work or adverse actions if deficiencies are noted

6. The report shall inform ISACA if there is cause to believe any unethical behaviors have occurred

7. For appraisal audits, the report shall recommend whether the organization has successfully achieved the targeted maturity level, or whether the results of the appraisal should be reviewed by ISACA's Quality Management department and possibly rejected

8. For course audits, the report shall recommend whether the quality of instruction provided students the tools and guidance to successfully achieve the Learner Objectives, or whether the results of the course should be reviewed by ISACA's Quality Management department and possibly invalidated

VI. Appraisal Submission and Quality Review

When an audited appraisal is submitted to ISACA, Quality Management staff will review the appraisal record as a final check for compliance with the CMMI model and method, CMMI Partner and Certification Agreements, and the COPC. ISACA will determine, at its sole discretion, if the quality of each delivery is sufficient to meet the standards for the relevant product. If the quality is deemed insufficient, the appraisal will be rejected.

VII. Unethical Behavior

If the Auditor observes any unethical behavior during the audit, it is reported to ISACA, and further investigation will occur.

PHASE 3

VIII. Communicating Audit Results

ISACA is solely responsible for determining the outcome of the audit, based on the submitted report from the auditor. Potential outcomes include, but are not limited to:

- Closed – Identifies that the audit is closed with no further action required
- Remediation – Identifies activities that can be performed to address issues or improvements noted in the report
- Corrective Actions – Identifies actions taken by ISACA to address serious issues related to the appraisal or course delivery or ethics violations that cannot be remediated. Corrective action covers a wide spectrum, from measures considered remedial in nature to more severe penalties including loss of certification and termination of an organization's CMMI Partner Agreement. Each issue subject to corrective action is evaluated in terms of intent, severity, and number of occurrences. ISACA analyzes and investigates each issue with the

goal of having the corrective action be in proportion to the error. ISACA always looks to help the individual recover from the mistake and learn from it. Decertification is never the first choice but is arrived at if all other avenues have not solved the problem or the issue is not appropriate for remediation

Within 15 days of receiving the completed audit report and appraisal record, ISACA's Quality Management will communicate the results of the audit to the auditee. ISACA retains the right to approve or disapprove of the results of any CMMI appraisal or course. Questions regarding audits can be directed to support.isaca.org. If remediation is required, an assignment, including the timeframe for completion, is identified.

ISACA SMEs will review additional training or remediation assignments within 10 days of receipt to determine if the actions taken are satisfactory, and feedback will be provided to the auditee.

IX. Remediation or Additional Training

If remediation or additional training is recommended by the Auditor, the auditee is informed of the required remediation or training tasks. During the time that the auditee is performing these tasks, their certification(s) may be suspended. Failure to accept the terms of remediation or additional training may result in corrective action up to and including decertification of the auditee's credentials at ISACA's discretion.

X. Unsatisfactory Performance on Additional Training or Remediation

If continued corrective or remedial actions are necessary, additional support services provided by ISACA shall not be at ISACA's expense but will be billed in accordance with observation pricing.

Appendix A: Steps of the Audit Process

Audit Types				Audit Process
DIA	DA	IA	QIC	An appraisal is registered in CAS a minimum of 35 days prior to the Conduct Appraisal Phase. A course is registered in the Course Management System (CMS) a minimum of 14 days prior to delivery
DIA	DA	IA	QIC	The appraisal or course is identified for audit (see Identification of an Audit)
DIA	DA	IA	QIC	The auditee must respond to the notification (and, for an appraisal audit, inform the Appraisal Sponsor)
DIA	DA	IA	QIC	The auditee sends the appraisal or course plan (including the schedule) to the Auditor, copying quality@cmmiinstitute.com
DIA	DA	IA	QIC	The Auditor reviews the plan and begins the audit dialogue with the Auditee. Depending on the scope of the appraisal or course, the Auditor will determine what activities the audit will include. The Auditor will be provided with an Audit Checklist by ISACA detailing the required steps of the process for the Auditor to follow. The Auditor must utilize the checklist throughout the audit process and ensure that the necessary steps are taken. The audit may include the following: a. The Auditor may send a series of questions to the auditee, or request for appraisal artifacts, course plan; each with a deadline to respond b. Conference call, virtual meeting, or telecon c. Onsite visit
			QIC	The Auditor reviews the plan and schedule. Depending on the scope of the appraisal or course, the Auditor will determine what activities the audit will include. The Auditor will be provided with an Audit Checklist by ISACA detailing the required steps of the process for the Auditor to follow. The Auditor must utilize the checklist throughout the audit process and ensure that the necessary steps are taken

DIA	DA	IA		The auditee may be asked to provide their CMMI Partner's agreement for the delivery of the appraisal or course
DIA	DA	IA	QIC	The Auditor conducts the audit, collecting all available and relevant evidence
DIA	DA	IA	QIC	The Auditor submits the audit report and completed Audit Checklist to ISACA
DIA	DA	IA		Quality Management leadership and a CMMI SME (who did not perform the audit in question) review the audit report
			QIC	Process & Audit Control leadership reviews the audit report
DIA	DA	IA		The Auditor meets with Quality Management leadership and a CMMI SME (who did not perform the audit in question) to discuss the findings of the report, and all parties make a final determination of the audit outcome
DIA	DA	IA	QIC	Quality Management will communicate the audit results within 15 business days upon receipt of the full audit report
DIA	DA	IA	QIC	If additional training or remediation is required, the assignment and timeline for completion will be sent to the auditee
DIA	DA	IA	QIC	The auditee submits training or remediation to ISACA at quality@cmmiinstitute.com
DIA	DA	IA	QIC	The remediation assignment is reviewed within 10 days of receipt. Quality Management will communicate the outcome of the remediation assignment review to the auditee and the audit will be closed
DIA	DA	IA		At the discretion of ISACA and the Auditor, the Auditor may debrief the auditee on elements of the audit report. However, the final outcome of the audit will be communicated by Quality Management