Requirements for Empanelment of Cloud Audit Organisation

APRIL 2017

(CSP-02-03), Issue-1

STQC Directorate,
Ministry of Electronics & Information Technology,
Electronics Niketan, 6 CGO Complex, Lodi Road,
New Delhi – 110003

Title - Procedure and Requirements for Empanelment of Cloud Audit Organisation

Purpose - Purpose of this document is to define Procedure and Requirements for third party audit organisations and auditors for cloud services, who intend to provide their audit services for empanelment / certification of Cloud Service Providers.

Objective - Objective is to define criteria for empanelment for third party audit organisations /auditors who are competent to assess CSP for compliance as per defined requirements and criteria. The effectiveness of audit organisations is ensured by -

a. Having a formal system as per international standard ISO/IEC 17021:2011 to ensure audit results are reliable, repeatable and reproducible
b. Auditors of audit organisation who are professional, competent and have Knowledge, skill and experience in the area of cloud auditing.
c. Auditors who are well versed with the current technologies and standards published on this subject area and MeitY policies of empanelment/certification of CSPs.

Reference Document

1) ISO/IEC 17021:2011 : Conformity assessment -- Requirements for bodies providing audit and certification of management systems

Definitions

Cloud Auditor

A cloud auditor is a party that can conduct independent assessment of cloud services, information system operations, performance and the security of a cloud Service providers. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, and adherence to service level agreement parameters. He should possess education, skill set and experience as described in this document to conclude the ability of the process (Security, Performance, Privacy etc.) to meet the contractual agreements between CSP and Cloud user.

Structure of the document:

This document has three parts:

- Part I Procedure
- Part II Requirements
- Part III Auditor Qualification and Experience

Part - I

Procedure

1. The audit organisation which intends to get empanelled with STQC shall apply in a prescribed format to STQC (CSP-02-01), along with their quality manual / procedures and prescribed fee.
2. The generic requirement is cloud audit organisation shall be ISO 9001 Certified with Cloud Service auditing [also referred to as Cloud Service Provider (CSP) auditing] as one of the scope items.
3. The applicant shall prepare a compliance statement with the specific requirements which are based on ISO 17021 and given in Part II (Requirements) of this document in the column "comments". Reference to clause no. of internal procedure /policies /process shall be given.

   These requirements focus on specifics of Audit Organisations in the broad categories of:

   - Legal and contractual Matters, Management of impartiality and liability
   - Organisation Structure
   - Resource requirements
   - Information Management
   - Process and Handling of CSP audit data

4. The auditing organisation should have procedure to audit CSPs , additionally they should use following two STQC procedures for CSP empanelment / certification scheme operated by STQC:
   a. Cloud Service Provider: Audit Criteria - CSP-01-03
   b. Cloud Service Provider: Audit Report - CSP-01-07

5. The audit organisation shall provide the list of auditors specifying their competence, educational qualifications, skill-sets and experience with the following as a requirement given in part III.

6. STQC (The empanelment Body) will depute a team of evaluators to assess applicant Audit organisation. The audit team will evaluate the applicant based on the requirements Part II and Part III of this document and on the satisfactory completion of the audit, submit a report (CSP-02-04).

Part II

Requirements for Bodies Providing Audit of Cloud Service Providers (CSP)

ISO/IEC 17021 Requirements	Compliance (Y/N)	Comment
1. General requirements **1.1. Legal and contractual matters**		
1.1.1. Legal responsibility Legal entity or a defined part of a legal entity that can be held legally responsible. • *Verify registration with Registers of Companies* • *Governmental auditing body is a legal entity based on its governmental status. Identity department.*		
1.1.2. Auditing agreement Legally enforceable agreement (contract) for provision of auditing activities to customer? • *Are multiple offices of a auditing body or multiple sites of a audited customer covered by the agreement?* • *Are all the sites covered by the scope of the auditing?*		
1.1.3. Responsibility for auditing decisions Does auditing body retain authority and responsibility for its decisions relating to auditing?		
1.2. Management of impartiality		
1.2.1. Is auditing body top management commitment to impartiality? *Is there a publicly accessible statement?* *Does it cover:* • *Importance of impartiality* • *Conflict of interest and* • *Objectivity of its management system auditing activities?*		
1.2.2. Are conflicts of interest identified, analysed and documented and managed through the system? • *Are relationships posing a threat to impartiality documented?* • *How does the auditing body demonstrate that it eliminates or minimizes such threats?* • *Information made available to the impartiality Committee?* ***Note**: A relationship that threatens the impartiality of the auditing body can be based on ownership, governance, management,*		

personnel, shared resources, finances, contracts, marketing and payment of a sales commission or other inducement for the referral of new clients, etc.		
1.2.3. Not offering auditing when relationships that threaten impartiality cannot be eliminated or minimized.		
1.2.4. Does the auditing body audit another auditing body as per ISO 17021 management system auditing activities as an Audit Organization of a CSP		
1.2.5. Do the auditing body and any part of the same legal entity offer or provide management system consultancy (ISO 27001, 27018, 27017 etc.) ? This applies also to that part of government identified as the auditing body.		
1.2.6. Does the auditing body provide internal audits to its audited customers? (as per 27001, 27017, 27018) Does the auditing body audit a management system on which it provided internal audits within 2 years following the end of the internal audits? This applies also to that part of government identified as auditing body.		
1.2.7. Does the auditing body audit a customer when the auditing body's relationship with a management system consultancy or internal audits, poses an unacceptable threat to the impartiality of the auditing body?		
1.2.8. Does the auditing body outsource audits to a consultancy organization? (Unacceptable threat to impartiality).		
1.2.9. Are the auditing body's activities marketed or linked with consultancy? • *Auditing body takes action to correct inappropriate claims by any consultancy organization?* • *Are there any implications by auditing body that auditing would be simpler, easier, faster or less expensive if a specified consultancy organization is used?*		
1.2.10. Does auditing body ensure no conflict of interest of personnel? *2 Years rule applied, how effective is the process?*		
1.2.11. Is action taken to respond to any threats to auditing body's impartiality arising from the Actions of other persons, bodies or organizations?		
1.2.12. Do all auditing body personnel, internal, external or committees act impartially and does the auditing body allow commercial, financial or other pressure to compromise impartiality?		

1.2.13.	Does the auditing body require all personnel to reveal any conflict of interest situations? Information used as input to identifying threats to impartiality?		
1.3.	**Liability and Financing**		
1.3.1.	Is the auditing body able to demonstrate that it has evaluated risks arising from its auditing activities and that it has adequate arrangements (e.g. insurance or reserves) to cover liabilities arising from its operations in each of its field of activities and the geographic areas in which it operates?		
1.3.2.	Does the auditing body evaluate its finances and sources of income and demonstrate to the committee that initially and on an ongoing basis, commercial, financial or other pressures do not compromise its impartiality?		
2. **2.1.**	**Structural requirements** **Organizational structure and top management**		
2.1.1.	Organizational structure documented including duties, responsibilities and authorities for personnel and committees; and relationships to other parts within the same legal entity?		
2.1.2.	Does the auditing body identify the top management (board, group of persons, or person) having overall authority and responsibility for each of the following: a) development of policies relating to the operation of the body? b) supervision of the implementation of policies and procedures? c) supervision of the finances of the body? d) Development of management system auditing services and schemes? e) Performance of audits and auditing and responsiveness to complaints? f) Decisions on auditing? g) delegation of authority to committees or individuals, as required, to undertake defined activities on its behalf? h) Contractual arrangements? i) Providing adequate resources for auditing activities?		
2.1.3.	Formal rules for the appointment, terms of reference and operation of any committees involved in the auditing activities?		

2.2. Committee for safeguarding impartiality		
2.2.1. Does the structure of the auditing body safeguard the impartiality of the activities of the auditing body and does it provide for a committee to: a) Assist in developing the policies relating to impartiality of its auditing activities? b) Counteract any tendency on the part of an auditing body to allow commercial or other considerations to present the consistent objective provision of auditing activities? c) advise on matters affecting confidence d) including openness and public perception? e) Conduct an annual review of the impartiality of the audit and decision-making processes of the auditing body?		
2.2.2. Is the composition, terms of reference, duties, authorities, competence of members and responsibilities of this committee formally documented and authorized by top management of the auditing body to ensure: a) representation of a balance of interests? b) access to all the information c) The right to take independent action, where the top management of the auditing body does not respect the advice of the committee Is confidentiality maintained when taking independent actions?		
2.2.3. Are key interests identified and invited to this committee?		
3. Resource requirements **3.1. Competence of management and personnel**		
3.1.1. Does an auditing body have a process to ensure that personnel have appropriate knowledge relevant to the types of management systems and geographical areas in which it operates? Is competence required for each technical area and for each function in the auditing activity determined for each technical area? Is the means for the demonstration of competence determined?		
3.1.2. Are competences requirements determined for all auditing body personnel and are this as per documented process? Is the documented process as per auditing scheme?		
3.1.3. Evaluation processes Does the auditing body have documented processes for the initial competence evaluation and on-going monitoring of competence and performance of all personnel involved in the management and performance of audits and auditing? Are these methods effective?		
3.1.4. Other considerations		

3.1.4.1. Does the auditing body address the functions undertaken by management and administrative personnel while determining the competence requirements? 3.1.4.2. Does the auditing body have access to the necessary technical expertise for technical areas, types of management system and geographic areas in which it operates?		
3.2. Personnel involved in the auditing activities		
3.2.1. Does the auditing body as part of its own organization have personnel with sufficient competence for managing the type and range of audit programmes and other auditing work performed?		
3.2.2. Does the auditing body employ or have access to a sufficient number of auditors including audit team leaders and technical experts to cover all activities and volume of work?		
3.2.3. Does the auditing body make clear to each person concerned duties, responsibilities and authorities?		
3.2.4. Does the auditing body have defined processes for: • Selecting • Training • Formally authorizing auditors and • Selecting technical experts? Does the initial competence evaluation of an auditor include the ability to apply required knowledge and skill during audits, as determined by a competent evaluator observing (witnessing) the auditor conducting an audit?		
3.2.5. Does the auditing body have a process to achieve and demonstrate effective auditing, including the use of auditors and audit team leaders possessing generic auditing skills and knowledge in specific technical areas? Does the auditing body define the knowledge and skills for specific auditing functions?		
3.2.6. Are auditors and technical experts knowledgeable of the auditing body's audit processes, auditing scheme and its requirements and other relevant requirements? Does the auditing body give auditors and technical expert's access to an up-to-date set of documented procedures giving audit instructions and all relevant information on the auditing activities?		
3.2.7. Are auditors and technical experts used in these activities where they have demonstrated competence?		
3.2.8. Are training needs identified for functions performed? Where there is need, is training offered or provided?		
3.2.9. Are person(s) taking the auditing decisions knowledgeable on the: • applicable standard; • auditing requirements; • have demonstrated competence to evaluate the audit processes and		

	related recommendations of the audit team?		
3.2.10.	Does documented procedures and criteria for monitoring and measurement of performance of all personnel exist? Competence reviewed to identify training needs?		
3.2.11.	Do procedures include a combination of on-site observation, review of audit reports and feedback from customers or from the market?		
3.2.12.	Does the auditing body periodically observe the performance of each auditor on-site? Is the frequency of on-site observations based on need determined from all monitoring information available?		
3.3.	**Use of individual external auditors and external technical experts**		
	Does an auditing body have a written agreement with external auditors and external technical experts in place by which they commit themselves to comply with applicable policies and procedures as defined? Does the agreement address all relevant aspects?		
3.4.	**Personnel records**		
3.4.1.	Does the auditing body maintain up-to-date personnel records including: • Relevant qualifications; • Training; • Experience; • Affiliations; • Professional status; • Competence; and • Any relevant consultancy services? Does this include management and administrative personnel in addition to those performing auditing activities?		
3.5.	**Outsourcing**		
3.5.1.	Does the auditing body have a process in which it describes the conditions under which outsourcing may take place? Legally enforceable agreement with each body that provides outsourced services?		
3.5.2.	Is the auditing body outsourcing auditing decisions?		
3.5.3.	Does the auditing body: a) take responsibilities for all activities outsourced? b) ensure that the body that provides outsources activities: • conforms to the auditing body's requirements • conforms to the applicable provisions of this international standard including competence, impartiality and confidentiality? c) ensure that the outsourced services are not involved in any way that impartiality could be compromised?		
3.5.4.	Documented procedures for the qualification and monitoring of all outsourced services used for auditing activities?		

	Records of the competence of auditors and technical experts maintained?		
4.	**Information requirements**		
4.1.	**Publicly accessible information**		
4.1.1.	Does the auditing body maintains and make publicly accessible or provide upon request information describing its audit processes, auditing processes and about the auditing activities, types of management systems and geographical areas in which it operates?		
4.1.2.	Is the information provided by the auditing body to any client or to the market place including advertising accurate and not misleading?		
4.1.3.	Does the auditing body on request from any party provide means to confirm the validity of a given auditing report.		
4.2.	Auditing documents		
4.2.1.	Does the auditing body provide auditing documents to the audited client by any means it chooses?		
4.2.2.	Is the effective date on a auditing document the date before the auditing decision?		
4.2.3.	Does the auditing document(s) identify the following: a) The name and geographic location of each client and any sites within the scope of a multi-site auditing? b) The dates of conducting auditing? c) The re-auditing due date consistent with the re-auditing cycle? d) a unique identification code? e) The standard and/or other normative document including issue number and/or revision used for the audited customer? f) The scope of auditing with respect to product (including service), process, etc. as applicable at each site? g) The name, address and auditing mark of the auditing body; other marks (e.g. accreditation symbol)? h) Any other information required by the standard and/or other normative document used for auditing? i) In the event of issuing any revised auditing documents, a means to distinguish the revised documents from any prior obsolete documents?		
4.3.	**Directory of audited customers**		
	Does the auditing body maintain and make publicly accessible or provide upon request, by any means it chooses, a directory of valid auditing reports		
4.4.	**Reference to auditing and use of marks**		
4.4.1.	Does the auditing body have a policy governing any mark that it authorizes audited customers to use?		
4.4.2.	Does the auditing body require that the client organization: a) Conforms to the requirements of the auditing body when making reference to its auditing status in communication media?		

	b) Does not make or permit any misleading statement regarding its auditing? c) Does not use or permit the use of a auditing document or any part thereof in a misleading manner? d) Upon suspension or withdrawal of its auditing discontinues its use of all advertising matter that contains a reference to auditing, as directed by the auditing body? e) Amends all advertising matter when the scope of auditing has been reduced? f) Does not imply that the auditing applies to activities that are outside the scope of auditing? And g) Does not use its auditing in such a manner that would bring the auditing body and/or auditing system into disrepute and lose public trust?		
4.4.3.	Does the auditing body exercise proper control of ownership and take action to deal with incorrect references to auditing status or misleading use of audit reports?		
4.5.	**Confidentiality**		
4.5.1.	Does the auditing body through legally enforceable agreements have a policy and arrangements to safeguard the confidentiality of the information at all levels of its structure, including committees and external bodies or individuals acting on its behalf?		
4.5.2.	Client informed by the auditing body of the confidential information it intends to place in the public domain?		
4.5.3.	Is information about a particular client or individual disclosed to a third party without the written consent of the client or individual concerned? Where the auditing body is required by law to release confidential information to a third party, is the customer or individual concerned, unless regulated by law, notified in advance of the information provided?		
4.5.4.	Is information about the client treated as confidential, consistent with the auditing body's policy?		
4.5.5.	Do all personnel acting on the auditing body behalf keep confidential all information obtained or created during the performance of the auditing body's activities?		
4.5.6.	Does the auditing body have available and use equipment and facilities that ensure the secure handling of confidential information (e.g. documents, records)?		
4.5.7.	When confidential information is made available to other bodies (e.g. Accreditation Body, agreement group of a peer assessment scheme) does the auditing body inform its client of this action?		
4.6.	**Information exchange between a auditing body and its customers**		
4.6.1.	Information on the auditing activity and requirements Does the auditing body provide and update clients on the following:		

	a) a detailed description of the initial and continuing auditing activity including the application, initial audits, surveillance audits b) The normative requirements for auditing? c) Information about the fees for application, initial auditing and continuing auditing? d) The auditing body's requirements for the prospective customer: 1. To comply with auditing requirements? 2. To make all necessary arrangements for the conduct of the audits including provision for examining documentation and the access to all processes and areas, records and personnel for the purposes of initial auditing, surveillance, re-auditing and resolution of complaints, and? 3. To make provisions where applicable to accommodate the presence of observers (e.g. accreditation auditors or trainee auditors)? e) Documents describing the rights and duties of audited clients including requirements when making reference to its auditing in communication of any kind in line with the requirements? f) Information on procedures for handling complaints and appeals?		
4.6.2.	Notice of changes by a auditing body Does the auditing body give its audited clients due notice of any changes to its requirements for auditing? Does the auditing body verify that each audited client complies with the new requirements?		
4.6.3.	Notice of changes by a client Legally enforceable arrangements to ensure that the audited customer informs the auditing body of matters that may affect the management system's ability to continue to fulfil the requirements of the standard/criteria used for auditing?		
5. **5.1.**	**Process requirements** **General requirements**		
5.1.1. 5.1.1.1. 5.1.1.2. 5.1.1.3.	Audit programme Is the audit programme for the full auditing cycle developed and does it clearly identify the audit activity (ies) required for auditing to the selected standard(s) or other normative documents? Does the audit programme include a two stage initial audit, surveillance audits in the 1st and 2nd years and a re-auditing audit in the 3rd year prior to expiration of auditing? (The 3-year auditing cycle begins with the auditing or re-auditing decision). Where a auditing body is taking account of auditing or other audits already granted to the customer, does it collect		

sufficient, verifiable information to justify and record any adjustments to the audit programme?		
5.1.2. Audit plan 5.1.2.1. General Is an audit plan established for each audit to provide the basis for agreement regarding the conduct and scheduling of the audit activities? Is the audit plan based on documented requirements of the auditing body? 5.1.2.2. Determining audit objectives, scope and criteria 5.1.2.2.1. Does the auditing body determine the audit objectives? Is the audit scope and criteria including changes established by the auditing body after discussions with the client? 5.1.2.2.2. Are audit objectives describe what is to be accomplished by the audit and does it include the following: a) determination of the conformity of the client's management system, or parts of it, with the audit criteria b) evaluation of the ability of the management system to ensure the client organization meets applicable statutory, regulatory and contractual requirements c) evaluation of the effectiveness of the management system to ensure the client organization is continually meeting its specified objectives d) as applicable, identification of areas of potential improvement of the management system 5.1.2.2.3. Does the audit scope describe the extent and boundaries of the audit? Where the initial or re-auditing process consists of more than one audit, are total audits consistent with the scope in the auditing? 5.1.2.2.4. Is the audit criteria used as a reference against which conformity is determined and does it include: • The requirements of a defined normative document on management systems • The defined processes and documentation of the management system developed by the client 5.1.2.3. **Preparing the audit plan:** Is the audit plan appropriate to the objectives and the scope of the audit; and **Preparing the audit plan:** Does it at least include or refer to the following: a. The audit objectives b. The audit criteria c. The audit scope including identification of the organizational and functional units or processes to be audited d. The dates and sites where the on-site audit activities are to be conducted including visits to temporary sites, as appropriate e. The expected time and duration of on-site audit activities f. The roles and responsibilities of the audit team members and accompanying persons		

5.1.3. Audit team selection and assignments 5.1.3.1. Process in place for selecting and appointing the audit team taking into account the competence needed to achieve the objectives of the audit? Where there is only one auditor, is the auditor competent to perform? 5.1.3.2. In deciding the size and composition of the audit team was the following considered: a) audit objectives, scope, criteria and estimated time of the audit b) whether the audit is a combined, integrated or joint audit c) the overall competence of the audit team needed to achieve the objectives of the audit d) Auditing requirements (including any applicable statutory, regulatory or contractual requirements? e) Language and culture f) Whether the members of the audit team have previously audited the client's management system. 5.1.3.3. Where the necessary knowledge and skill of the audit team leader and auditors was supplemented by technical experts, translators and interpreters, were they selected such that they do not unduly influence the audit? 5.1.3.4. Where auditors-in-training are included in the audit team as participants, was an evaluator appointed? Was the evaluator competent to take over the duties and have final responsibility for the activities and findings of the auditor-in-training? 5.1.3.5. Does the audit team leader, in consultation with the audit team assign to each team member responsibility for specific processes, functions, sites, areas or activities and are such assignments taking into account the need for competence? Were changes to assignments made to ensure achievement of the audit objectives?		
5.1.4. Determining audit time 5.1.4.1. Does the auditing body have documented procedures for determining audit time need to plan and accomplish a complete and effective audit? Does the procedure based on international norms like IAF GD2 and GD6 documents? In determining the audit time, does the auditing body consider among other things the following aspects: a. The requirements of the standard? b. Size and complexity? c. Technological and regulatory context? d. Any outsourcing? e. The results of any prior audits? f. Number of sites and multi-site considerations? g. The risks associated with the services, processes or activities of the organization? h. When audits are combined, joint or integrated? i. Specific criteria for specific auditing scheme where established?		

5.1.4.2. Does the auditing body include time spent by any team member that is not assigned as an auditor?		
5.1.5. Multi-site sampling Where multi-site sampling is utilized, did the auditing body develop an adequate sampling programme to ensure proper audit of the management system? Is the rationale for the sampling plan documented? (IAF guidance applies)		
5.1.6. Communication of audit team tasks Are the tasks given to the audit team defined and make known to the client? Does the audit team: a) Examine and verify the structure, policies, processes, procedures, records and related documents of the customer organization relevant to the management system? b) Determine that these meet all the requirements relevant to the intended scope of auditing? c) Determine that the processes and procedures are established, implemented and maintained effectively, to provide a basis for confidence in the client management system? and d) Communicate to the customer, for its action, any inconsistencies between the customer's policy, objectives and targets and the results?		
5.1.7. Communication concerning audit team members Does the auditing body provide the name and, when requested, make available background information of each member of the audit team with sufficient time for the client organization to object to the appointment of any particular auditor or technical expert and for the auditing body to reconstitute the team in response to any valid objection?		
5.1.8. Communication of audit plan Is the audit plan communicated and the dates of the audit agreed upon, in advance, with the client organization?		
5.1.9. Conducting on-site audits 5.1.9.1. General Does the auditing body have a process for conducting on-site audits? Does the process include opening meeting at the start of the audit and closing meeting at the conclusion of the audit? 5.1.9.2. Conducting the opening meeting Does the audit team have a formal opening meeting with the client's management and those responsible for the functions or processes to be audited? Is the opening meeting conducted by the Lead auditor? Are audit activities explained including the following: a) Introduction of the participants including an outline of their roles b) Confirmation of the scope of auditing c) Confirmation of the audit plan (including type and scope of audit, objectives and criteria), any changes and other relevant arrangements with the client such		

as the date and time for the closing meeting, interim meetings between the audit team and client's management d) Confirmation of formal communication channels between the audit team and the client e) Confirmation that the resources and facilities needed by audit team are available f) Confirmation of matters relating to confidentiality g) Confirmation of relevant work safety, emergency and security procedures for the audit team h) Confirmation of the availability, roles and identities of any guides and observers i) The method of reporting including any grading of audit findings j) Information about the conditions under which the audit may be prematurely terminated k) Confirmation that the audit team leader and audit team representing the auditing body is responsible for the audit and shall be in control of executing the audit plan including audit activities and audit trails l) confirmation of the status of findings of the previous review or audit, if applicable m) methods and procedures to be used to conduct the audit based on sampling n) confirmation of the language to be used during the audit o) confirmation that during the audit the client will be kept informed of audit progress and any concerns p) opportunity for the client to ask questions 5.1.9.3. Communication during the audit 5.1.9.3.1. During the audit does the audit team periodically assess audit progress and exchange information and does the team leader re-assign work as needed between the audit team members and periodically communicate the progress of the audit and any concerns to the client? 5.1.9.3.2. Does the audit team leader report to the client and where possible to the auditing body presence of an immediate and significant risk (e.g. safety)? Is the outcome of the action taken reported to the auditing body? 5.1.9.3.3. Does the team leader review with the client any need for changes to the audit scope which becomes apparent as on-site auditing activities progress and report this to the auditing body? 5.1.9.4. Observers and Guides 5.1.9.4.1. Observers Prior to the conduct of the audit does the client agree to the presence and justification of observers during an audit activity? 5.1.9.4.2. Guides Does each auditor accompanied by a guide, unless otherwise agreed to by the audit team leader and the client? Does the audit team ensure that guides do not		

influence or interfere in the audit process or outcome of the audit? 5.1.9.5. Collecting and verifying information 5.1.9.5.1. Is information relevant to the audit objective, scope and criteria collected by appropriate sampling and verified to become audit evidence? 5.1.9.5.2. Are methods to collect information included? a) interviews b) observation of processes and activities c) review of documentation and records 5.1.9.6. Identifying and recording audit findings 5.1.9.6.1. Are audit findings summarizing conformity and detailing non-conformity audits and its supporting evidence recorded and reported? 5.1.9.6.2. Where opportunities for improvement are not prohibited by the requirements of a management system scheme, are they identified and recorded? 5.1.9.6.3. Is a finding of non-conformity recorded against a specific requirement of the audit criteria and does it contain a clear statement of the non-conformity and identify in detail the objective evidence on which the non-conformity is based? Are non-conformities discussed with the client to ensure that the evidence is accurate and that the non-conformities are understood? 5.1.9.6.4. Does the audit team leader attempt to resolve any diverging opinions between the audit team and the client concerning audit evidence on findings and are unresolved points recorded? 5.1.9.7. Preparing audit conclusions Prior to the closing meeting does the audit team: a) review the audit findings and any other appropriate information collected during the audit against the audit objectives b) agree upon the audit conclusions taking into account the uncertainty inherent in the audit process c) identify any necessary follow-up actions d) confirm the appropriateness of the audit programme or identify any modification required (e.g. scope, audit time or dates, surveillance frequency, competence) 5.1.9.8. Conduct the closing meeting 5.1.9.8.1. Does the team hold a formal closing meeting with management and are nonconformities presented in such a manner that they are understood, and are timeframes for responding agreed? Is attendance recorded? 5.1.9.8.2. Does the closing meeting include the following: a) advising the client that the audit evidence collected was based on sample of the information; thereby introducing an element of uncertainty b) the method and timeframe of reporting including any grading of audit findings		

c) the auditing body's process for handling nonconformities including any consequences relating to the status of the client's auditing d) the timeframe for the client to present a plan for correction and corrective action for any nonconformities identified during the audit e) the auditing body's post audit activities f) information about the complaint handling and appeal processes 5.1.9.8.3. Is the client given opportunity for questions? Are diverging opinions regarding the audit findings or conclusions discussed, resolved where possible? Are unresolved diverging opinions recorded and referred to the auditing body?		
5.1.10. Audit report 5.1.10.1. Does the auditing body provide a written report for each audit and is ownership of the report maintained by the auditing body? If the audit team identifies opportunities for improvement, do they recommend specific solutions? 5.1.10.2. Does the team leader ensure that the report is prepared and takes responsibility of the content of the report? Does the report provide accurate, concise and clear record of the audit and does it include the following: a) identification of the auditing body b) name and address of the client's management representative c) type of audit (e.g. initial, surveillance or re-auditing) d) audit criteria e) audit objectives f) audit scope, particularly identification of the organizational of functional units or processes audited and the time of the audit g) identification of the audit team leader, audit team members and any accompanying persons h) dates and places where the audit activities (on-site of offsite) were conducted i) audit findings, evidence and conclusions, consistent with the requirements of the type of audit j) any unresolved issues, if identified		
5.1.11. Cause analysis of nonconformities Does the auditing body require the client to analyse the cause and describe the specific correction and corrective actions taken or planned to be taken to eliminate detected non-conformities within a define timeline?		
5.1.12. Effectiveness of corrections and corrective actions Does the auditing body review the corrections, identified causes and corrective actions submitted by the customer to determine if these are acceptable? Does the auditing body verify the effectiveness of any correction and corrective action taken? Is the evidence obtained to support the		

	resolution of non-conformities recorded? Does the client get informed of the result of the review and verification?		
5.1.13.	Auditing decision Is the client informed if an additional full audit, an additional limited audit or documented evidence (to be confirmed during future surveillance audits) will be needed to verify effective correction and corrective actions?		
5.1.14.	Does the auditing body ensure that the persons or committees that make the auditing or re-auditing decisions are different from those who carried out the audits?		
5.1.15.	Actions prior to making a decision Does the auditing body confirm, prior to making a decision that: a) The information provided by the audit team is sufficient? b) It has reviewed, accepted and verified the effectiveness of corrections and corrective actions for all non-conformities that represent: 1. failure to fulfil one or more requirements of the standard? or 2. a situation that raises significant doubt about the ability of the customer's management system to achieve its intended outputs c) It has reviewed and accepted the client's planned correction and corrective action for any other non-conformity?		
5.2.	**Initial audit and auditing**		
5.2.1.	Application Does the auditing body require an authorized representative of the applicant organization to provide the necessary information to enable it to establish: a) The desired scope of the auditing? b) The general features of the applicant organization including its name and the address(es) of its physical location(s), significant aspects of its process and operations and any relevant legal obligations? c) General information relevant for the field of auditing applied for, concerning the applicant organization, such as its activities, human and technical resources, functions and relationship in a larger corporation, if any? d) Information concerning all outsourced processes used by the organization that will affect conformity to requirements? e) The standards or other requirements for which the applicant organization is seeking auditing? f) Information concerning the use of consultancy relating to the management system?		
5.2.2.	Application review		

5.2.2.1. Before proceeding with the audit does the auditing body conduct a review of the application and supplementary information for auditing to ensure that: a) The information about the applicant and its management system is sufficient for the conduct of the audit? b) The requirements for auditing are clearly defined and documented and have been provided to the applicant organization? c) Any known difference in understanding between the auditing body and the applicant organization is resolved? d) The auditing body has the competence and ability to perform the auditing activity? e) The scope of auditing sought, the location(s) of the applicants' organization's operations, time required to complete f) Audits and any other points influencing the auditing activity are taken into account (language, safety conditions, threats to impartiality, etc.)? g) Records of the justification for the decision to undertake the audit shall be maintained? 5.2.2.2. Following the review of the application does the auditing body accept or decline an application or auditing? When declined, are reasons for declining documented made clear to the client? 5.2.2.3. Based on this review does the auditing body determine the competences it needs to include in its audit team and for the auditing decision? 5.2.2.4. Is the audit team appointed and do they have the totality of the competences identified by the auditing body as set out for the auditing of the applicant organization? Is selection of the team performed with reference to the designations of competence of auditors and technical experts made? 5.2.2.5. Is the individual(s) who will be conducting the auditing decision appointed to ensure appropriate competence is available?		
5.2.3. Initial audit Is the initial audit of a management system conducted in two stages – Stage 1 and Stage 2 5.2.3.1. Stage 1 audit 5.2.3.1.1. Is the stage 1 audit performed: a) to audit the client's management system documentation (ISMS, ITSM, etc.); b) to evaluate the client's location and site-specific conditions and to undertake discussions with the client's personnel to determine to the preparedness for the Stage 2 audit; c) to review the client's status and understanding regarding requirements of the standard, in particular with respect to the identification of key performance		

or significant aspects, processes, objectives and operation of the management system? d) to collect necessary information regarding the scope of the management, processes and location(s) of the client, and related statutory and regulatory aspects and compliance (e.g. IT Act, Aadhaar Act, legal aspects of the client's operation, associated risks, etc.)? e) to review the allocation of resources for Stage 2 audit and agree with the client on the details of the Stage 2 audit? f) to provide a focus for planning the Stage 2 audit by gaining a sufficient understanding of the client's management system and site operations in the context of possible significant aspects? g) to evaluate if the initial audits and management review are being planned and performed and that the level of implementation of the management system substantiates that the client is ready for the Stage 2 audit? h) For most management systems it is recommended that at least part of the Stage 1 audit be carried out at the client's premises in order to achieve the objectives stated above. 5.2.3.1.2. Are Stage 1 audit findings documented and communicated to the client organization including identification of any areas of concern that could be classified as nonconformity during Stage 2 audit? 5.2.3.1.3. In determining the interval between Stage 1 and Stage 2, is consideration given to the needs of the client to resolve areas of concern identified during the Stage 1 audit? The auditing body may also need to revise its arrangement for Stage 2 5.2.3.2. Stage 2 audit 5.2.3.2.1. The purpose of the Stage 2 audit is to evaluate the implementation including effectiveness of the customer's management system (ISMS, ITSM, etc.). Is the Stage 2 audit taking place at the site(s) of the client? Does it include at least the following: a) Information and evidence about conformity to all requirements of the applicable management system standard or other normative document? b) performance monitoring, measuring, reporting and reviewing against key performance objectives and targets? c) the client's management system and performance as regards legal compliance? d) operational control of the client's processes? e) internal auditing and management review? f) management responsibility for the client organization's policies?		

g) links between the normative requirements, policy, performance objectives and targets, any applicable legal requirements, responsibilities, competence of personnel, operations, procedures, performance data and internal audit findings and conclusions? h) Internal procedure for handling Audit related data should be in line with CSP-02-05		
5.2.4. Initial auditing audit conclusions Does the audit team analyze all information and audit evidence gathered during the Stage 1 and Stage 2 audits to review the audit findings and agree on the audit conclusions?		
5.2.5. Information for granting initial auditing 5.2.5.1. Does the information provided by the audit team to the auditing body for the auditing decision include as a minimum: a) the audit reports? b) comments on the nonconformities and, where applicable, the correction and corrective actions taken by the client? c) Confirmation on the information provided to the auditing body used in the application review? and d) A recommendation whether or not to grant auditing together with any conditions or observations? 5.2.5.2. Does the auditing body make the auditing decision on the basis of an evaluation of the audit findings and conclusions and any other relevant information (e.g. public information, comments on the audit report from the customer)?		
5.3. Surveillance activities 5.3.1. General 5.3.1.1. Did the auditing body develop its surveillance activities so that representative areas and functions covered by the scope of the management system are monitored on a regular basis and take into account changes to its audited client and its management system? Is surveillance audit done as per agreement with certification body/Recognised body? 5.3.1.2. Do surveillance activities include on-site audits assessing the audited client's management system fulfilment of specified requirements with respect to the standard to which the auditing is granted? Other surveillance activities may include: a) Enquiries from the auditing body to the audited on aspects of auditing; b) Reviewing any client's statements with respect to its operations (e.g. promotional material, website); c) Requests to the client to provide documents and records (on paper or electronic media); and d) Other means of monitoring the audited client's performance.		

5.3.2. Surveillance audit 5.3.2.1. Are on-site audits planned with other surveillance activities, so that the auditing body can maintain confidence that the audited management continues to fulfil requirements in between re-auditing audits? Does the surveillance audit programme include at least: a) Internal audits and management review? b) Review of action taken on non-conformities identified during the previous audits? c) Treatment of complaints? d) Effectiveness of the management system with regard to achieving the audited client's objectives? e) Progress of planned activities aimed at continual improvement? f) continuing operational cost? g) review of any changes? and h) Use of marks and/or any other reference to auditing? 5.3.2.2. Are surveillance audits conducted at least once a year? Is the date of the 1st surveillance audit following initial auditing not more than12 months from the last day of the Stage 2 audit?		
5.3.3. Maintaining auditing status Does the auditing body maintain auditing status (audit conclusion) based on demonstration that the client continues to satisfy the requirements of the management system standard? Does the auditing body maintain an organization's auditing based on a positive recommendation by the audit team leader without further independent review provided that: a) For any nonconformity or other situation that may lead to suspension or withdrawal of auditing, the auditing body needs to initiate a review by appropriately competent personnel different from those who carried out the audit to determine whether auditing can be maintained? and b) Competent personnel of the auditing body monitor its surveillance activities, including monitoring the reporting by its auditors, to confirm that the auditing activity are operating effectively?		
5.4. Re-auditing		
5.4.1. Re-auditing cycle 5.4.1.1. Is a re-auditing audit planned and conducted to evaluate the continued fulfilment of all the requirements of the relevant management system standard or other normative document? 5.4.1.2. Does the re-auditing audit consider the performance of the management system over the period of auditing and include the review of previous surveillance audit reports? 5.4.1.3. In situations where they have been significant changes (e.g. changes to legislation, management, processes, etc.) do the re-auditing audit activities include a Stage 1 audit?		

5.4.1.4. In the case of multiple sites or auditing multiple management system standards being provided by the auditing body, does the planning for the audit ensure adequate onsite audit coverage to provide confidence in the auditing?		
5.4.2. Re-auditing audit 5.4.2.1. Does the re-auditing audit include an on-site audit that addresses the following: a) the effectiveness of the management system? b) demonstrated commitment to maintain the effectiveness and improvement? c) Whether the operation of the audited management system contributes to the achievement of the organization's policy and objectives? 5.4.2.2. When during a re-auditing audit instances of nonconformity or lack of evidence of conformity are identified, does the auditing body define time limits for correction and corrective actions to be implemented prior the expiry of auditing?		
5.4.3. Information for granting re-auditing Does the auditing body make decisions on renewing auditing based on: • The results of re-auditing audit? • The results of the review of the system over the period of auditing? and • The complaints received from users of auditing?		
5.5. Special audits		
5.5.1. Extensions to scope Does the auditing body in response to an application for extension to the scope of a auditing already granted, undertake a review of the application and determine any audit activities necessary to decide whether or not the extension may be granted? (This may be conducted in conjunction with a surveillance audit)		
5.5.2. Short-notice audits If it is necessary for the auditing body to conduct audits of audited clients at short notice to investigate complaints or in response to changes or as follow up on suspended customers : a) Does the auditing body describe and make known in advance to the audited clients the conditions under which these short notice visits are to be conducted? And b) Does the exercise take additional care in the assignment of the audit team because of the lack of opportunity for the client to brief audit team members?		
5.6. Suspending, withdrawing or reducing scope of auditing		
5.6.1. Does the auditing body have a policy and documented procedure(s) for suspension, withdrawal or reduction of the		

	scope of auditing and does it specify the subsequent actions by the auditing body?		
5.6.2.	Does the auditing body suspend auditing in cases when for example: • The customer's audited management system has persistently or seriously failed to meet auditing requirements including requirements for the effectiveness of the management system? • The audited client does not allow surveillance or re-auditing audits to be conducted at the required frequencies? or • The audited client has voluntarily requested a suspension?		
5.6.3.	Under suspension the customer's management system auditing is temporarily invalid. Does the auditing body have enforceable arrangements with its clients to ensure that in case of suspension the client refrains from further promotion of its auditing? Does the auditing body make the suspended status of the auditing publicly available and take any other measures it deems appropriate?		
5.6.4.	Does failure to resolve the issues that have resulted in the suspension in a time established by auditing body result in withdrawal or reduction of the scope of auditing?		
5.6.5.	Does the auditing body reduce the customer's scope of auditing to exclude the parts not meeting the requirements when the client has persistently or seriously failed to meet the auditing requirements for those parts of the scope of auditing?		
5.6.6.	Does the auditing body have enforceable arrangements with the audited customer concerning conditions of withdrawal ensuring upon notice of withdrawal of auditing that the customer discontinues its use of all advertising matter that contains any reference to a audited status?		
5.7.	**Appeals**		
5.7.1.	Does the auditing body have a documented process to receive, evaluate and make decisions on appeals?		
5.7.2.	Is a description of the appeals handling process publicly available?		
5.7.3.	Is the auditing body responsible for all decisions at all levels of the appeals handling process? Does the auditing body ensure that the persons engaged in appeals handling process are different from those who carried out the audits and made the auditing decisions?		
5.7.4.	Do submission, investigation and decision on appeals result in any discriminatory actions against the appellant?		
5.7.5.	Does the appeal handling process include at least the following elements and methods: a) an outline of the process for receiving, validating, investigating the appeal and for deciding what actions are to be taken in response to it, taking into account the results of previous similar appeals;		

	b) tracking and recording appeals including actions undertaken to resolve them; c) ensuring that any appropriate correction and corrective action is taken.		
5.7.6.	Does the auditing body acknowledge receipt of the appeal and provide the appellant with progress reports and the outcome?		
5.7.7.	Are the decision to be communicated to the appellant made by, or reviewed and approved by, individual(s) not previously involved in the subject of the appeal?		
5.7.8.	Does the auditing body give formal notice of the end of the appeal handling process to the appellant?		
5.8.	**Complaints**		
5.8.1.	Is a description of the complaints handling process publicly accessible?		
5.8.2.	Upon receipt of a complaint does the auditing body confirm whether the complaint relates to auditing activities that is responsible for and, if so, deals with? If the complaint relates to a audited client does the examination of the complaint, consider the effectiveness of the audited management system?		
5.8.3.	Is a complaint about a audited client also referred by the auditing body to the audited client in question at an appropriate time?		
5.8.4.	Does the auditing body have a documented process to receive, evaluate and make decisions on complaints? Is this process subject to requirements for confidentiality as it relates to the complainant and to the subject of the complaint?		
5.8.5.	Does the complaints handling process include at least the following elements and methods : a) an outline of the process for receiving, validating, investigating the complaint and for deciding what actions are to be taken in response to it? b) tracking and recording complaints including actions undertaken to resolve them? c) Ensuring that an appropriate correction and corrective actions are taken?		
5.8.6.	Is the auditing body receiving the complaint responsible for gathering and verifying all necessary information to validate the complaint?		
5.8.7.	Whenever possible does the auditing body acknowledge receipt of the complaint and provide the complainant with progress reports and the outcome?		
5.8.8.	Is the decision to be communicated to the complainant made by, or reviewed and approved by, individual(s) not previously involved in the subject of the complaint?		
5.8.9.	Whenever possible does the auditing body give formal notice of the end of the complaint handling process to the complainant?		

5.8.10.	Does the auditing body determine together with the client and the complainant whether and, if so to what extent, the subject of the complaint and its resolution shall be made public?		
5.9.	**Records of applicants and clients**		
5.9.1.	Does the auditing body maintain records on the audit and other auditing activity for all clients including all organizations that submitted applications and all organizations audited, audited or with auditing withdrawn?		
5.9.2.	Do the records on audited clients include the following: a) Application information and initial, surveillance and re-auditing audit reports? b) Auditing agreement? c) justification of the methodology used for sampling? d) Justification for auditor time determination? e) Verification of correction and corrective actions? f) records of complaints and appeals and any subsequent correction and corrective actions? g) committee deliberations and decisions, if applicable? h) Documentation of the auditing decisions? i) Auditing documents including the scope of auditing with respect to product, process or services as applicable? j) Related records necessary to establish the credibility of the auditing such as evidence of the competence of auditor and technical expert?		
5.9.3.	Does the auditing body keep the records on applicants and customers secure to ensure that the information is kept confidential? Are records transported, transmitted or transferred in a way that ensures that confidentiality is maintained?		
5.9.4.	Does the auditing body have a documented policy and documented procedures on retention of records? Are records retained for the duration of the current cycle plus one (1) full auditing cycle?		

PART III

Auditor qualification and experience

a) Auditor should have a background of graduation in computer science/IT or equivalent subject with 10 yrs experience in IT and 1yr in Security Auditing (covering at least 2 audits) and for Lead Assessor Cloud Auditing (at least 1 Audit in last 1 year) .

b) Auditor should be well versed with principles of Cloud Computing, Differences between traditional Data Centers and Cloud Data Centers, Reference Architecture, Organization and Functions (Layers, interfaces; VMs, Middleware, Containers, Cloud O/S, Storage, Network); Services; Cloud enablement of applications; Migration; Vulnerabilities, Testing etc.

c) Auditor should be well versed with applicable ISO and NIST standards.

1. NIST SP 800-145: The NIST Definition of Cloud Computing

2. ISO/ IEC 20000-1: 2011 Information technology -- Service management -- Part 1: Service management system requirements

3. ISO / IEC 20000-9: 2015 Information technology — Service management — Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services

4. ISO 19086: Information technology -- Cloud computing -- Service level agreement (SLA) framework and technology -- Part 4: Security and privacy

5. ISO 27001: 2013 - Information technology -- Security techniques -- Information security management systems – Requirements

6. ISO 27017: 2015 - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services

7. ISO 27018: Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

8. ISO 9001: 2015 - Quality Management Systems – Requirements

d) Auditor should be qualified auditor as per the requirements of ISO 27001 & ISO 20000-1

e) Auditor should be well versed with the STQC certification scheme of empanelment of cloud service providers with focus on the following documents-

- Cloud Service Providers:-Audit Criteria (CSP-01-03), Issue-1
- Cloud Service Providers:- Audit Reports(CSP-01-07), Issue-1