CLOUD4C

01 January 2022

INTERNAL AUDIT POLICY

Compliance Team

CLOUD4C SERVICES PVT LTD

DOCUMENT CONTROL:

Preparation

Draft	**Author**	**Date**
1.0	M.Venkataniranjan	25/06/2016
1.1	M.Venkataniranjan	08/01/2017
1.2	M.Venkataniranjan	06/01/2018
1.3	M.Venkataniranjan	10/10/2018
1.3	M.Venkataniranjan	05/01/2019
1.3	M.Venkataniranjan	03/01/2020
1.3	Keerthana Ravikanti	31/12/2020
1.3	Swathi Bachanaboina	31/12/2021

Classification	**Storage Location**
Confidential	Shared folder

Review & Approval

Reviewer & Approver	**Version**	**Date**	**Reviewed Draft Version**
RS Prasad Rao	1.0	04/07/2016	1.0
RS Prasad Rao	1.1	10/01/2017	1.1
RS Prasad Rao	1.2	07/01/2018	1.2
RS Prasad Rao	1.3	10/10/2018	1.3
RS Prasad Rao	1.3	07/01/2019	1.3
RS Prasad Rao	1.3	03/01/2020	1.3
RS Prasad Rao	1.3	01/01/2021	1.3
RS Prasad Rao	1.3	01/01/2022	1.3

Release

Release Version	**Date Released**
1.0	04/07/2016
1.1	10/01/2017
1.2	07/01/2018
1.3	10/10/2018
1.3	07/01/2019
1.3	03/01/2020
1.3	01/01/2021
1.3	01/01/2022

Distribution List

Name	Designation	Department
COE Teams	COE Engineers	Service Delivery
BU Heads		

Change Control

Version	Change Reason	Effective Date
1.1	Updated cloud4C Scope and Departments	10/01/2017
1.2	Reviewed and Updated version control	07/01/2018
1.3	Reviewed and added Training section – 10, Review of the policy section 11	10/10/2018
1.3	No updates	05/01/2019
1.3	No Updates	03/01/2020
1.3	No updates	31/12/2020
1.3	No updates	31/12/2021

STATEMENT OF CONFIDENTIALITY

This document contains proprietary trade secret and confidential information to be used solely for evaluating Cloud4C Services Private Ltd. The information contained herein is to be considered confidential. Customer, by receiving this document, agrees that neither this document nor the information disclosed herein, nor any part thereof, shall be reproduced or transferred to other documents, or used or disclosed to others for any purpose except as specifically authorized in writing by Cloud4C Services Private Ltd.

CONTENTS

1 INTRODUCTION

Internal audit Policy is to contribute to the improvement of Cloud4C management by ensuring a strong, credible, effective and sustainable internal audit function within the organisation. Internal Audit is a service function, organized and operated primarily for the purpose of conducting audits in accordance with Integrated Audit for ISO 9001, ISO 20k, ISO 27K and ISO 22301 standards.

Cloud4C ITS2MS (Information Security Management and IT Service Management) framework requires implementing the policies and processes as defined in ITS2MS

2 SCOPE

This policy and procedure shall be applicable to all employees of Cloud4C, its contractors, subcontractors, associated third parties who are users of Cloud4C services or who have access to Cloud4C facility.

3 OBJECTIVE

Internal audits objective is to verify the compliance of information security practices to ITS2MS requirements and is conducted every six months. Trained internal auditors conduct the audits. Internal Auditors independent of the department being audited are deputed for conducting the audit. The planning and execution of audits should be in accordance with the Internal Audit and Management Review process of Cloud4C.

4 CONFIDENTIALITY

All the information obtained during an internal audit is deemed confidential unless or otherwise stated instructed to. It is understood that certain data is confidential in nature and special arrangements may be required when examining and reporting on such items. Internal Audit will handle all information obtained during a review as the original custodian of the information.

Internal Audit respects the value and ownership of information received and will not disclose information without the approval of appropriate authority.

Audit reports are considered highly confidential. They are distributed to the respective Dept. Head, and in the MRM and in the External Audit. Other individuals interested in the audit report may gain access by getting the appropriate approval of the Director.

5 AUDIT SCOPE

To verify in a planned and comprehensive manner the compliance of practices to be arranged and to assess how to satisfy Information security policies and protection policies in the areas under audit. The audit scope covers all the business processes and systems associated functions such as sales, marketing, finance, Infrastructure, stores, data privacy, client contractual compliance, technical vulnerability, physical security, HR security, IT network security, security awareness, business continuity. The biannual audits will cover all the functional related controls in accordance with Integrated system of ISO 20k, ISO 27K and ISO 22301 standards. In achieving the objective the Internal Audit will develop and implement an audit strategy as part audit plan for every internal audit.

Related and support documentation

- Internal Audit and Management Review Process
- Internal audit plan

6 OVERVIEW OF THE AUDIT PROCESS

The internal audit is conducted biannually. The audit process is the same for most engagements and usually includes various departments (Ref.6). Through these Internal Audits will determine ways to minimize risks and increase efficiencies within the departments. Auditee involvement is critical at each stage of the audit process. An audit will result in a certain amount of time being diverted from usual operations. One of the key objectives is to minimize this time and avoid disrupting the on-going activities.

- ➢ The quality team develops an audit plan (Ref.7) based on a review of all pertinent information. Sources may include, but are not limited to: a risk assessment, internal and external evaluations and management guidance.
- ➢ Once internal Audit schedule calendar is prepared and it is sent to the Director for an approval. The audit calendar and MRM (Management review meeting) is communicated to all stakeholders and the senior managers of the process to be audited.
- ➢ During the open MRM, scope of the audit and objectives are discussed.
- ➢ Once the audit is completed, the report is finalized which includes, Summary and Opinion, Findings and Audit Recommendations.
- ➢ After the audit a Closed MRM is scheduled with all stakeholders during which discussion are held on the on the observations found in the Previous or current audit results (NCs).
- ➢ Minutes of the MRM will be maintained consistently.
- ➢ The quality team will conduct a follow up action on the Management Responses to the audit Findings within a specific time frame.

This subsequent review will be discussed with the Director and the comments published.

6.1 Knowledge and skills

Auditors should possess the knowledge and skills necessary to achieve the intended results of the audits they are expected to perform. All auditors should possess generic knowledge and skills and should also be expected to possess some discipline and sector-specific knowledge and skills. Audit team leaders should have the additional knowledge and skills necessary to provide leadership to the audit team.

Auditors should have knowledge and skills in the areas outlined below.

a) Audit principles, procedures and methods: knowledge and skills in this area enable the auditor to apply the appropriate principles, procedures and methods to different audits, and to ensure that audits are conducted in a consistent and systematic manner. An auditor should be able to do the following:

- apply audit principles, procedures, and methods;
- plan and organize the work effectively;
- conduct the audit within the agreed time schedule;
- prioritize and focus on matters of significance;
- collect information through effective interviewing, listening, observing and reviewing documents, records and data;
- understand and consider the experts' opinions;
- understand the appropriateness and consequences of using sampling techniques for auditing;
- verify the relevance and accuracy of collected information;
- confirm the sufficiency and appropriateness of audit evidence to support audit findings and conclusions;
- assess those factors that may affect the reliability of the audit findings and conclusions;
- Use work documents to record audit activities;
- document audit findings and prepare appropriate audit reports;
- maintain the confidentiality and security of information, data, documents and records;
- communicate effectively, orally and in writing (either personally, or through the use of interpreters and translators);
- understand the types of risks associated with auditing.

While carrying out their duties, the Internal Auditor is responsible for utilizing a systematic, disciplined approach to evaluating and improving the effectiveness of internal controls and should include the following:

a) Developing and maintaining a comprehensive audit program necessary to ensure compliance with accounting standards, policies and procedures necessary to safeguard organization resources.
b) Communicating the results of audits and reviews by preparing timely reports, including recommendations for modifications of management practices, fiscal policies and accounting procedures as warranted by audit findings.
c) Establishing and maintaining a quality assurance program to evaluate the Internal Audit operations. This program should include the following:

Uniformity of work paper preparation, audit sampling, work paper review, report preparation and review, report communication and issuance and record retention.

6.2 Types of evidence

If the evidence supports the basic test of sufficiency, competence and relevance, it may be used to support the auditor's findings. The following outlines the different types of evidence obtained during the course of an audit:

- Physical evidence: Obtained through observation and inquiry
- Testimonial evidence: Based on interviews and statements form involved persons
- Documentary evidence: Consists of legislation, reports, minutes, memoranda, contracts, extracts from accounting records, formal charts and specifications of documentation flows, systems design, operational and organizational structure
- Analytical evidence: Secured by analysis of information collected by the auditor.

6.3 Types of Samples

- Statistical or probability sampling. Allows the auditor to stipulate, with a given level of confidence, the condition of a large population by reviewing only a percentage of the total items. Several sampling techniques are available to the auditor.
- Attribute sampling: Used when the auditor has identified the expected frequency or occurrence of an event.
- Variable sampling: Used when the auditor samples for values in a population which vary from item to item.
- Judgment sampling: Used when it is not essential to have a precise determination of the probable condition of the universe, or where it is not possible, practical or necessary to use statistical sampling.

Evidential Matter

- Evidential matter obtained during the course of fieldwork provides the documented basis for the auditor's opinions, observations and recommendations as expressed in the auditor's opinions, observations and recommendations as noted in the audit report. The Internal Audit Department is obligated by professional standards to act objectively, exercise due professional care and collect sufficient and relevant information to provide a sound basis for audit observations and recommendations. Auditors must obtain all evidence necessary for the effective completion of the audit. The decision on how much evidence is enough and what type to seek requires the exercise of the auditor's judgment based on experience, education and intuition. A thorough knowledge of the concepts underlying audit evidence will help the auditor to improve the audit quality and efficiency of the process.
- Standards for the Professional Practice of Internal Auditing require that work papers possess certain attributes to provide a sound basis for audit observations and opinions and to be considered as evidential matter. These attributes are: Sufficient information is factual and adequate so that a prudent, informed person would reach the same conclusions as the auditor Information is reliable and the best attainable through use of appropriate audit techniques
- Relevant information supports audit findings and recommendations and is consistent with the audit objectives for the audit
- Useful information helps the organization meet its goals. It also provides a reference for the preparer when called upon to answer questions.

6.4 Code of Ethics

The Internal Audit staff shall adhere to the establish policies by the management. In addition, the Internal Audit staff will uphold the following:

a) **Integrity**: Establish trust and thus provide the basis for reliance on the judgment of Internal Audit. Remain tactful, honest, objective and credible in all relationships as a representative of internal audit.

b) **Objectivity**: Exhibit the highest level of professional objectivity in gathering, evaluating and communications information about the area under examination. Make balanced assessments of all the relevant circumstances and do not become unduly influenced by individual interests or by others in forming judgments.

c) **Confidentiality**: Respect the value and ownership of information received. Do not disclose information without appropriate authority.

d) **Competency**: Apply the knowledge, skills and experience required in the performance of internal auditing services and continually improve the proficiency, effectiveness and quality of the services provided.

6.5 What are Findings?

- **Observations**
  Observation are simply pointed out by the auditor as areas being in compliance but very close to becoming a non-conformance or that given additional evidence could transform into a non-conformance. Observations can be looked as "accidents waiting to happen". Advice teams to treat observation very seriously and in fact incorporate them into the Depts./Teams' as preventive actions and handle them as such. This helps tremendously with the balancing of corrective and preventive action –most organizations have a real hard time to issue preventive actions. It also makes effective use of audit reports by taking into account the auditor efforts and experience.
- **Non-conformance**
  Non-conformances or NCNs are areas where the organization's quality management system does not comply with one of the requirements of the standard or where the organization failed to show evidence of compliance. Non-conformances have a clear requirement that was not met and there is clear evidence of what was seen –or not seen. Non-conformances have 3 elements:
    - Requirement
    - Non-conformance
    - Evidence

  Nonconformities are in essence, just another type of finding, however it is the one that everyone concentrates on and what the organization worries more about.
- **Opportunities for Improvement**
  Opportunities for improvement are areas that are not necessarily wrong or not meeting the requirements of the standard. Unlike observations, opportunities for improvement are not accidents waiting to happen but rather these are practices that have been implemented poorly and either do not add value or consist of several non-value added steps. Auditor usually point opportunities for improvement, when they believe –based on their expertise and expanded view of quality management systems-that those practices could be enhanced or done more efficiently.

6.6 Grading or classifying Nonconformities

Some registrars classify their non-conformances into major and minor, such as in major nonconformance and minor non-conformance. Other registrars classify non-conformances as Category 1 and Category 2. Those terms are basically interchangeable:

Major non-conformances or Category 1
Are those findings where an element of the ISO standard has not been met or where there is a significant breakdown in the quality management system. A group of Minor NCNs in the same specific area of the standard may also be elevated to category 1. Minor NCNs that

have not been properly addressed after a whole audit cycle may also be elevated to category 1.

Minor non-conformances or Category 2

Minor nonconformities are those where there is a minor lapse on the quality management system and where basically it is evident that the system or requirement has been established and for the most part are implemented correctly.

7 MANAGEMENT REVIEW

Management Reviews are conducted half-yearly to review the continuing suitability, adequacy and effectiveness of ITS2MS. Management reviews are conducted on the recommendations proposed by. This review shall include assessing opportunities for improvement and the need for changes to the ITS2MS audit. Management Reviews are coordinated by the Head, Process Improvement and chaired by the Director. All department heads and Information Security Forum members from all locations are part of Management Review Meetings as applicable in the scope of ITS2MS.

The agenda for the Management Review Meetings shall include:

- Results of ITS2MS audit and reviews;
- Feedback form interested parties;
- Customer Satisfaction;
- Achievement against defined service levels;
- Techniques, products or procedures, which could be used in the organization to improve the ITS2MS performance and effectiveness‟;
- Status of preventive and corrective actions;
- Vulnerabilities or threats not adequately addressed in the previous risk assessment;
- Follow-up actions form previous management review;
- Any changes that could affect the ITS2MS;
- Review of ITS2MS Policy and Objectives;
- Recommendations for improvement.

The output from the management review shall include any decisions and actions related to the following:

Improvement of the effectiveness of the ITS2MS.

Modification of procedures that effect information security, as necessary, to respond to internal or external events that may impact on the ITS2MS, including changes to:

- Business requirements;
- Security requirements;
- Business processes effecting the existing business requirements;
- Regulatory or legal environments;
- Levels of risk and / or levels of risk acceptance.
- Resource needs.

The minutes of the meetings are circulated to all the Management Review participants. The Head, Process Improvement tracks the actions points to closure.

6 DEPARTMENTS

- IT Admin
- Stores Noida/Mumbai/Bangalore/Hyderabad
- SD (N & S)
- SD (Backup)
- SD (V&S)
- SD (Windows/Linux)
- Cloud4C CRM
- Cloud4C Infra
- Cloud4C Implementation
- Cloud4C PM team
- Training
- HR
- Sales
- Marketing
- Procurement
- Automation
- Presales
- Cloud4C International Sites

Please refer latest Org chart or Audit plan to view complete teams list.

8 AUDIT PLAN

Dept. to be audited	Year 20XX											
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec

Annual Internal Audit Calendar – 20XX						
Month	Opening Date and Time	Closing Date and Time	Department Name	Auditee (s)	Auditor1 (s)	Lead Auditor(s)

9 TRAINING

Cloud4C shall ensure all team members undergo periodical training outlined in this policy.

10 REVIEW OF THE POLICY

- This document will be reviewed and updated on an annual basis or when significant changes occur to the organization systems and information security standards.