IS Audit approach , Applicable Standards
(Module -1 : DISSA Course)

Arijit Chakraborty
09.01.2022

Goal of IS Audit - ISACA

- to Assist the organization’s IT managers to effectively fulfil their responsibilities to achieve the Organization’s IT Management Goals.
- The Organization’s IT Management Objectives **are to ensure:**

✓ that Organization’s IT strategy fully reflects Organization’s Business Strategic Objectives,

✓ Improve Reliability, Stability, Security, and Data Processing Integrity and

✓ Accuracy of Information System on which the Organization Depends, and

✓ Improve Effectiveness and Efficiency of the IS Operation & ensure that the Operation of IS Complies with requirements of Laws, Regulations, & Compliance.

ISACA Audit Standards , Guidelines & Code of Ethics

- Such standards will require to be internationally accepted standards only.
- This will ensure = IS auditor performs auditing, conforming to minimum level of acceptable performance & meeting required professional responsibilities.
- Standards = define mandatory requirements
- Guidance / Guidelines = guidance , IG, AG
- Tools & Techniques = illustrate how to meet the Standards

ISACA Audit Standards

- General
- Performance & fieldwork
- Reporting

CISA® Certified Information Systems Auditor®
An ISACA® Certification

Standards - Category

- **General standards (1000 series)—** guiding principles under which the IS assurance profession operates.
- Apply to conduct of all assignments & deal with IS audit and assurance professional's ethics, independence, objectivity and due care as well as knowledge, competency and skill.
- • **Performance standards (1200 series)—**Deal with conduct of the assignment, such as planning and supervision, scoping, risk and materiality, resource mobilization, supervision and assignment management, audit and assurance evidence, and exercising of professional judgment and due care.
- • **Reporting standards (1400 series)—**Address types of reports, means of communication & information communicated.

ISACA Standards

- IS audit & assurance standards define mandatory requirements for IS auditing.
- They report and inform:
- • IS audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
- • Management and other interested parties of the profession’s expectations concerning the work of practitioners
- • Holders of the Certified Information Systems Auditor® (CISA®) designation of requirements.
- Failure to comply with these standards may result in an investigation into the CISA holder’s conduct by the ISACA Board of Directors or appropriate committee and, ultimately, in disciplinary action.

ISACA Code of Ethics

- **Members and ISACA certification holders shall:**

1. Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise IS and technology, including: audit, control, security and risk management.
2. Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.
3. Serve in the interest of stakeholders in a lawful manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.
4. Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information **shall not be used for personal benefit** or released to inappropriate parties.

5. Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.
6. Inform appropriate parties of the results of work performed including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.
7. Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise IS and technology, including: audit, control, security and risk management.

- *Failure to comply with this Code of Professional Ethics* ***can result in an investigation into a member's or certification holder's conduct and, ultimately, in disciplinary measures.***

COBIT

- Developed by ISACA
- A comprehensive framework that assist enterprises in achieving their objectives for the governance and management of enterprise IT (GEIT)
- COBIT 5 based on *5 principles and 7 enablers*

COBIT

5 Principles	7 Enablers
1. Meeting Shareholders needs	1. Principles, Policies and Frameworks
2. End-to-End coverage	2. Processes
3. Holistic Approach	3. Organizational Structures
4. Integrated Framework	4. Culture, Ethics and Behaviour
5. Separate governance from management	5. Information
	6. Services, Infrastructure and Applications
	7. People, Skills and Competencies

IS Audit Planning

- Similar to ISA 300, 315
- Risk assessment
- H. M, L
- Accordingly Audit plan to be prepared

Plan steps

- Setting audit scope is critical, because "the IS auditor will need to understand the IT environment and its components to identify the resources that will be required to conduct a comprehensive evaluation."
- A clear scope helps the auditor determine the testing points relevant to the audit's objective.
- **Pre-audit planning includes** : conducting

✓ risk assessment,

✓ identifying regulatory compliance requirements

✓ determining the resources needed to perform the audit.

- The final planning step—determining audit procedures and steps for data gathering—involves

✓ obtaining departmental policies for review,

✓ developing methodology to test and verify controls

✓ developing test scripts plus criteria to evaluate the test.

- Once planning is complete, auditors can move on to the fieldwork and documentation phase (acquiring data, testing controls, issue discovery and validation, documenting results) and the reporting phase (gathering report requirements, drafting the report, issuing the report and follow-up)
- “Creating Audit Programs” indicates 3 key success elements:
- IS auditors should be familiar with :
- 1. standard frameworks,
- 2. operating environment of the entity under review and
- 3. audit process used internally.

8 Business Knowledge Areas

1. How is the enterprise *organized*?
2. How is the enterprise *governed*?
3. Under what *laws/regulations* does the enterprise operate?
4. What are the enterprise's *business processes*?
5. How does the enterprise *operate*?
6. How does the enterprise use *technology*?
7. How does the enterprise *finance* itself?
8. How does the enterprise *measure business success*?

Knowledge of IS Auditor

- The IS auditor should also understand how basic business accounting results in 3 types of reports:
- **Financial reporting**—Allows the enterprise to comply with statutory reporting requirements, such as quarterly and annual filings with stock exchanges
- **Regulatory reporting**—Such as to taxation authorities, utility regulators, or insurance and financial regulators, allows the enterprise to demonstrate compliance with specific requirements
- **Operational reporting**—Provides senior management, supervisors and line managers with information to control business processes, as well as to report various operational information to senior and executive management

IS Controls

- **Internal Control Components**

1. **The control environment**. It is the overall environment and tone of the organization regarding controls. Attitude of the senior management and their awareness about internal controls matters a lot.
2. **Risk assessment**. Good internal controls can only be designed after the entity has performed risk assessment and identified risk areas that require controls.
3. **Information system**. With the ever increasing dependence on information technology, it is logical that IS systems form critical components of internal controls.
4. **Control Activities**. These are the actual controls that are introduced to manage risks.
5. **Monitoring of controls**. Designing of controls is not enough. How effectively the organization monitors the implantation and effectiveness of controls determine the success of an internal control environment.

Factors which influence audit risk

1. **Inherent risk** – Risk that an activity would pose if no controls/ other mitigating factors were in place.
2. **Control risk** – Risk that a material error exists that would not be prevented or detected on a timely basis by the system of internal controls
3. **Detection risk** – The risk that material errors or misstatements that have occurred will not be detected by the IS auditor
4. **Residual risk** – Risk that remains after controls are taken into account

Risk Treatment

- Risk identified in risk assessment needs to be treated.
- **Possible risk response options include:**

1. **Risk mitigation**—Applying appropriate controls to reduce the risk
2. **Risk acceptance**—Knowingly and objectively not taking action, providing the risk clearly satisfies the organization’s policy and criteria for risk acceptance
3. **Risk avoidance**—Avoiding risk by not allowing actions that would cause the risk to occur
4. **Risk transfer/sharing**—Transferring the associated risk to other parties (e.g., insurers or suppliers)

- **Compliance testing –** determines whether controls are in compliance with management policies and procedures

- **Substantive testing –** gathers evidences to evaluate the integrity of individual transactions, data or other information

Effect of L&R on IS Audit plan

- ISA 250
- Country specific guidelines
- IT Act
- ISO
- Regulator enforced standards, practices, SOP

ISA 620 : Using the Work of Other Experts

- The IS auditor should, where appropriate, consider using the work of other experts for the audit.
- IS auditor should assess and be satisfied with the professional qualifications, competencies, relevant experience, resources, independence and quality control processes of other experts, prior to engagement.
- IS auditor should assess, review & evaluate the work of other experts as part of the audit and conclude the extent of use and reliance on expert's work.
- The IS auditor should determine and conclude whether the work of other experts is adequate and complete to enable the IS auditor to conclude on the current audit objectives. Such conclusion should be clearly documented

IS auditor should apply additional test procedures to gain sufficient and appropriate audit evidence in circumstances where the work of other experts does not provide sufficient and appropriate audit evidence.

- IS auditor should provide appropriate audit opinion & include scope limitation where required evidence is not obtained through additional test procedures.

- The IS auditor should have access to all work papers, supporting documentation and reports of other experts, where such access does not create legal issues. Where the expert’s access to records creates legal issues and hence such access is not available, the IS auditor should appropriately determine and conclude the extent of use and reliance on the expert’s work
- The IS auditor's views/relevance/comments on adoptability of the expert's report should form a part of the IS auditor's report.
- The IS auditor should refer to IS Auditing Standard -Performance of Audit Work that states the IS auditor should obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives.
- If the IS auditor does not have the required skills or other competencies to perform the audit, the IS auditor should seek competent assistance from other experts; however, the IS auditor should have good knowledge of the work performed but not be expected to have a knowledge level equivalent to the expert

Compliance & Substantive Testing-Point to Remember: DISSA

- (1) compliance testing will be performed first. Substantive testing will be the next step
- (compliance testing test controls, while substantive testing tests details
- (3) compliance testing checks for the presence of controls whereas substantive testing checks the integrity of contents i.e. test of individual transactions
- (4 outcome/result of compliance testing will form the basis for planning of substantive testing.
- For example, if compliance testing indicates strong internal control, substantive testing may be waived off or reduced.
- In case compliance testing indicates weak internal controls then substantive testing to be more rigorous.
- The development of substantive tests is often dependent on the outcome of compliance tests

Closure meeting

- Generally accepted audit practice requires reporting of finding even if corrective action is taken by auditee before issuance of report.

- Closure meeting ensures that there have been no misunderstandings or misinterpretation of facts.

- Closing meeting helps to enhance the understanding between the auditor and the auditee in terms of what was presented, discussed, and agreed upon.

- For communication of audit results, IS auditor is ultimately responsible to senior management and the audit committee of the board of directors.

- During assignment, **if any control weakness is observed which is not in scope** of audit, it should be reported to management.

- Same should not be ignored.

Global Technology Audit Guide (IIA)

- User-friendly guide for IA to understand IT Audit & management, risk, control & security.
- **GTAG List:**

✓ Assessing Cybersecurity Risk: Roles of the Three Lines of Defense

✓ Auditing Application Controls, Management of IT Auditing

✓ Auditing IT Governance, Auditing IT Projects

✓ Auditing Smart Devices: An Internal Auditor's Guide

✓ Auditing User-developed Applications

✓ Business Continuity Management

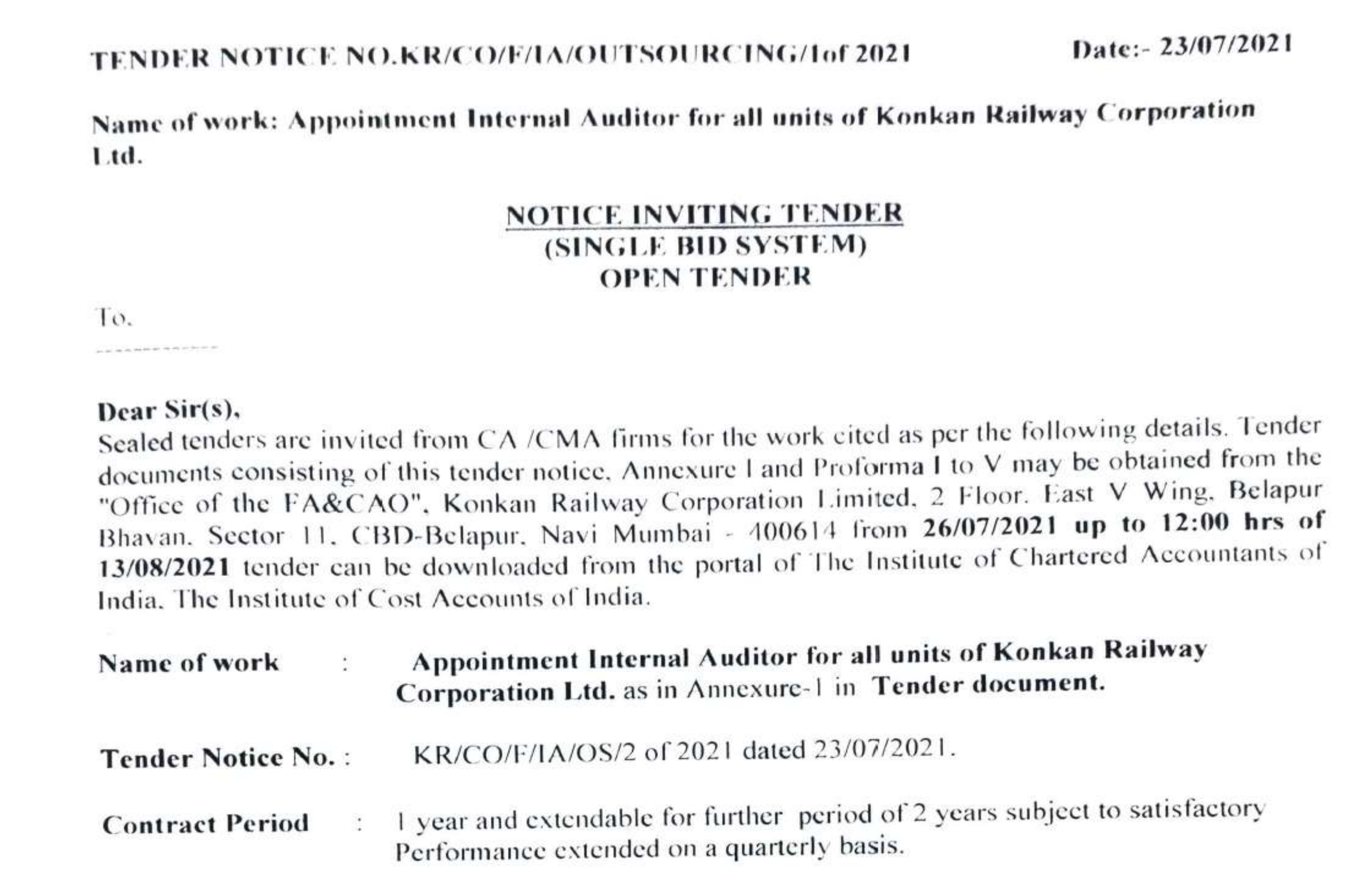
✓ Change and Patch Management Controls: Critical for Organizational Success

✓ Continuous Auditing: Coordinating Continuous Auditing and Monitoring

✓ Data Analysis Technologies

✓ Developing the IT Audit Plan

Case study :
KRCL Case : DISSA Recognition



TENDER NOTICE NO.KR/CO/F/IA/OUTSOURCING/1of 2021 **Date:- 23/07/2021**

Name of work: Appointment Internal Auditor for all units of Konkan Railway Corporation Ltd.

NOTICE INVITING TENDER
(SINGLE BID SYSTEM)
OPEN TENDER

To,

Dear Sir(s),
Sealed tenders are invited from CA /CMA firms for the work cited as per the following details. Tender documents consisting of this tender notice, Annexure I and Proforma I to V may be obtained from the "Office of the FA&CAO", Konkan Railway Corporation Limited, 2 Floor, East V Wing, Belapur Bhavan, Sector 11, CBD-Belapur, Navi Mumbai - 400614 from **26/07/2021 up to 12:00 hrs of 13/08/2021** tender can be downloaded from the portal of The Institute of Chartered Accountants of India, The Institute of Cost Accounts of India.

Name of work : **Appointment Internal Auditor for all units of Konkan Railway Corporation Ltd.** as in Annexure-I in **Tender document.**

Tender Notice No. : KR/CO/F/IA/OS/2 of 2021 dated 23/07/2021.

Contract Period : 1 year and extendable for further period of 2 years subject to satisfactory Performance extended on a quarterly basis.

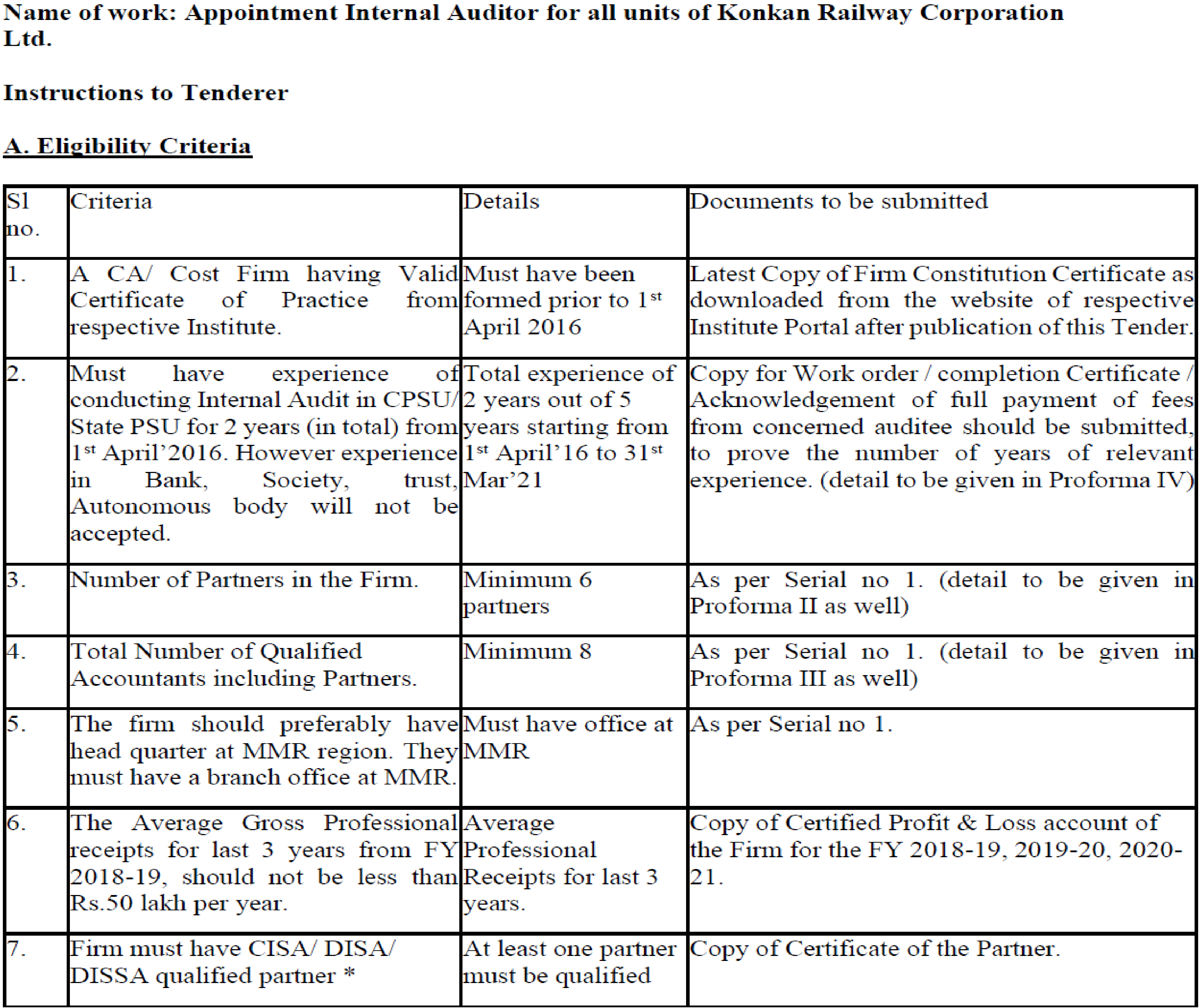
Date and Time of opening of tender : 15:30 Hrs. on 13/08/2021

Cost of tender form (Non refundable): Nil

In case, the date of opening of tender happens to be a holiday, the tender will be opened on the next working day at the same time and place. The rates should be quoted in words and figures. The corporation reserves the right to accept/reject one or all tenders without assigning any reason. Anticipating your participation in the tender.

For Konkan Railway Corporation Ltd.

(MATHEW PHILIP)
FA&CAO
Tel: 022 27587314
facao@krcl.co.in

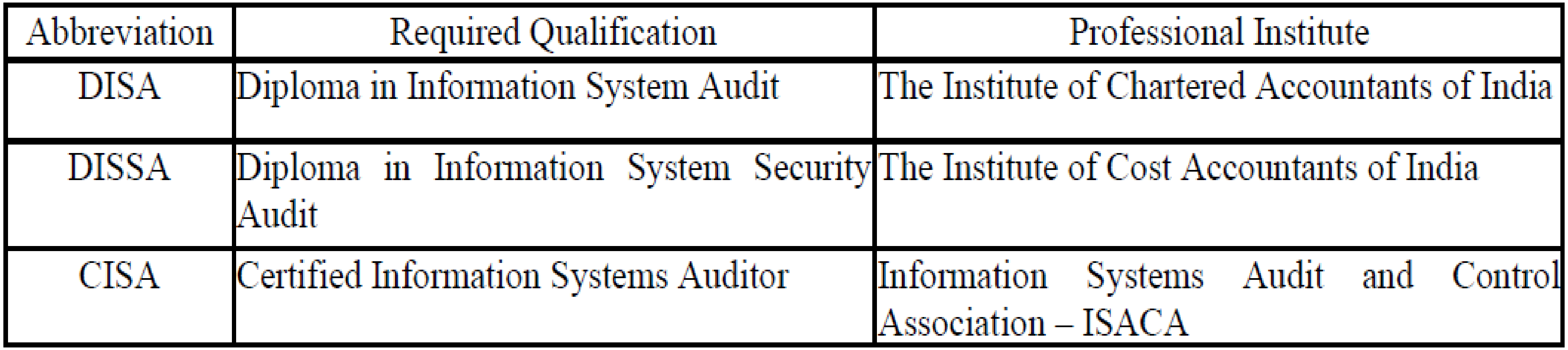


Name of work: Appointment Internal Auditor for all units of Konkan Railway Corporation Ltd.

Instructions to Tenderer

A. Eligibility Criteria

Sl no.	Criteria	Details	Documents to be submitted
1.	A CA/ Cost Firm having Valid Certificate of Practice from respective Institute.	Must have been formed prior to 1st April 2016	Latest Copy of Firm Constitution Certificate as downloaded from the website of respective Institute Portal after publication of this Tender.
2.	Must have experience of conducting Internal Audit in CPSU/ State PSU for 2 years (in total) from 1st April'2016. However experience in Bank, Society, trust, Autonomous body will not be accepted.	Total experience of 2 years out of 5 years starting from 1st April'16 to 31st Mar'21	Copy for Work order / completion Certificate / Acknowledgement of full payment of fees from concerned auditee should be submitted, to prove the number of years of relevant experience. (detail to be given in Proforma IV)
3.	Number of Partners in the Firm.	Minimum 6 partners	As per Serial no 1. (detail to be given in Proforma II as well)
4.	Total Number of Qualified Accountants including Partners.	Minimum 8	As per Serial no 1. (detail to be given in Proforma III as well)
5.	The firm should preferably have head quarter at MMR region. They must have a branch office at MMR.	Must have office at MMR	As per Serial no 1.
6.	The Average Gross Professional receipts for last 3 years from FY 2018-19, should not be less than Rs.50 lakh per year.	Average Professional Receipts for last 3 years.	Copy of Certified Profit & Loss account of the Firm for the FY 2018-19, 2019-20, 2020-21.
7.	Firm must have CISA/ DISA/ DISSA qualified partner *	At least one partner must be qualified	Copy of Certificate of the Partner.



Abbreviation	Required Qualification	Professional Institute
DISA	Diploma in Information System Audit	The Institute of Chartered Accountants of India
DISSA	Diploma in Information System Security Audit	The Institute of Cost Accountants of India
CISA	Certified Information Systems Auditor	Information Systems Audit and Control Association – ISACA

Internal Audit shall adopt a system and process, focus on methodology in conducting Audit procedure and identify deviation from system, suggest opportunity for system improvement, strengthen the process and prevent repetition of error. The auditor should evaluate or measure the existing internal control process in our ERP Software.