PREMIER FERRO ALLOYS & SECURITIES LIMITED

Information Security Audit Policy

1. Introduction

The framework and policy formulation for audit of technological risks has emanated from Reserve Bank of India's "Master Directions- Information Technology Framework for the NBFC Sector" published on June 8, 2017 and the "Standard on Internal Audit- 14, Internal Audit in an Information Technology Environment", issued by the Council of the Institute of Chartered Accountants of India, published on March, 2009.

2. Objectives

1. The purpose of the Information Security (IS) Audit is to provide an insight on the effectiveness of controls that are in place to ensure confidentiality, integrity and availability of the organization's Information Technology (IT) infrastructure. IS Audit shall identify risks and methods to mitigate risk arising out of IT infrastructure such as server architecture, local and wide area networks, physical and information security, telecommunications and such like.

2. It is essential for the Company to ensure that its systems assets/ resources and IT processes are dependable, controlled and protected from misuse at all times. As part of the confirmatory process, it would ensure that all IT systems are audited at periodic intervals and a report on their status are submitted to Audit Committee of the Board.

3. Major objectives of the IS Audit Policy:

i. **Safeguarding IS Assets / Resources and IT Processes:**

a) Monitoring effective usage of hardware, software, networking and communication facilities, people (knowledge resource), system documentation and similar components of the IT system of the Company.

b) Evaluating the adequacy of infrastructure for safeguarding IS Assets/Resources, including but not limited to that of physical security, surveillance, incident monitoring etc.

c) **Verification of Data integrity and Security:** Validate that the data entered and captured in the system is duly authorised, verified and completed and that proper control is exercised at all stages viz. data preparation, input, verification, output, modification, deletion, electronic transmission and so on to ensure authenticity and correctness of data.

PREMIER FERRO ALLOYS & SECURITIES LTD. Kolkata

d) **Evaluation of System Effectiveness and Efficiency:** Evaluate the extent to which the organisational goals, business and user needs have been met with and to determine whether resource utilisation is effective and efficient in achieving the desired objectives.

ii. **Verification of compliance:** Evaluate the level of adherence to: i) maintenance of integrity, confidentiality, reliability, availability and dependability of information resources; ii) legal, regulatory and statutory requirements; iii) internal policy and procedures based on prescribed standards and guidelines.

3. Scope

1. The scope of IS audit includes the collection and evaluation of evidence/ information to determine whether the information systems in use safeguards the assets, maintain data security/ integrity/ availability, achieve the organisational goals effectively and utilise the resources efficiently.

2. It also includes the processes for the planning and organisation of the IS's activity, the processes for monitoring of such activities and the examination of the adequacy of the organisation and management of the IS specialist staff and non-specialists with IS responsibilities to address the IS exposures of the organisation.

3. This would cover all the computerised branches/offices of the Company and includes all the activities/areas of the organisation, where IT systems are used for business purposes (implemented or to be implemented).

4. Audit Charter

The responsibility, authority and accountability of internal IS auditors shall be as per the prevailing audit guidelines and in accordance with this Policy.

5. Organizational structure

1. **IS Audit Cell-** The Company will have an exclusive cell with IS Audit function led by an IS Audit Head- Assistant General Manager (AGM), preferably a Certified Information System Auditor or with Diploma in Information System Audit (CISA/DISA), assuming responsibility and accountability of the IS Audit function, reporting to the Chief Audit Executive (CAE)/General Manager. Preferably officers with experience (say three to five years) in information technology (IT) shall be inducted into IS Audit Cell. They shall be periodically provided with necessary training (class room as well as on the job) to update/ upgrade their IT knowledge and

skills to conduct IS audit using audit tools and testing accelerators which will enable them to effectively carry out the job assigned to them.

2. **Directors to manage the complexity of IS Audit oversight-** A designated member of the ACB needs to possess the relevant knowledge of Information Systems, IS Controls and IS Audit issues. The designated member should also have relevant competencies to understand the ultimate impact of deficiencies identified in IT Internal Control framework by the IS Audit function. The BOD or ACB members should be imparted training to fill any gaps in the knowledge related to IT risks and controls.

3. **External IS Audit firms-** Wherever the Company uses external resources for conducting IS Audit in areas where the required expertise/ professional skills are lacking within the Company, the responsibility and accountability for such external IS audits shall remain with the AGM and CAE/General Manager. Depending on the nature and criticality of assignment, the Company may stipulate eligibility criteria of the External IS Audit firms, fees payable etc. The engagement letter should cover the scope of IS Audit, objectivity, duration etc. apart from addressing the areas of responsibility, authority, and accountability.

4. **Independence**
   a) Maintaining the independence of IS Audit function from other departments and offices, its personnel shall report to AGM, IS Audit Cell. AGM, IS Audit Cell will report to CAE /General Manager, who shall report to the ACB through Executive Director/ Chairman and Managing Director.
   b) ACB should devote appropriate and sufficient time to IS Audit findings identified during IS Audits and members of the ACB would need to review critical issues highlighted and provide appropriate guidance to the Company's management. Also, the BOD shall follow up for rectification of deficiencies and place periodical note to ACB on the steps initiated as risk mitigation measure.
   c) IS Audit being a specialized job, the scope and function of IS Audit Cell shall be limited to auditing of the computer based information systems and shall not include financial/ transactional audit.

5. **Responsibilities-** The primary responsibility of the IS Audit Cell is to achieve the objectives of the IS Audit as enumerated in this Policy. In brief, the functions of IS Audit is to:
   a) Identify and assess potential risks to the Company's operations;
   b) Assess the means of risk mitigation and safeguarding of IT assets;
   c) Review the adequacy of controls established, to ensure compliance with the policies, plans, procedures, and business objectives;

d) Assess the level of compliance to established procedures/ controls;

e) Assess the reliability and security of financial/ management information and the systems and operations that provide this information;

f) Assess the level of utilization of IT resources to understand their efficient and effective use for business growth.

6. **Authority**

a) The IS Audit Cell, in the course of its IS Audit activities, is authorized to have unrestricted access to all areas of the Company, including all the activities, documents, records, information, properties, personnel and such like, relevant to the performance of IS Audit function.

b) It shall require all members of staff and management to supply such information and explanations as may be needed within a reasonable period of time to IS Audit staff. Heads of branches should inform IS Audit Cell without delay of any significant incident concerning security and/ or compliance with regulations and procedures.

7. **Accountability**

a) The IS Audit Cell shall prepare annual plan for IS Audit along with Risk Based IS Audit ("RBIA") Plan, covering all the computerized environments of the Company viz. branches/ offices/ etc. The plan covering IS Audit of branches/ offices/ critical resources approved and finalized by the General Manager shall be placed for approval/ adoption by ACB. In case of need, General Manager may make modifications to the approved plan based on the exigencies and keep ACB appraised of such modifications.

b) The IS Audit Cell is responsible for deciding on the scope/ timing of IS Audits and in finalization/ implementation of IS Audit Plan.

6. IS Audit Methodology

1. The methodology adopted for IS Audit/ Computer audit includes a blend of input-output report reconciliation, interview and interaction with the concerned IT users/ IT personnel, verification of reports/ registers maintained both manually as well as in the system.

2. **Specific audit tools-** Suitable audit tools such as Computer Assisted Audit Tools (CAAT) and testing accelerators may be introduced/ used in addition to other audit techniques like "audit through the computer" and audit with the computer, so as to timely identify and plug vulnerable areas in safeguarding IT assets, by way of risk mitigation for the audit of IT resources at centralized locations and for generation of

PREMIER FERRO ALLOYS & SECURITIES LTD. Kolkata

certain special/ specific reports. Core team of IS auditors shall be thoroughly exposed to the use of CAAT and related system tools in carrying out the IS audit.

3. **Periodicity of IS Audit**- IS Audit of all branches shall be scheduled by the IS Audit Cell, as per risk profile of the branch under RBIA. The IS Audit of overseas branches shall also be carried out along with the regular inspection of the branch.

4. **Parameters to be considered while conducting IS Audit**
   a) Identify the risks that the organisation is exposed to, in the existing computerised environment and to prioritise such risks for remedial action.
   b) Whether the implementation of IT in the organisation is as per the parameters laid down in the IS policy and as duly approved by the BOD.
   c) Verify whether the information systems policies have been devised covering various information assets for the entire organisation and that the organisation's systems and procedures and laid down IS policies are adhered to.
   d) Verify whether the checks and balances prescribed by IS policy and other relevant guidelines are strictly adhered to/ complied with, towards risk mitigation through proper maintenance and prevention of abuse/misuse of IT assets and computer crimes.
   e) Verify and comment on the level of checks and balances for ensuring compliance of laid down control measures.
   f) Adhere to the established norms of ethics and professional standards to ensure quality and consistency of audit work.

5. Compliance
   a) Company's IS Audit policy generally conforms to "the Master Directions- Information Technology Framework" of RBI published on June 8, 2017. Wherever a specific mention is not made herein, details provided in RBI guidelines mentioned above, shall hold good as far as it is applicable to the environment.
   b) IS Audit cell shall monitor the compliance to various IT guidelines/ RBI/ legal/ statutory requirements by various wings of the organisation that are making use of IT assets and the Inspecting officials shall ensure that the branches/ offices using IT infrastructure are strictly adhering to the various guidelines issued by IS Audit Cell from time to time.
   c) AGM with the approval of General Manager may devise/ modify the reporting formats for IS Audit, as and when required.

PREMIER FERRO ALLOYS & SECURITIES LTD. Kolkata

7. Policy Review

1. This Policy must be reviewed by the Board of the Company or if delegated by the Board, the Audit Committee, at such intervals, as may be decided by the Board.

2. The IS Audit Cell must update and report to the Board, forthwith of any changes to be made in the process flow. Accordingly, changes must be implemented in the system by the Board or the Audit Committee as the case may be.