ISACA Guidelines , RBI SAR, IS Audit Observations , RFP
(Module - 5 : DISSA Course)

Arijit Chakraborty
March 13 , 2022

IS Audit Report – ISACA

- **Scope of the Audit Engagement**
- **Source of Management's Representation**
- **Objectives of the Audit**
- **Source of the Criteria-** e.g., contracts, SLAs, policies, standards
- **Findings, Conclusions and Recommendations**
- good practice to allocate a rating to indicate the significance of each finding
- **An Expression of Opinion**

Types of IS Audit Opinion

- **1. Unqualified opinion—**
- **Notes no exceptions or** none of the exceptions noted aggregate to a significant deficiency.
- Essentially a clean bill of health with respect to the audit objectives.
- 2. **Qualified opinion—Notes exceptions aggregated** to a significant deficiency (but not a material weakness).
- In this instance, the report should include an explanatory paragraph stating reasons why a qualified opinion is expressed in the report.
- **3. Adverse opinion—Notes one or more significant** deficiencies aggregating to a material weakness.
- From an internal control perspective, an adverse opinion is expressed when adequate controls are not in place or in effect to provide reasonable assurance that control objectives are met, or that there is a reasonable likelihood that the control objectives are not met
- **4. Disclaimer of opinion** = *issued when the auditor is unable to obtain sufficient appropriate audit evidence on which to base an opinion or if it is impossible to form an opinion due to the potential interactions of multiple uncertainties and their possible cumulative impact.*
- Use of judgment
- Material but not pervasive – qualified
- Material & pervasive – adverse

Sample ISA Report = Executive Summary Auditor General's overview

- **A. Cyber-Attacks**
- *In the context of intensifying cyber attacks on all sectors, this report contains a number of important findings and recommendations resulting from our general computer controls audits and capability maturity assessments.*
- *All public sector entities should consider how they can apply the recommendations and case studies in the report to their operations with the expectation of an increasingly demanding threat environment into the future.*
- **B. Controls performance**
- *While entities improved their controls in 4 categories and remained constant in 1, information security continues to be an area of significant weakness.*
- *It is disappointing to see only 50% of entities met our benchmark in this area, a drop of 7% from last year.*
- *Poor information security controls leave entity systems and information vulnerable to misuse and may impact critical services provided to the public.*

- **C. COVID specific IS Risks**
- *The report also includes a summary of common issues related to remote access. During the COVID-19 response periods, entities supported their workforces with flexible working from home arrangements.*
- *This transformation also brought security challenges as entities changed the way they operate, in some cases significantly.*
- **D. WFH – Remote working**
- *Remote work is stated to become more prevalent and entities may continue to operate with a mix of remote and on-site workforces. Entities should consider these findings and ensure that adequate policies, strong access controls and monitoring are in place to address the inherent risks associated with remote working arrangements. This will require them to develop plans and implement controls to manage a range of hybrid environment risks*
- **E. Changes in Audit Standards**
- *Upcoming changes to the Auditing Standards clarify and enhance the need for auditors to understand general computer controls and their impact on the financial report. In particular, auditors are required to assess controls for each aspect of the IT environment including the network, operating system, database and application layers.*

IS Audit Approach

- *The model we have developed for our audits is based on accepted industry good practice.*
- *Our assessment is also influenced by various factors including the:*
- • *business objectives of the entity*
- *• level of entity dependence on IT*
- *• technological sophistication of entity computer systems*
- *• value of information managed by the entity*
- *For our capability assessments, entities improved their controls in 4 of the 6 audited categories. However, we continue to find a large number of weaknesses that could compromise the confidentiality, integrity and availability of information systems.*
- *Information security remains our biggest area of concern with only 50% of entities meeting our benchmark in this category, a drop of 7% from last year.*

Business continuity- IS Auditor comments

- *The percentage of entities that met our benchmark for this category in 2019-20 was the highest since we started benchmarking 13 years ago. This may, in part, be attributable to the need for entities to respond to COVID-19 pandemic. However, we found many still do not have adequate business continuity and disaster recovery arrangements in place.*
- *Interruptions to business can have serious impacts on the critical services entities deliver to the public. To ensure business continuity, entities should have an up-to-date BCP, DRP and incident response plan (IRP). The BCP defines and prioritises business critical operations and therefore determines the resourcing and focus areas of the DRP. The IRP needs to consider potential incidents and detail the immediate steps to ensure a timely, appropriate and effective response.*
- *Entities should test these plans on a periodic basis. Such planning and testing helps entities assess and improve their processes to recover information systems in the event of an unplanned disruption to business operations and services. Senior executives should monitor that plans are developed and tested in accordance with the risk profile and appetite of the entity*

IT operations

- *There has been steady improvement in the IT operations category since we added it to our assessment criteria in 2011. This year, entities continued to improve with 82% reaching our benchmark.*
- *Effective management of IT operations is key to maintaining data integrity and ensuring that IT infrastructure can resist and recover from errors and failures. We assessed whether entities had adequately defined their requirements for IT service levels and allocated sufficient resources to meet these requirements. We also tested whether service and support levels within entities were adequate and met good practice.*
- *Other tests included if:*
- *• policies and plans were implemented and working effectively*
- *• repeatable functions were formally defined, standardised, documented and communicated*
- *effective preventative and monitoring controls and processes had been implemented to ensure data integrity*

Common Control weaknesses

- *Without appropriate IT risk policies and practices, entities may not identify and mitigate threats within reasonable timeframes.*
- *Entities may not meet their business objectives when risks are not identified and appropriately managed.*
- ***Change control***
- *Entities' change control practices continue to improve with 85% meeting our benchmark in 2019-20.*
- *We examined if system changes are appropriately authorised, implemented, recorded and tested.*
- *We reviewed any new applications acquired or developed to evaluate if the changes were made in line with management's intentions*
- *An overarching change control framework is essential to ensuring changes are made consistently, reliably and efficiently. When examining change control, we expect entities to be following their approved change management procedures*

RBI : Compliance of System Audit Report (SAR)

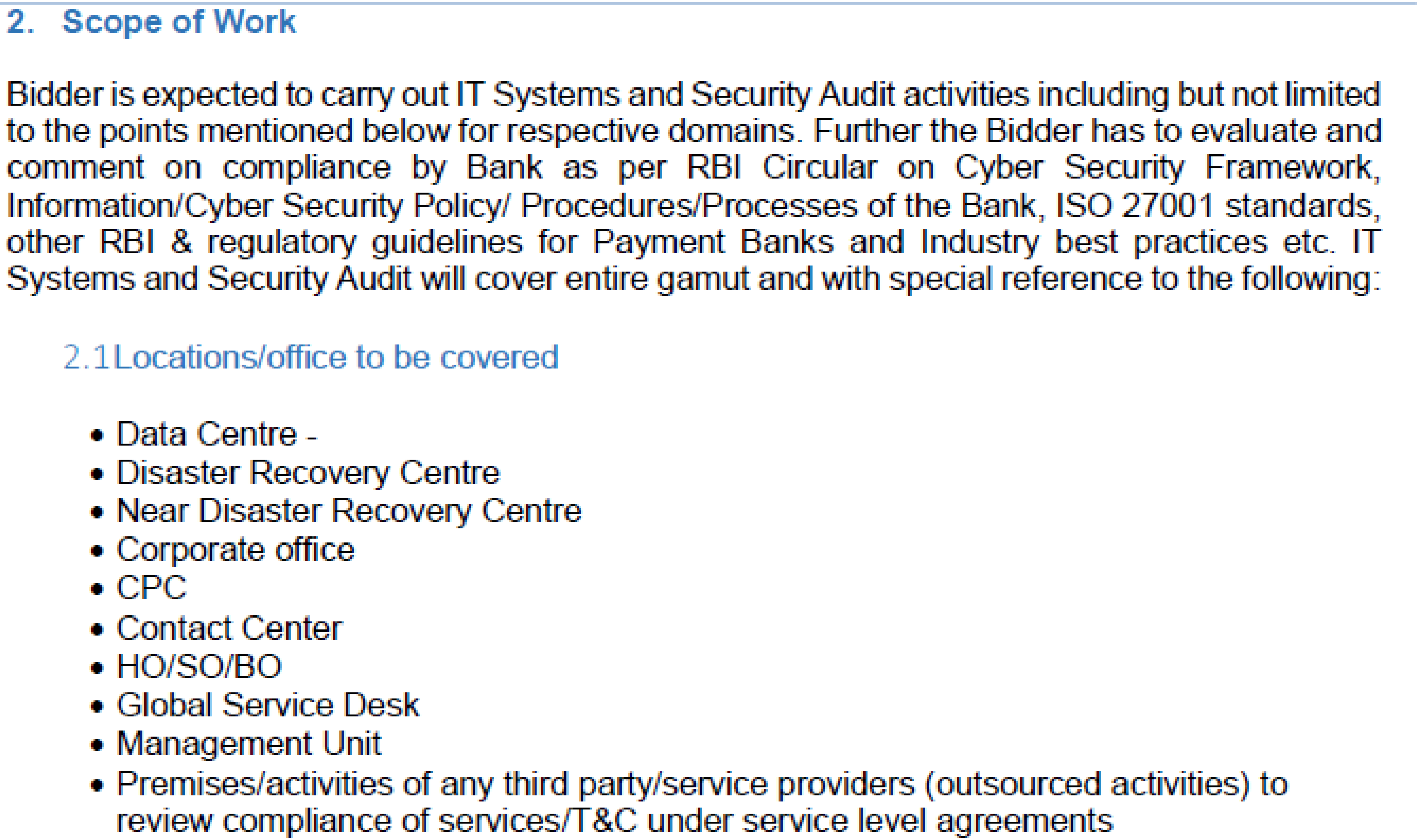
- RBI : most banks yet to submit **system audit reports** certifying compliance with data store rules **even after 3 years of issuing circulars.**
- RBI : stated many foreign banks contesting : audit rules **do not apply to them** ‘’this was not acceptable’’.
- RBI : banks to submit compliance with plan by May 15, 2021.
- ‘’On soil’’ data storage

- **RBI : Data Localisation**
- several foreign banks unable to issue audit report stating : all personal & non personal data sent overseas for processing **has been deleted.**
- RBI barred **AmEx Bank & Diners Club** from adding new customers due to data storage rule violation.
- RBI’s “on soil” data storage norms

SAR requirement

- Banks required to provide a **System Audit Report** certifying compliance with RBI Rules
- **Systems Audit** : by auditors empanelled with CERT-In (Ministry of Electronics & IT)
- **Auditors :**
- Analyse all storage locations
- Ensure data deleted from offshore servers

Scope of IS Audit



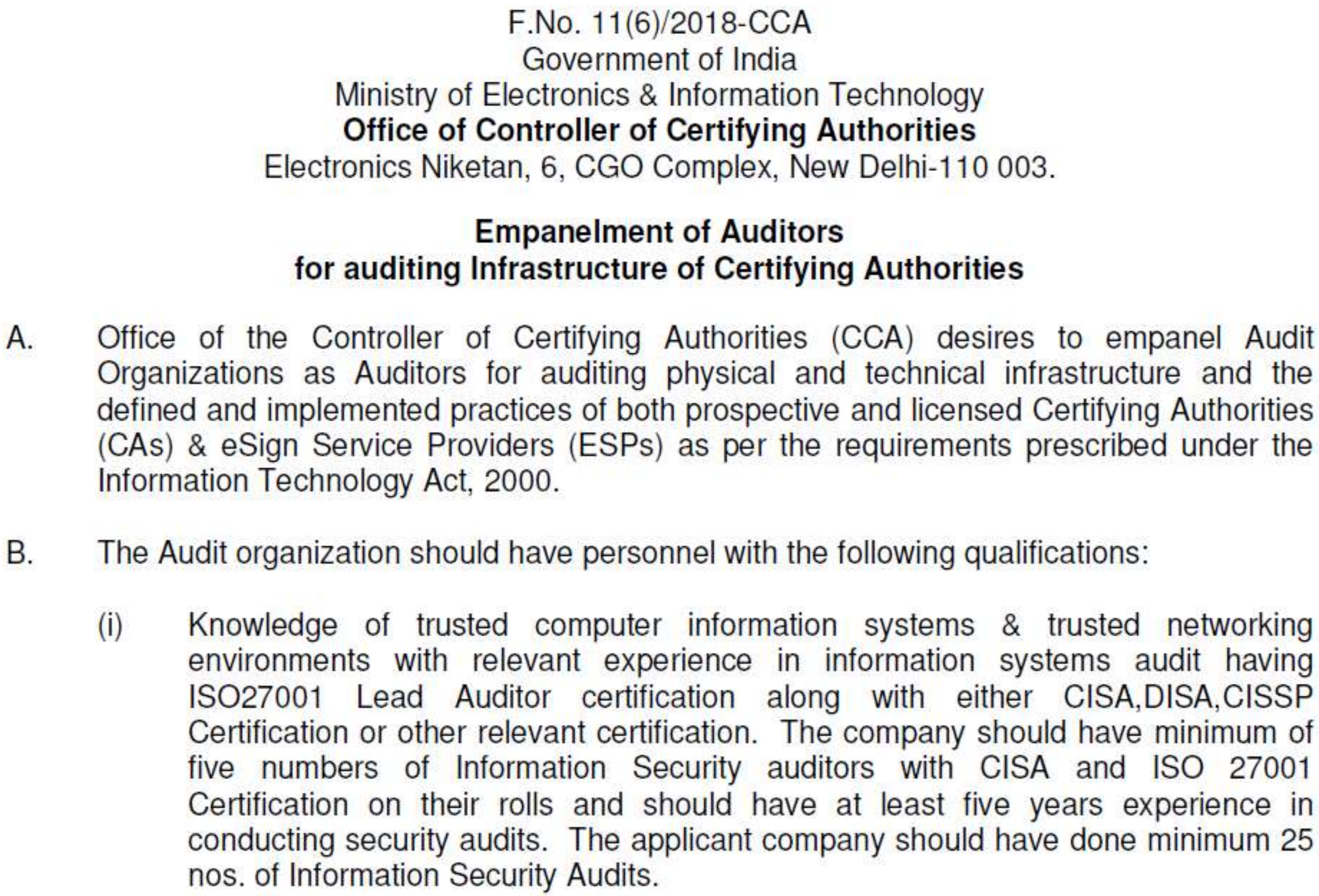
2. Scope of Work

Bidder is expected to carry out IT Systems and Security Audit activities including but not limited to the points mentioned below for respective domains. Further the Bidder has to evaluate and comment on compliance by Bank as per RBI Circular on Cyber Security Framework, Information/Cyber Security Policy/ Procedures/Processes of the Bank, ISO 27001 standards, other RBI & regulatory guidelines for Payment Banks and Industry best practices etc. IT Systems and Security Audit will cover entire gamut and with special reference to the following:

2.1Locations/office to be covered

- Data Centre -
- Disaster Recovery Centre
- Near Disaster Recovery Centre
- Corporate office
- CPC
- Contact Center
- HO/SO/BO
- Global Service Desk
- Management Unit
- Premises/activities of any third party/service providers (outsourced activities) to review compliance of services/T&C under service level agreements

Ministry of Electronics & IT



F.No. 11(6)/2018-CCA
Government of India
Ministry of Electronics & Information Technology
Office of Controller of Certifying Authorities
Electronics Niketan, 6, CGO Complex, New Delhi-110 003.

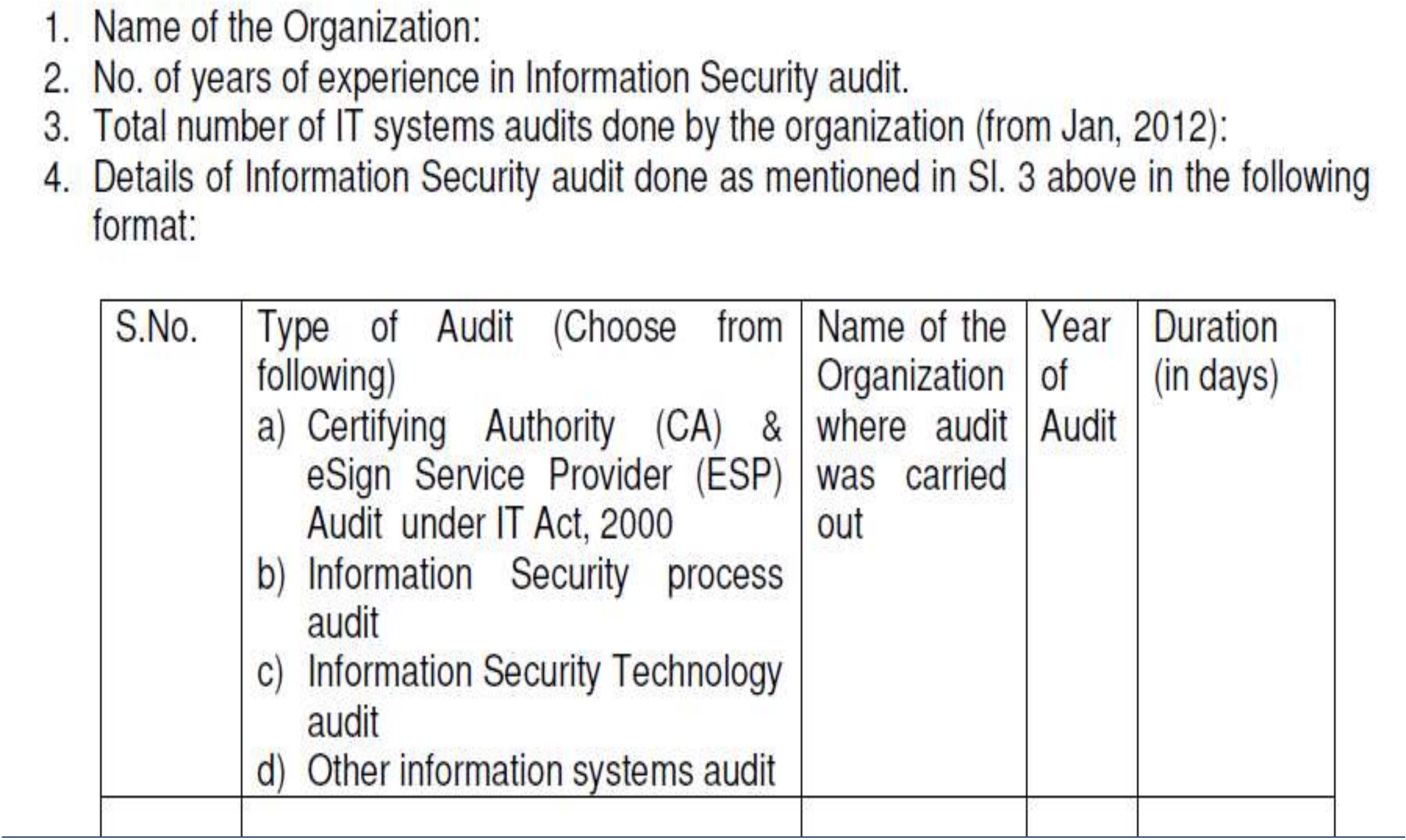
Empanelment of Auditors
for auditing Infrastructure of Certifying Authorities

A. Office of the Controller of Certifying Authorities (CCA) desires to empanel Audit Organizations as Auditors for auditing physical and technical infrastructure and the defined and implemented practices of both prospective and licensed Certifying Authorities (CAs) & eSign Service Providers (ESPs) as per the requirements prescribed under the Information Technology Act, 2000.

B. The Audit organization should have personnel with the following qualifications:

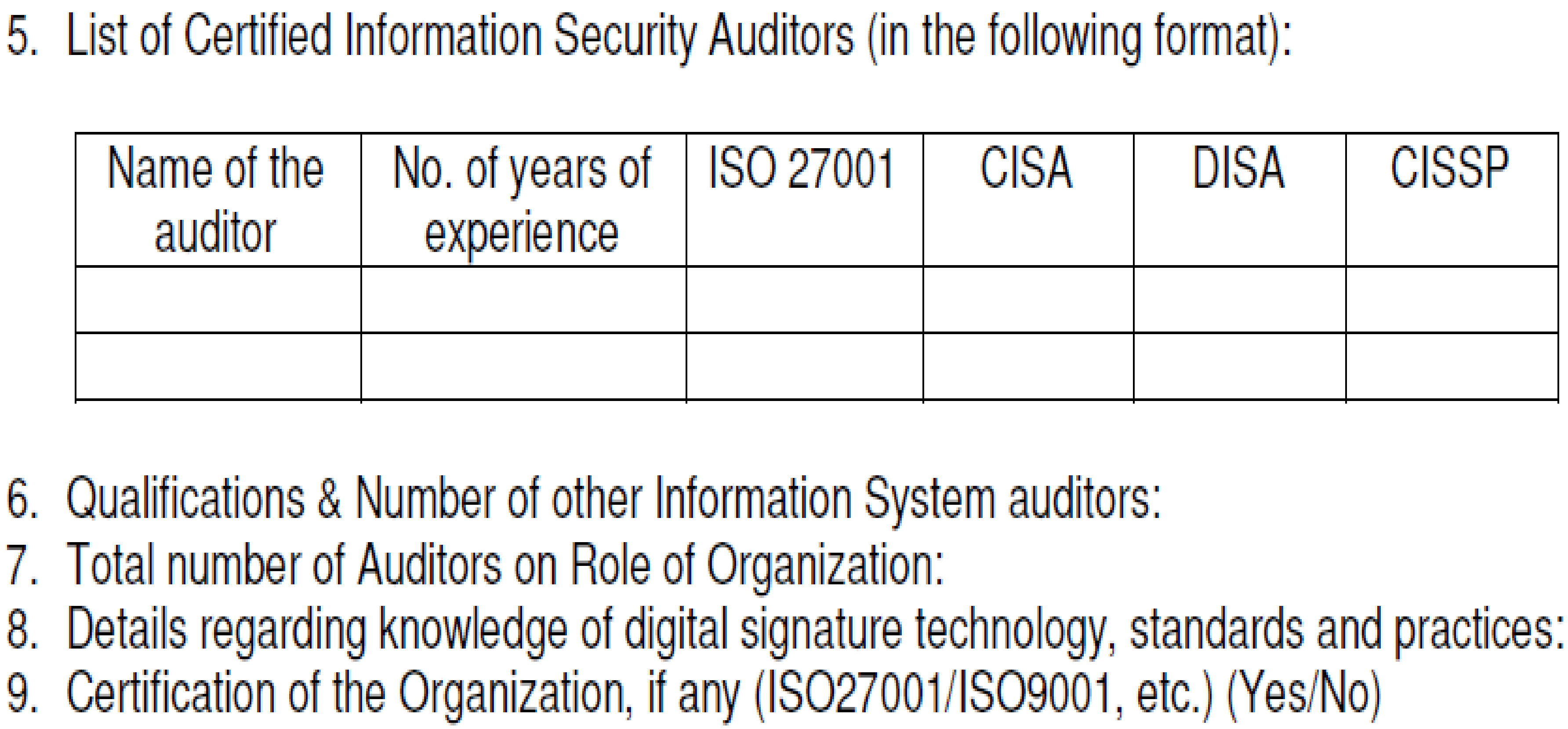
(i) Knowledge of trusted computer information systems & trusted networking environments with relevant experience in information systems audit having ISO27001 Lead Auditor certification along with either CISA,DISA,CISSP Certification or other relevant certification. The company should have minimum of five numbers of Information Security auditors with CISA and ISO 27001 Certification on their rolls and should have at least five years experience in conducting security audits. The applicant company should have done minimum 25 nos. of Information Security Audits.

Application format



1. Name of the Organization:
2. No. of years of experience in Information Security audit.
3. Total number of IT systems audits done by the organization (from Jan, 2012):
4. Details of Information Security audit done as mentioned in Sl. 3 above in the following format:

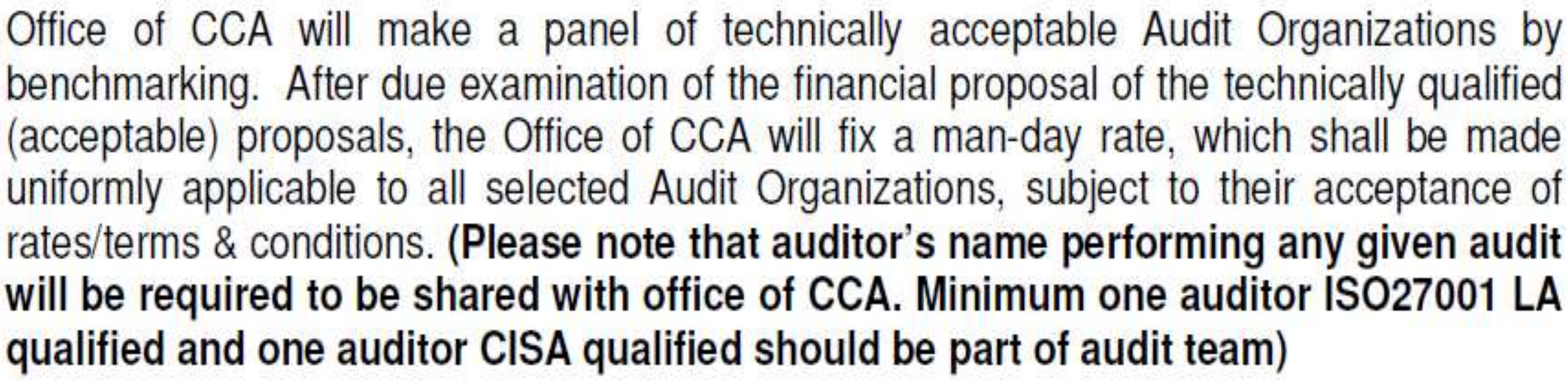
S.No.	Type of Audit (Choose from following) a) Certifying Authority (CA) & eSign Service Provider (ESP) Audit under IT Act, 2000 b) Information Security process audit c) Information Security Technology audit d) Other information systems audit	Name of the Organization where audit was carried out	Year of Audit	Duration (in days)



5. List of Certified Information Security Auditors (in the following format):

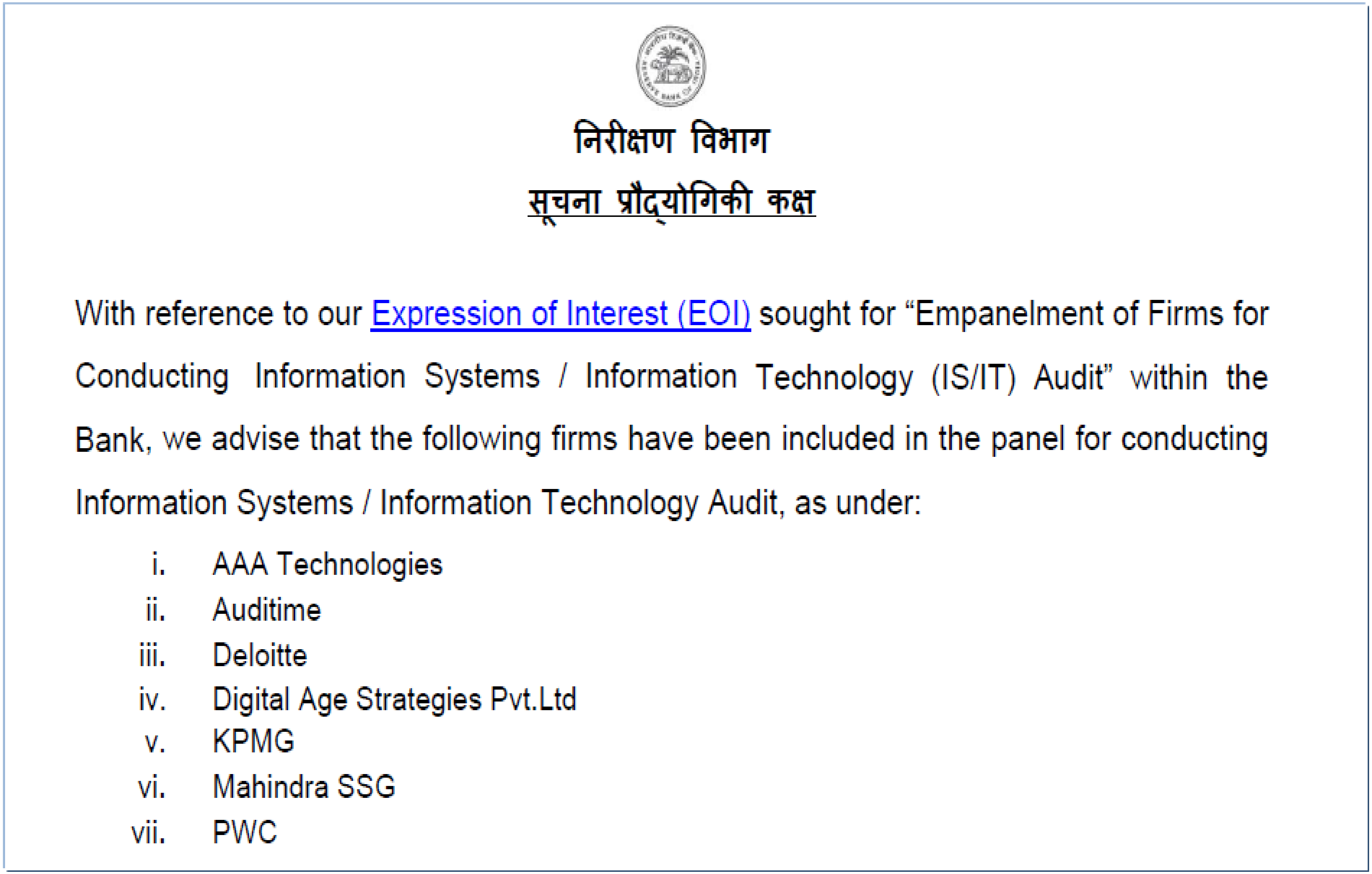
Name of the auditor	No. of years of experience	ISO 27001	CISA	DISA	CISSP

6. Qualifications & Number of other Information System auditors:
7. Total number of Auditors on Role of Organization:
8. Details regarding knowledge of digital signature technology, standards and practices:
9. Certification of the Organization, if any (ISO27001/ISO9001, etc.) (Yes/No)



Office of CCA will make a panel of technically acceptable Audit Organizations by benchmarking. After due examination of the financial proposal of the technically qualified (acceptable) proposals, the Office of CCA will fix a man-day rate, which shall be made uniformly applicable to all selected Audit Organizations, subject to their acceptance of rates/terms & conditions. **(Please note that auditor's name performing any given audit will be required to be shared with office of CCA. Minimum one auditor ISO27001 LA qualified and one auditor CISA qualified should be part of audit team)**

RBI IS Audit



निरीक्षण विभाग

सूचना प्रौद्योगिकी कक्ष

With reference to our Expression of Interest (EOI) sought for “Empanelment of Firms for Conducting Information Systems / Information Technology (IS/IT) Audit” within the Bank, we advise that the following firms have been included in the panel for conducting Information Systems / Information Technology Audit, as under:

i. AAA Technologies
ii. Auditime
iii. Deloitte
iv. Digital Age Strategies Pvt.Ltd
v. KPMG
vi. Mahindra SSG
vii. PWC

Terms and conditions

1. *The panel will remain valid for a **period of 3 years**, in normal course, subject to the condition that the firms/individuals continue to be on the panel of approved auditors released by CERT-In.*
2. *The broad scope of work would be on similar lines as that indicated in CERT-In empanelment and may, inter alia, include the following:- **conduct of VA&PT, security assessments/reviews of - application, network, operating systems, databases, source code, SDLC** etc.*
3. *3. Any firm/company empanelled with the Bank in this process shall cease to exist in Bank's panel of external IS Auditors, if the firm's/ company's CERT-In empanelment is revoked and/ or if the firm/company **is blacklisted by any Government Agency/ Public Sector Undertaking/ Scheduled Commercial** Bank in India any time during the period of validity of the Bank's panel.*

- *4. For the purposes of computation of man-days, the following definition will apply: "Auditing Man-day" shall mean IT Security auditing effort (both on-site as well as off-site)* ***of minimum 8 hours, excluding breaks****, by a person with suitable* ***IT Security auditing related qualification such as CISSP, ISO 27001 Lead Assessor, CISM, CISA, CEH etc.***
- *5. Bank reserves the right to limit the number of audits that can be concurrently executed by a firm for the Bank.*
- *6. The empanelled firms shall be required to enter into a contract with the Bank before undertaking any assignment.*