Journal of Communications Finance
Volume I, Issue I, Jul-Dec 2024, pp. 24-33

3.2 Risk Based Internal Audit

Shri Kaushik Chawdhary, AO(RMC), Pr. CCA, Kolkata

Abstract

Risk Based Internal Audit emphasizes identifying and addressing critical risks, such as compliance lapses, financial inaccuracies, and system vulnerabilities, rather than routine procedural errors. It highlights key risk categories, including compliance, inherent, control, financial, and credential risks, with practical examples like discrepancies in bank guarantees, delayed pension settlements, and misclassification of financial transactions. The current paper outlines the principles, tools, and methodologies for Risk-Based Internal Audit (RBIA) in the telecommunications sector. The paper also stresses the importance of skilled auditors, advanced tools like SARAS and SAMPANN, and data-driven approaches for enhancing audit effectiveness. Benefits of RBIA include improved decision- making, targeted risk mitigation, and alignment with government priorities, though challenges like false alarms and cost are noted. The approach is vital for managing sector-specific risks and ensuring revenue assurance, regulatory compliance, and operational stability.

Keywords

Risk-Based Audit, Compliance, Revenue Assurance, Internal Audit, Telecom Sector, Financial Risk, Data Analytics, Governance, Cybersecurity, Regulatory Compliance, Technological Advancement.

Introduction

Risk-based Internal Audit (IA) is a style of internal audit of an organization which focuses upon the analysis and management of risk. Unlike traditional approach, which focus upon the procedural lapses for deviation of Rules & orders, errors in accounting of transactions, and detection of overpayments etc. only; a risk-based approach ensures that, the internal audit activity is focusing its efforts on providing assurance and advisory services related to the organization's top risks. It helps the administration to understand, whether the risk management tools of an organization are sufficient to detect and prevent leakage in revenue earning, misappropriation

of Government money and check in expenditure to better achieve organizational objectives through good governance and control.

Roles of Auditors & Scope

Internal auditors play a critical role in risk management. The inspection should be independent/objectively derived and the auditors should not compromise with the objectives of internal audit. The auditors are responsible for identifying the potential risks in the existing system as well as speculating the risk may involve in changed scenario. They should not only detect the risk but suggest or provide recommendations on how to mitigate these risks and help the organization implement these measures. Internal auditors can reduce duplicate efforts and increase the effectiveness of overall risk management by coordinating the internal audit reports with the risk management team.

Criteria for Selection of Audit Team

Selection of auditors in the internal audit team is important and auditors should be well versed in rules and latest Government orders, Standard Operating Procedures (SOPs), etc. Auditors should have basic concepts, frameworks, tools, and techniques related to risk and risk management. They must also have the working knowledge in relevant software and applications run in the department and its limitation so that system audit can be done to check & prevent manipulation of data, if any.

In addition, they should have the knowledge in all fields of works in the department and maintenance of records and registers in the manuscript formats also.

Identification of Risks

The first approach to Risk Based Audit is to identify the nature of Risk. Following are the type of risks involved in financial audit.

Compliance Risk: Risk involved when the right Procedures, SOPs and Guidelines as per prevailing Rules & Orders are not followed.

Inherent Risk: It is the possibility of inaccurate information appearing in financial statements or bills due to error on commission or omission. Like imposing wrong percentage of GST or TDS on Income Tax.

Control Risk: This kind of risk may be involved due to lack of control over routine workflow or non-adherence to timeline, like non issuance of required Bank Guarantee (BG) after BG rationalization or non-issuance of demand notice to the TSPs/ISPs on time, contempt of Court Cases, imposing of heavy penalty, interest in delayed settlement of claim cases, wrong assessment of dues, over payment or short payment, and surplus adjustment. Sometimes, leakage in revenue generation or revenue collection due to lack of control may lead to control risk.

Financial Risk: Financial Risk involved due to misclassification of account head or wrong booking (Dr. or Cr. Swap) or improper accounting affect the financial statement, resulting in adverse balances or negative balances.

Detention Risk: Sometimes a superficial auditing may not detect the risk involved in manipulation of account figures, if any, and thereby may lead to detention risk. Cross checking of figures from different statements or registers may overcome this detention risk.

Credential Risk: This type of risk involved when credential of the customer or Licensee or Pensioner is not known or in doubt. Review of KYC/KYP, CAF is very crucial else payment to wrong person cannot be averted. In the case of TSPs & ISPs, ascertaining the credential of the authorized person or the signatory is very crucial. In the case of payment authority, the specimen signature of the authorized signatory is essential to check to avoid credential risk. Validation of DSC and its tracking may be done at the time of system audit.

Tools for Risk based Internal Audit

- Verification of Gross Revenue by checking P&L statement & UDIN from ICAI portal to detect under reporting of revenue by TSPs & ISPs.
- Review of BGs submitted by TSPs & ISPs, whether as per norms.
- Analysis of data by comparing with previous financial year to check the trend.
- Query based analysis of data. (Example: Sample checking of Normal & Enhanced Family Pension, Commutation of Pension, CRD/IDA Rate, Arrear bills, Additional quantum rate eligibility etc.)
- Sample case study of long pending grievances and repetition of same nature of grievances.
- Observations from previous audits and actions taken.

- Previous corrective actions suggested and its implementation.
- Areas that were not inspected during previous audits.
- Procedural and system changes from previous audits.

Best Practices That May Be Adopted in the Course of Internal Audit Inspection [(1)]

In Internal Audit analytical processes including

(1) Computations
(2) Comparison
(3) Component wise segregation of information
(4) Rational discussion to arrive at any evidence to determine final conclusions. Observation, inquiry & inspection enable internal audit teams to collect evidence of risks in the merit.

Planning for Risk-Based Audit

Broad Principles

(i) Strategic review & understanding of Govt priorities.
(ii) Review of nature & structure of internal control.
(iii) Preparation of audit plan.
(iv) Risk assessment of activities of entity.
(v) Categorization of risk.
(vi) Execution of the plan strategy & feedback of auditee.

Action to Be Taken

Study of Previous Reports: Study of previous audits bring out the financial compliance & operational risks. Old reports may be studied along with action taken report. Compliance given may be reviewed for its accuracy, implementation & risk covered. Area not covered may be identified & procedural & systematic modifications may be made to improve upon the previous audit.

Sample Size: Action taken formations & drawing up of audit plan regarding high-risk areas may be prioritized. Since audit team has access to the previous reports as well as current activity reports like Status of Work Report (SWR), System for Accounting and Management of Pension (SAMPANN) & System for Assessment

of LF Revenue and SUC (SARAS) reports, proper sample size may be identified. Size of the sample should be neither too small nor too big. Sample size should be at least 10% of total records for a meaningful audit. Records which have different time duration should be sampled separately, activities with deadlines may be seen from the point of view of time overruns leading to cost overruns.

Assessing the Risk Profile: Periodic recurring activity like pension payment are less risk prone in procedural irregularity. However financial implication needs to be thoroughly checked within a decent sample size. Activities with financial implications are considered as high-risk activity. Therefore, financial loss on leakage can be checked with greater sample size. Since telecom sector is technology driven & is a system based set up, collection of data should be purified in the audit phase to eliminate duplicity, inaccuracy on inconsistency. Information in the data form needs to be analyzed in accordance with defined rules & procedures to identify irregularity.

Risk cause matrix

Likelihood of occurrence (probability)				
High				Impact
Moderate				
Low				
	Low	Moderate	High	

Severity

Benefits of Risk-Based Audit (RBA)

Auditor can easily justify the work carried out by him with complete details & reason. No oversight or negligence can be alleged on the auditor and it is a systematic approach which saves time & efforts.

It eliminates over auditing or under auditing and helps auditor to identify & prove the high-risk/low risk areas. Audit report should be prepared for highlighting the irregularities as per the risk involved.

Improves the understanding of critical areas, thus preventive & corrective action can be suggested by the internal auditor.

RBA improves understanding of vulnerability & leads to better decision-making.

Disadvantages of Risk-Based Audit

It is proved to generate an excessive number of false alarms which may overwhelming impact on management thereby diluting their focus. Lack of contextual information in the alerts may generate complexities & lack of differentiation between actual threat & false alarms. It may also be expensive & not suitable for small units. Uncertain in standards. Disruption in smooth functioning.

Risk based audit may highlight a problem without any bearing on finding a solution, for example, there are leakages in revenue is high risk due to lack of data analysis in trend & pattern of recovery. However, way to recovery may be totally elusive unless payment processes are rectified.

Risk Management Within the Telecom Sector

In an ever-evolving realm which is technology driven with a disruptive pace of change like telecommunication, adept risk management becomes the key element in ensuring operational stability and resilient network as well as revenue assurance for the government from various telecom operators and internet service providers, etc. Risk management involves recognizing, evaluating and reducing the likely disruption that could impede seamless functioning of telecom networks.

Recognizing: To provide quality of service to customers, earn revenue from service, the operator must ensure smooth transmission of voice, data and video access, diverse network irrespective of extensive distances, terrains and geographics within the country as an NLD provider. The introduction of 5G technology transcends mere acceleration of internet speeds along with a web of interconnected devices, smart infrastructure and AI driven applications [(2)]. The landscape of risks extends far beyond cyber threats, hacking and cyber intrusion that pose a threat to the integrity of the entire network architecture. The TRAI provides a dynamic regulatory environment which necessitates continual attention and adaptation for the operators. They need to navigate stringent regulations while audit needs to stay ahead of the technological achievements and associated risks they introduce just as much as the operators require it.

Some Issues to Be Looked into and Risk Associated for Reference

1. Collection register not showing receipt of payment properly (Low Risk).
2. Interest rate not charged as per DoT guidelines (Low Risk).
3. Some decentralized licensees neither paid minimum license fee nor paid license fee based on actual / presumptive AGR (Moderate Risk).
4. BG invoked due to non-renewal of BG within prescribed due date. But the same not replenished by the TSP/ISPs in the form of fresh BGs (Moderate Risk).
5. BGs not booked in proper Head of account (Low Risk).
6. Though, claim for deduction by the concerned TSPs has been disallowed by the CCA office, proper reasons /orders are not shown against each disallowed amount (Low Risk).
7. Revenue for few companies as per UDIN is higher than the Audited AGR (High Risk).
8. Collection Register of LF/SUC have not been updated and counter Signed by the Competent Authority resulting in improper verification checking work not in order (Low Risk).
9. The date of commissioning of mobile tower is not ascertained, resulting in non-utilization of USO Fund properly (Low Risk).

Decentralized Licenses

10. Pending assessments for the ISPs for different financial years (High Risk).
11. If while adjusting Outstanding dues and penal interest, DoT guidelines not followed (Moderate Risk).
12. ISPs have not submitted relevant documents in SARAS, resulting in delayed completion of DVR (High Risk).
13. Collection Register of LF/SUC have not been updated and counter Signed by the Competent Authority resulting in improper verification (Low Risk).

Pension

14. Excess payment on account of over drawn interest on deferred DCRG after date of instead of till Date of death (High Risk).
15. Periodic verification of qualifying service (completion of 18 yrs and left with 5 yrs service) not done in due time (Low Risk).
16. Short payment of Pension made by Bank (Low Risk).
17. Delay towards settlement of Family pension cases on a/c of death in service (Low Risk).

18. Non-Revision of provisional pension of CDA Pensioner under Rule 69 of CCS pension Rules 1972 and irregular payment of CDR at constant rate. (Low Risk).
19. Extended family pension cases other than spouse being processed through COMPACT instead of SAMPANN (Low Risk).
20. Delayed deferred DCRG payment (Low Risk).
21. Delayed remittance of LSPC attracts penal interest on it. Non-realization of the same (High Risk).

Certain Strategies for Mitigation of the Risks Must be Adopted by Creating

Digital transformation like System for Assessment of LF Revenue and SUC (SARAS) and System for Accounting and Management of Pension (SAMPANN) with Public Financial Management System (PFMS) enables certain resilience in driving efficiency and effectiveness in CCAs. Embracing innovative technologies along with environmental, social and governance matrices (ESG) bolsters sustainability along with regulatory compliance and resource optimization. "Staying ahead" in the face of all challenges and threats requires a holistic perspective in Internal Audit methodology also. There is a dire need of deploying comprehensive mitigation strategy which includes Customer centricity, Adaptive work environment, Sustainability, Technological resilience, etc.

When risk-based approach is combined with service industry like telecom, it is evident that internal audit cannot become one-size-fits-all approach. An effective audit department will have many approaches so that case by case most optimal approach can be selected.[3] Audit planning & research which is a preaudit process involving data collection, analysis, documentation as well as sending the request list after getting access to document repositioning a precursor test is conducted. On site field work with auditor interview, perform the tests obtain follow up & entry & exit meetings where draft findings are shares. Finalization, editing & report writing is then completed within a fortnight. After finalizing the audit report compliance is also sought in a time bound manner.

This Rapid assurance method helps to recognize well defined & limited scope without any complication auditor shoulders prior effort & after field work light interaction after a week of crisp engagement. This mandates that auditors receive their requested evidence & documents timely.

Project assurance Audit manages risks in real time. Auditor evaluates program implementation with clear deadlines e.g. implementation of SAMPANN by migration of pensioners from bank & post offices to CCA offices. Auditors need to be involved from beginning to finish of the project & monitor control capabilities of the project team of facilitate risk & control dialogue throughout the project.

Problem solving audit where auditors serve as facilitators to fix a problem by assessing their own processes. Pension Voucher Audit (PVA) is one such exercise of facilitated self-assessment for improving risk analysis & response time.

Creating customized models also helps to assess the current solution & improve process to meet the objectives. Data analytics is most comprehensive when combined with above mentioned methods. Quantitative & qualitative analytics may generate insight into may risk areas. Auditors need skills to investigate unanticipated results without jumping to conclusions.

By thoughtfully tailoring the various approaches risk-based audit can be successfully conducted. In telecom sector, risk management needs to account for unique challenges faced by TSPs & ISPs in transmission of data over long distances & across different networks along with natural geographical conditions, disasters & damages along with cyber security. [(4)] Telecom sector is constantly evolving change. It is the responsibility of internal audit to ensure risks to change have been clearly identified as well as provide assurance that risks are being controlled.

Conclusion

Audit methodology in telecom must follow a multifaceted approach and internal audit teams must be trained with skills to audit cutting edge technologies such as AI, machine learning, Internet of Things along with skills of predictive analytics to proactively detect and prevent potential threats, fostering a sense of accountability, involvement and vigilance within the department. Internal audit while using the risk-based audit method must help management in:

Revenue assurance; Process compliance; Regulatory compliance; Operational efficiency; Data security; Technology adoption; Procurement and inventory management, and help in achieving the vision and mission of the department.

References

1. Controller General of Communication Accounts. (n.d.). *Internal Audit Manual*. CGCA. Retrieved from https://cgca.gov.in

2. Subex. (n.d.). *Navigating risk management and assurance in the evolving telecommunications landscape*. Retrieved from https://www.subex.com/article/navigating-risk-management-and-assurance-in-the-evolving-telecommunications-landscape/

3. Audit Board. (n.d.). *5 risk-based internal auditing approaches*.

4. Empowered Systems. (n.d.). *Risk management in telecommunications: An overview*.

*****

Author's Profile

Kaushik Chowdhury, AO (IA) at the Office of the Principal Chief Controller of Accounts (Pr. CCA), Kolkata, has been serving in the Internal Audit Section and RMC Section since 2022. He has conducted internal audits for various CCA offices in the Eastern Region and participated in cross audits at the offices of the CCA in Gujarat and Madhya Pradesh on behalf of the Office of the Controller General of Communication Accounts (CGCA). Kaushik holds an M.Sc. in Chemistry from Calcutta University. Beyond his professional pursuits, he has a passion for singing and has represented the All India Postal Carrom Tournament.