RISK BASED INTERNAL AUDIT POLICY

TAMILNADU URBAN FINANCE AND INFRASTRUCTURE DEVELOPMENT CORPORATION LIMITED

Policy Formulation and Implementation

Introduction

Objectives and Scope

1. The internal audit function broadly assesses and contributes to the overall improvement of the organization'sgovernance, risk management, and control processes using a systematic and disciplined approach. The function is an integral part of sound corporate governance and is considered as the third line of defence.
2. Risk based internal audit (RBIA) policy lays a framework for entity-level risk assessment and assures the Board of Directors and the Senior Management on the quality and effectiveness of the organisation's internal controls, risk management and governance-related systems and processes.
3. Risk-based internal audit is expected to be an aid to the ongoing risk management by providing necessary checks and balances in the system.
4. The internal audit team would undertake an independent risk assessment to formulate a risk-based audit plan which considers the inherent business risks emanating from an activity/location and the effectiveness of the control systems for monitoring such inherent risks.
5. The risk assessment of business and other functions of the organization shall at the minimum be conducted on an annual basis. Every activity/location, including the risk management and compliance functions, shall be subjected to risk assessment by the RBIA.
6. The scope of risk-based internal audit includes identifying potential inherent business risks and control risks, suggesting various corrective measures. The audit mechanism should also ensure adequacy, effectiveness of laid down procedures and ensure compliance with the same to control the risks to the optimum level.
7. The scope of the internal audit includes all the auditable entities/units within Tamilnadu Urban Finance and Infrastructure Development Corporation Limited (TUFIDCO) including technology-related aspects.
8. The internal audit report should be based on appropriate analysis and evaluation. It should bring out adequate, reliable, relevant, and useful information to support the observations and conclusions. It should cover the objectives, scope, and results of the audit assignment and make appropriate recommendations and/or action plans.

9. All the pending high and medium risk observations and persisting irregularities should be reported to the ACB/Board to highlight key areas in which risk mitigation has not been undertaken despite risk identification.
10. The internal audit function should have a system to monitor compliance with the observations made by the internal audit. Status of compliance should be an integral part of reporting to the ACB/Board.
11. The information systems audit (IS Audit) should also be carried out using the risk-based approach.
12. Ensure compliance with regulatory guidelines specific to Internal Audit and related aspects.
13. The RBIA policy must be reviewed annually.

Distribution of the Policy document

This is a confidential document and is meant for restricted distribution among TUFIDCO employees only. Any unauthorised copying or distribution of this document is strictly prohibited. Individuals in the custody of this document are responsible for ensuring the confidentiality of the document. It is the responsibility of the Internal Audit Department to ensure that the document is updated with changes as and when required.

Policy Governance

Risk Based Internal Audit Policy Implementation

All employees of TUFIDCO and management are responsible for ensuring that Risk based Internal Audit policy is adhered to. The Internal Audit department is responsible for ensuring that staff are aware of, and adhere to, this Policy and the standards thereunder

Policy Compliance

The Internal Audit Department shall ensure that:

• All users including TUFIDCO employees and management adhere to the Policy standards.

• Continuous compliance monitoring and measurement processes shall be adopted.

• Reports about continuous compliance monitoring and measurement processes shall be shared with the ACB/Board annually.

Review of Risk based Internal Audit Policy

The document shall be reviewed at least annually by the Head of Internal Audit. The risk based internal audit policy and standard operating procedure documents shall be updated in line with any major or minor changes in the operating environment. This Policy shall also be reviewed and updated in line with recommendations provided by various stakeholders including risk management function, external auditors, and legal counsel.

Exceptions to the Policy

Notwithstanding any guidance by the regulator, the Internal Audit Department shall identify instances where exceptions to the Policy requirement shall be allowed for process, procedure, systems, and specifications. Such requests shall be approved by the Managing Director (MD) and reported to the Audit Committee. Exceptions allowed shall be reviewed periodically by the Internal Audit Department.

Non- compliance/Violation of the Policy

Violation of standards defined in this document may include, but not limited to:

• Users do not comply with the Policy standards

• Violation of guidelines provided by the regulators

Non-compliance of users to the Risk Based Internal Audit Policy would result in disciplinary actions including, but not limited to:

• Suspension

• Termination

• Other disciplinary action

• Civil and/or criminal prosecution

Training and Awareness

1. All employees of TUFIDCO should be provided with an awareness of the Risk based Internal Audit policies and procedures to enable them to ensure adherence and they operate in such a manner as to ensure its risk is appropriately addressed.
2. TUFIDCO should arrange and coordinate periodic training and awareness programs through the training systems of the organization to ensure that sufficient, competent,

and capable human resources are available. These programs should be targeted at all levels of employees including end-users in the organization, top management personnel and personnel managing the Internal Audit of the organization.

3. The respective departments should monitor the work performance of their staff and should hold periodic assessments to identify Internal Audit training needs and to discover any problem areas, particularly where staff deal with sensitive information, or work on sensitive information.
4. All management and staff should be briefed on their role in ensuring the protection of the organization's risk areas and complying with the relevant policies and procedures.
5. All TUFIDCO employees should receive prompt notice of changes in TUFIDCO's risk based internal audit policies and procedures, including how these changes may affect them and how to obtain additional information.

Organisational Structure

The objective of this Policy is to create a risk based internal audit mechanism that manages inherent business risk emanating from an activity/location and the effectiveness of the control systems for monitoring such inherent risks. To disseminate the policy, an organisational structure has been set. The detailed roles and responsibilities have been spelt out to bring about clarity of roles of responsibilities of each stakeholder in the organisational structure.

Roles and Responsibilities

A. Board of Directors / Audit Committee of Board/IT Strategy Committee

1. The Board of Directors (the Board) / Audit Committee of Board (ACB) of TUFIDCO are primarily responsible for establishing and overseeing the internal audit function in the organization.
2. The ACB/Board shall approve the RBIA policy and RBIA plan to determine the priorities of the internal audit function based on the level and direction of risk, as consistent with the entity's goals.
3. Developing an effective culture around the importance of internal audit
4. The ACB/Board will review the performance of RBIA annually.
5. The ACB/Board should formulate and maintain a quality assurance and improvement program that covers all aspects of the internal audit function. The quality assurance program may include assessment of the internal audit function at least once a year for adherence to the internal audit policy, objectives and expected outcomes.

6. The ACB/Board shall promote the use of new audit tools/ new technologies for reducing the extent of manual monitoring/transaction testing/compliance monitoring, etc
7. The findings of the system and process audit including but not limited to IS Audit, shall be presented before the IT Strategy Committee of the Board.

B. Senior Management

1. The senior management is responsible for ensuring adherence to the internal audit policy guidelines as approved by the Board and development of an effective internal control function that identifies, measures, monitors and reports all risks faced.
2. The senior management shall ensure that appropriate action is taken on the internal audit findings within given timelines and status on the closure of audit reports is placed before the ACB/Board.
3. The senior management is responsible for establishing a comprehensive and independent internal audit function that should promote accountability and transparency.
4. It shall ensure that the RBIA Function is adequately staffed with skilled personnel of right aptitude and attitude who are periodically trained to update their knowledge, skill, and competencies.
5. A consolidated position of major risks faced by the organization shall be presented at least annually to the ACB/Board, based on inputs from all forms of audit.

C. Internal Audit Department

The Internal Audit Department (IAD) will be responsible for undertaking risk based internal audits under the guidance of the Audit Committee / Board. IAD must have sufficient authority, stature, independence, and resources thereby enabling internal auditors to carry out their assignments properly. IAD shall be headed by a senior executive with independent reporting to the Audit Committee.

The internal audit function shall not be outsourced. However, where required, experts including former employees can be hired on a contractual basis subject to the ACB/Board being assured that such expertise does not exist within the audit function. Any conflict of interest in such matters shall be recognised and effectively addressed. Ownership of audit reports in all cases shall rest with regular functionaries of the internal audit function.

Head – Internal Audit

• Provide annual assessment on the effectiveness of the organization's controls in managing key risks and control activities.

• Evaluate the reliability and operation of the accounting and reporting system.

• Consider the scope of work of the external auditors and regulators to determine audit coverage.

• Evaluate the effectiveness of risk management processes

• Evaluate fraud risk management process

• Conduct or participate in internal investigations of suspected fraud, theft, or mismanagement, and provide advice relating to internal fraud and security at the request of those charged with governance

• Maintain adequate professional audit staff with sufficient knowledge, skills, experience, and professional certifications to meet the requirements of this policy

• The Head Internal Audit shall ensure that the department has the necessary resources, financial and otherwise, available to carry out his or her duties commensurate with the annual audit plan, scope and budget approved by the Audit Committee.

• Assess the effectiveness of the management in communicating risk and control information to appropriate areas of the organization

• Coordinate and communicate information with the external auditors

• Report on potential improvements to the existing controls

• Assess and make appropriate recommendations for improving the governance process in promoting ethics and values within the organization

• Provide periodic information on the status of the implementation of the annual audit programme and the sufficiency of the Internal Audit Department resources

• Issue periodic reports to those responsible for governance, and summarize results of the internal audits

• Present quarterly report/update to the Audit Committee, confirming on annual basis independence of the Internal Audit Department and its audit staff, its performance during the period against key performance indicators.

• Maintain properly documented files supporting conclusions, holding in safe custody any documents or property or other material obtained for audit use or investigation.

• Ensure independence of Audit leads and staff.

The Head – Internal Audit will be supported by Internal Audit leads for various business units and support functions. These audit leads will be responsible for audit planning and execution of their respective areas.
Key responsibilities of the Audit Leads include:

• Determine the scope, risk, and frequency of audit activities in identified areas of responsibility
• Monitor the implementation of the audit plan
• Review and approve audit procedures
• Deliberate on the issues raised with the IAD and management
• Finalize the audit report including action plans
• Discuss the audit report with the Head – Internal Audit
• Implement a tracking system to independently follow up on the open issues and escalate, if required; and
• Identify the need for follow-on audits to validate the remedial actions put in place.
• On-going engagement with their respective Branch Unit heads to understand business developments and identify new risks emerging in their work area.

Internal Audit Structure

Authority, Stature, Independence, and Resources

The internal audit function must have sufficient authority, stature, independence, and resources thereby enabling internal auditors to carry out their assignments properly. The Head of Internal Audit (HIA) and internal audit functionaries shall have the authority to communicate with any staff member and get access to all records that are necessary to carry out the entrusted responsibilities.

Competence

Requisite professional competence, knowledge and experience of each internal auditor are essential for the effectiveness of the internal audit function. The staff possessing the requisite skills should be assigned the job of undertaking risk-based internal audits. They should also be trained periodically to enable them to understand the business activities, operating Procedures, risk management and control systems, MIS, etc.

Rotation of Staff

The minimum period of service in the internal audit function shall be 6 months. The Board prescribes at least one stint of service in the internal audit function for those staff possessing specialized knowledge useful for the audit function, but who are posted in other areas, to have adequate skills for the staff in the internal audit function

Reporting Line

The Head of Internal Audit shall directly report to MD & CEO with approval from the Board of Directors. Accordingly, the 'Reviewing authority' shall be the ACB/Board and the 'Accepting authority' shall be the Board in matters of performance appraisal of the Head of Internal Audit. The ACB/Board shall meet the Head of Internal Audit at least once in a quarter, without the presence of the senior management (including the MD & CEO/WTD). The Head of Internal Audit shall not have any reporting relationship with the business verticals and shall not be given any business targets.

Remuneration

As such all auditors are full-time employees of the company. Auditors may also be appointed on a contract basis or any method. In any arrangement as decided, the remuneration policies of auditors should be structured in a way to avoid creating a conflict of interest and compromising the audit's independence and objectivity.

Out Sources Internal Audit Arrangements

Internal audit functions shall not be outsourced as per the regulatory guidelines. Wherever required, experts including former employees can be hired on a contractual basis subject to ACB / Board being assured that such expertise does not exist within the internal audit function of the Company. However, ownership of all audit reports shall rest with regular functionaries of the internal audit function.

The following aspects may, inter-alia, be kept in view to prevent any risk of a breakdown in internal controls on account of outsourcing arrangements:

(a) Before entering an outsourcing arrangement for a risk-based internal audit, due diligence should be performed to satisfy that the outsourcing vendor has the necessary expertise to undertake the contracted work.

(b) The contract, in writing, should at the minimum, specify the following:

- the scope and frequency of work to be performed by the vendor
- the manner and frequency of reporting to the entity the manner of determining the cost of damages arising from errors, omissions, and negligence on the part of the vendor
- the arrangements for incorporation of changes in the terms of the contract, should the need arise
- the locations where the work papers will be stored
- the internal audit reports are the property of the Company and all work papers are to be provided to the Company when required
- the authorised employees are to have reasonable and timely access to the work papers
- the supervisors are to be granted immediate and full access to related work papers

(c) The management should continue to satisfy itself that the outsourced activity is being competently managed.

(d) All work done by the vendor should be documented and reported to the top management through the internal audit department.

(e) To avoid the significant operational risk that may arise on account of sudden termination of the outsourcing arrangement, a contingency plan should be in place to mitigate any discontinuity in audit coverage.

(f) Periodic review of work performed by the outsourced vendor to be done by Head of Internal Audit for reliability, accuracy, and objectivity.

Access to Information

For the risk assessment to be accurate, it will be necessary to have proper MIS and data integrity arrangements. The internal audit function should be kept informed of all developments such as the introduction of new products, changes in reporting lines, changes in accounting practices/policies, etc. The risk assessment should invariably be undertaken yearly. The assessment should also be periodically updated to consider changes in the business environment, activities, and work processes, etc.

Documentation

For the risk assessment to be accurate, clearly understandable, be unambiguous and verifiable at a later stage, documentation of each process is of utmost importance. Documentation of the process would involve but not be limited to.

1. Maintaining of a register with columns to showcase the audit area, sub-area, process, risk rating, observation, methodology of assessment, details of data collected, curated observations
2. As far as possible all documentation will be in digital format and filed in a logical way for easy access
3. Data transferred on each finalized observation and updated thereon will be stored in a version-controlled method.
4. All past data about published audit reports should be in read-only format.
5. All data will be stored in compliance with as per IT policy.
6. Sensitive data to be stored and shared must be password protected

Code of Ethics

All employees including the employees in the internal audit team are governed by the general code of ethics as per the HR policy of TUFIDCO.

Auditees Responsibilties

Internal audit should not be a fault-finding mission. It is done to find out errors in the systems and working, lag from approved timelines, adequacy of controls and their effectiveness in managing inherent risk and to generate process improvement opportunities to improve overall efficiency in the area being audited.

To attain these objectives, there must be support from the auditee. His / her responsibilities are as follows.

1. Providing required data to auditors – The auditee must provide accurate data/additional data with all fields as requested by the auditor. If the data request contains sensitive information, the auditee can take suitable guidance/approval from the appropriate authority before sharing such data.
2. The audit is conducted as per the approved audit calendar and with time constraints. During the audit, the auditee must attend and discuss the issues or queries raised by the auditors on time.
3. The auditee is responsible to oversee the activity in the department. He should work towards improvements in all aspects of his area/domain.
4. The auditee must be positive and commit to the timely closure of observations. In all cases where he agrees with the observation for improvements but is not empowered to

decide on cost and other factors, he may take up the matter with suitable authority and get necessary approvals on time.

5. In cases where the observations are as per best industry practices but not feasible with current TUFIDCO practices, the auditee must ensure the observation is marked as PIO (Process Improvement Opportunity)
6. Closure of observations within the approved timeline is the responsibility of the auditee. He must close the audit observations of the period when he was not in the department also.
7. The auditee is responsible for rectification of observations immediately. He must not wait for the final audit report to start the rectification process. The management gains comfort when the observations in the audit report are rectified before presentation to management.

Man Power

The senior management is responsible for establishing a comprehensive and independent internal audit function that should promote accountability and transparency. It shall ensure that the RBIA Function is adequately staffed with skilled personnel of the right aptitude and attitude who are periodically trained to update their knowledge, skill, and competencies.

Policy Details

Risk Assessment Frame Work

Risk assessment is an important part of any internal audit process that is used to understand the impact of risk and the probability for the risk to be realized. The results of a risk assessment must be used to prioritize efforts to counteract the risks.

The process of risk assessment is not a one-time activity but an ongoing project, which is dynamic and responds to changes in the internal and external environment facing an organization at a point in time. Therefore, while risk assessment may be classified as a point in time exercise, an organizations' ability to assess and manage its risk continuously (in response to an ever-changing environment) is a key challenge.

Independent Risk Management

To prepare a risk based internal audit plan, the internal audit team must understand the existing and known risks in the system. It should be noted that the risk based internal audit plan would cover, based on criticality/ risk, all risks in the system. As and when a new risk is discovered, the risk based internal audit plan may be relooked and if the need arises, the plan may be updated.

Risk Assessment Methodology

The organization will undertake a yearly Risk Assessment to formulate the risk-based audit plan. The risk assessment would be performed as an independent activity to cover risks at various levels (corporate and branch; the portfolio and individual transactions, etc.) and the processes in place to identify, measure, monitor and control the risks.

Further, the assessment will be updated periodically to account for changes in the business environment, activities, and work processes.

The risk assessment process will cover the following activities:

• Identification of inherent business risks in various activities undertaken by the organization.

• Evaluation of the effectiveness of the control systems for monitoring the inherent risks of the business activities

(`Control risk').

• Drawing up a risk-matrix for considering both the factors viz., inherent business and control risks

The risk assessment process shall involve but not be limited to processing the following information:

- Previous internal audit reports and compliance
- Proposed changes in business lines or changes in focus
- A significant change in management / key personnel
- Results of the latest regulatory examination report
- Reports of external auditors
- Industry trends and other environmental factors
- Time elapsed since the last audit
- The volume of business and complexity of activities
- Substantial performance variations from the budget
- Business strategy of the entity vis-à-vis the risk appetite and adequacy of control.

The following phased approach shall be adopted for performing the independent risk assessment

a. Preparation: To undertake a risk assessment, an understanding of the scope and functions of the various functions that support the business processes shall be obtained. This involves, but is not limited to:

i. Identifying business functions and processes: Business functions critical to business delivery shall be identified and focused upon. Interviews with concerned stakeholders shall be scheduled to understand the business functions and priorities of the organization.

ii. Understanding existing risk management framework: Applicable risk standards relevant to the TUFIDCO environment shall be evaluated and assessed.

iii. Assess overall control environment: Obtain information regarding the overall control environment by reviewing the existing risk registers, audit reports, organisation structure, major changes within the function, business performance.

b. Preliminary risk assessment: The risks related to the various TUFIDCO processes shall be identified. This involves, but is not limited to:

i. Interviews with key stakeholders: Interviews shall be conducted with the key stakeholder to understand the processes and identify possible gaps in the definition of processes.

ii. Performing high-level process walkthroughs: Process walkthroughs shall be performed to understand the operation of business processes and to identify possible issues in the working of such processes.

iii. Verifying evidence of control design and implementation: Evidence of control design and implementation shall be verified to validate the efficacy of the control in mitigating risks.

c. Inherent risk and control risk rating/categorisation: The risk assessment is done at the inherent risk and control risk level. Inherent business risks indicate the intrinsic risk in a

particular area/activity of the organization and will be grouped into low, medium, and high categories depending on the severity of the risk. Inherent risk rating will be done based on the impact and likelihood of a particular risk rating. The methodology for grouping the risks into High, Medium, and low categories depends on the severity of the risk which is enumerated in ANNEXURE 1.

Control risks arise out of inadequate control systems, deficiencies/gaps and/or likely failures in the existing control processes. The control risks will be classified into low, medium, and high categories and the methodology is enumerated in ANNEXURE 2.

The Extremely High-Risk Areas would require immediate audit attention, maximum allocation of audit resources besides ongoing monitoring by the organization's top management. The inherent business risks and control risks will also be analysed to assess whether these are showing a stable, increasing or decreasing trend.

The risk matrix will be prepared for each business activity/location.

A – High Risk- Although the control risk is low, this is a High-Risk area due to high inherent business risks.

B – Very High Risk- The high inherent business risk coupled with medium control risk makes this a Very High-Risk area

C – Extremely High Risk – Both the inherent business risk and control risk are high which makes this an Extremely High-Risk area. This area would require immediate audit attention, maximum allocation of audit resources besides ongoing monitoring by the top management.

D – Medium Risk – Although the control risk is low this is a Medium Risk area due to medium inherent business risks.

E – High Risk – Although the inherent business risk is medium this is a High-Risk area because of control risk also being medium.

F – Very High Risk – Although the inherent business risk is medium, this is a Very High-Risk area due to high control risk.

G – Low Risk – Both the inherent business risk and control risk is low.

H – Medium Risk - The inherent business risk is low, and the control risk is medium.

I – High Risk – Although the inherent business risk is low, due to high control risk this becomes a High-Risk area.

The outcome of the risk assessment or final rating of an auditable unit will be a key factor to decide on the frequency of audit, the extent of audit to be undertaken and the type of audits to be performed. E.g., Extremely high-risk areas will be subjected to audits at a higher frequency or concurrent audits and higher scrutiny.

We must also analyse the inherent business risks and control risks to assess whether these are showing a stable, increasing or decreasing trend. Illustratively, if an area falls within cell ‘B’ or ‘F’ of the Risk Matrix and the risks are showing an increasing trend, these areas will also require immediate audit attention, maximum allocation of audit resources besides ongoing monitoring by the top management (as applicable for cell ‘C’).

Trend of Risk

Risk-based internal audit is expected to be an aid to the ongoing risk management by providing necessary checks and balances in the system.

The risk assessment needs to be done regularly and the finding must be compared with the findings of the earlier period to identify trends of shifting/reducing/increasing risks. This process will also help us identify among others, new areas of risk, areas of risk which have become redundant due to change in systems, operations, processes, automation etc. The trend will also be generated from the level of risk accepted in each domain. The actual risk generated will be compared with the benchmark risk (threshold risk) and the risk level as per previous periods to generate a trend.

Risk Based Audit Plan

• The Internal Audit Department will prepare Internal Audit Plan based on the Risk Assessment.

• The frequency of audits/prioritisation of areas will be determined based on the Risk Assessment process.

• The areas identified as high, very high, extremely high risk (based on the matrix) will be audited at shorter intervals as compared to medium and low-risk areas.

• The frequency of audit will be decided based on matrix

The Audit Plan will prioritize audit work to give greater attention to the areas of:

(i) High Magnitude and high frequency

(ii) High Magnitude and medium frequency

(iii) Medium magnitude and high frequency

(iv) High magnitude and low frequency

(v) Medium Magnitude and medium frequency.

All the units/businesses/locations (Even Low Risk) of TUFIDCO should get audited at least once in two years.

The risk based internal audit plan prepared by the audit team should be reviewed by the management and presented to the Audit Committee for approval. The audit plan should be revisited periodically based on changes and dynamic risk assessments undertaken.

Audit Execution

The internal audit execution will be undertaken by a combination of process audits, concurrent audits, systems audits, file audits by way of offsite/remote auditing methods as well as physical verification and visits. IAD will perform the following types of audits to provide comprehensive assurance to the management and the Audit Committee:

• Process audit based on risk assessment
• Branch/field audit based on risk assessment
• Concurrent audit
• Thematic audit
• Information systems audit
• Offsite monitoring and risk analytics

Based on the Internal Audit Plan, Head – Internal Audit in coordination with the IA team will ensure timely audit execution. The organization will strive to undertake audits through in-house audit resources. However, audits that require specialized skill sets and are not available within IAD may be performed with the help of experienced external auditors. The contract with the external auditor should specify the scope of work to be performed and critical terms.

Internal Audits shall be performed using Audit Programs defined for the specific type of audit/area being audited.

Head – Internal Audit shall ensure appropriate working paper documentation for all the audits and activities performed for record and future reference.

Audit Report and Reporting Observation

• Audit Reports will be prepared in the standard format and issued following the conclusion of each engagement and will be distributed as appropriate.
• The observations will be graded, classified in line with the agreed observation grading matrix.
• IAD will be responsible for appropriate follow-up activity on results from audit reports. The status of observations will be tracked until resolution and reported as part of the regular audit pack to the Audit Committee, including those observations that have not (yet) been addressed within an appropriate / agreed timeframe.

• The summary of the status of the audit plan, key observations, open audit points will be presented to the Audit
Committee quarterly.
• IAD will also assist in providing necessary information to RBI for Risk based Supervision and any other requirements.

Closure of Observation

All observations need to be closed within the timelines as agreed at the time of closure of the published internal audit report. These timelines are key to ensuring the systems are upgraded and improved to cover the identified risk areas.
There can be changes in the operational activities, systems, and controls during the period from publishing the internal audit report to the committed date of closure.
If due to any unforeseen circumstances, the auditee is unable to fix the issue and ensure closure of the observation, and/or if there are repeated observations, the auditee must get approval from management for extension of timelines or closure of the observation without fixing the issue as the risks have been mitigated with other controls/system upgrades.

Continuous Monitoring

A risk assessment is an important part of any internal audit process that is used to understand the impact of risk and the probability for the risk to be realized. The results of a risk assessment must be used to prioritize efforts to counteract the risks.
The process of risk assessment is not a one-time activity but an on-going project, which is dynamic in nature and responds to changes in the internal and external environment facing an organization at a point in time. Therefore, while risk assessment may be classified as a point in time exercise, an organizations' ability to assess and manage its risk continuously (in response to an ever-changing environment) is a key challenge

Communication

The communication channels between the risk-based internal audit staff and management should encourage reporting of negative and sensitive findings. All serious deficiencies should be reported to the appropriate level of management as soon as they are identified. Significant issues posing a threat to the business should be promptly brought to the notice of the Board of Directors, Audit Committee, or top management, as appropriate

Performance Evaluation

Periodic Review

The Internal Audit Department should conduct periodical reviews, annually or more frequently, of the risk-based internal audit undertaken by it vis-à-vis the approved audit plan.

1. The performance review should also include an evaluation of the effectiveness of risk-based internal audits in mitigating identified risks.
2. The Board of Directors/Audit Committee of Board should periodically assess the performance of the risk-based internal audit for reliability, accuracy, and objectivity.
3. Variations, if any, in the risk profile as revealed by the risk-based internal audit vis-à-vis the risk profile as documented in the audit plan should also be investigated to evaluate the reasonableness of the risk assessment methodology of the Internal Audit Department.

Code of Ethics for Internal Audit Department

There are certain moral principles that the Internal Auditors should follow. These are illustrative and not exhaustive; these provide the basic guidelines to the Internal Auditors about the moral hazards and conflicts which they may face while carrying out Internal Audit assignments.

Integrity, Objectivity & Independence of Internal Auditor

• Internal auditors shall have an obligation to exercise honesty, objectivity, and diligence in the performance of their duties and responsibilities.

• Internal Auditors holding the trust of the organization, shall exhibit loyalty in all matters about the affairs of the organization.

• Internal Auditors shall refrain from entering any activity which may conflict with the interest of the organization.

• Internal Auditors shall not accept a fee or a gift from an employee, a contractor, or a supplier.

• Internal Auditor must be fair and must not allow prejudice or bias to override his objectivity. She/he should maintain an impartial attitude. The internal auditor should not, therefore, to the extent possible, undertake activities, which are or might appear to be incompatible with her/his independence and objectivity. For example, to avoid any conflict of interest, the internal auditor should not review an activity for which she/he was previously responsible.

• Internal Auditor should immediately bring any actual or apparent conflict of interest to the attention of the appropriate level of management so that necessary corrective action may be taken.

Confidentiality

• Internal auditors shall be prudent in the use of information acquired in the course of their duties. She/he shall not use confidential information for any personal reason or in a manner that would be detrimental to the interest of the organization.

• Internal Auditor should not disclose any such information to a third party, including employees of the entity, without specific authority of management/ client or unless there is a legal or professional responsibility to do so.

Annexure 1-INHERITANT RISK RATING CRITERIA

Risk Impact Category	Low (1)	Medium (2)	High (3)
Financial Reporting	Impact below INR ___Crores. i.e., Less than 1% of PAT	The impact between INR ___ Crores and INR ____ Crores. i.e., 1% to 5% of PAT	Impact of more than INR ____ Crores, i.e., 5% of the PAT
Financial Impact	Financial transactions below INR 1 Lac	Financial transactions between INR 1 Lac to INR 5 Lacs	Financial transactions above INR 5 Lacs
Reputational	No reputational damage as news is not available to anyone other than key Stakeholders.	Reputational damage due to information with the Clients, Vendors, and Investors	Widespread reputational damage due to public news and media coverage

Regulatory	Non-compliances that may not result in any regulatory implications.	Non-compliances that could result in inspection comments or remarks from the regulator	Financial Penalty, Showcause notice from the regulator and Potential Cancellation of License
Operational	Operational errors / lapses below 1%	Operational errors / lapses between 1% to 5% of the transactions.	Operational errors/lapses beyond 5% of the transactions
Legal	Limited / No legal impact	Legal suits of medium impact/with the possibility of out of court settlements	Legal cases could result in financial penalties and regulatory fines for the Company, KMPs and Directors.

ANNEXURE-2 – CONTROL RISK RATING CRITERIA

Sl No	Control Rating Category	Audit Report Rating and Compliance Status	Control Risk Score	Control Risk Rating	Weight
1	Previous Internal Audit Report and Compliance Status	Satisfactory with no major pending open risks/gaps	3	Low	15%
		Needs Improvement with no or some pending open risks/gaps	2	Medium	
		Unsatisfactory with major pending open risks/gaps	1	High	

Sl No	Control Rating Category	Changes in Business/Processes/Product	Control Risk Score	Control Risk Rating	Weight
2	Proposed changes in business lines or changes in business focus or change in product/processes	Minor or no changes proposed/implemented since the previous audit	3	Low	10%
		Partial changes proposed/implemented since the previous audit	2	Medium	
		Major changes proposed/implemented since the previous audit	1	High	

Sl No	Control Rating Category	Changes in Management / Key Personnel	Control Risk Score	Control Risk Rating	Weight
3	A significant change in Management / Key Personnel	No Changes in the Management / Key Personnel	3	Low	10%
		Few changes in the Management / Key Personnel	2	Medium	
		Significant changes in the Management / Key Personnel	1	High	

Sl No	Control Rating Category	Audit comments in regulatory or other examinations	Control Risk Score	Control Risk Rating	Weight
4	Results of Regulatory examination report or any other audit	No negative comments or negligible comments	3	Low	20%
		Few negative comments/issues highlighted	2	Medium	
		Severe negative comments highlighted	1	High	

Sl No	Control Rating Category	Industry Trends / Environmental Factors	Control Risk Score	Control Risk Rating	Weight
5	Industry Trends / Environmental Factors	Growing industry trends/environment factors	3	Low	5%
		Status quo in industry trends / environmental factors	2	Medium	
		Adverse industry trends/concerns in the environmental factors	1	High	

Sl No	Control Rating Category	Time Lapsed	Control Risk Score	Control Risk Rating	Weight
6	Time elapsed since last audit	< 6 Months	3	Low	10%
		>6 Months x < 12 months	2	Medium	
		> 12 Months	1	High	

Sl No	Control Rating Category	Volume and Complexity	Control Risk Score	Control Risk Rating	Weight
7	The volume of Business and	Low Volumes or Less Complexity of Activities	3	Low	10%
		Medium level Volumes or Complexity of Activities	2	Medium	
		High Volumes or Complexity of Activities	1	High	

Sl No	Control Rating Category	Variations against Targets	Control Risk Score	Control Risk Rating	Weight
8	Substantial performance variations from targets (business volumes/performance numbers)	A variance of up to 10% between business targets and actual performance (underachievement or overachievement)	3	Low	5%
		A variance of greater than 10% but less than 20% between business targets and actual performance (underachievement or overachievement)	2	Medium	
		A variance of greater than 20% between business targets and actual performance (underachievement or overachievement)	1	High	

Sl No	Control Rating Category	Business Strategy	Control Risk Score	Control Risk Rating	Weight
9	Previous Internal Audit Report and Compliance Status	Business Strategy factors overall risk appetite of the Company	3	Low	5%
		Business strategy is aligned with the risk appetite of the Company and control environment	2	Medium	
		Business strategy is not aligned with the risk appetite of the Company and Control environment	1	High	

Sl No	Control Rating Category	Systems Environment	Control Risk Score	Control Risk Rating	Weight
10	Systems environment and system-based controls	A highly automated environment with minimal manual controls (i.e., if 75% of the total controls are automated)	3	Low	5%
		Moderately automated environment with combination of manual & automated controls (30% - 75% automated controls)	2	Medium	
		High reliability on manual controls (less than 30% automated controls)	1	High	