Success Stories
on
Risk Management

Ashok Leyland Limited

Chennai

Organizational Description

Ashok Leyland Limited (hereinafter referred to as, "Ashok Leyland", or "the Company"), flagship of the Hinduja group, is the 2nd largest manufacturer of Commercial Vehicles in India. Globally, Ashok Leyland is the 4th largest manufacturer of Buses, and the 10th largest manufacturer of Trucks.

Headquartered in Chennai, India, the Company has a wide product portfolio encompassing Trucks, Buses, Light Commercial Vehicles, Defence Mobility Solutions, Power Solutions, as also Aftermarket services backed by a strong dealer and service network.

Ashok Leyland's Vision is "*To be a Top 10 Global CV Player creating reliable and differentiated products & solutions, while delivering outstanding stakeholder value"*

Since its incorporation in 1948, Ashok Leyland has grown to become one of India's foremost commercial vehicle manufacturers with a 11,966-strong workforce as of March 31, 2019. Driven by innovative products suitable for a wide range of applications and an excellent understanding of the customers and local market conditions, the Company has been at the forefront of the commercial vehicle industry for decades. Over millions of passengers use Ashok Leyland buses to get to their destinations every day and 7,00,000 trucks keep the wheels of the economy moving. With the largest fleet of logistics vehicles deployed in the Indian Army and significant partnerships with armed forces across the globe, Ashok Leyland helps keep borders secure. Ashok Leyland launched India's first electric bus and Euro 6 compliant truck in 2016.

A US$ 4.2 billion company, Ashok Leyland's enterprise is spread over 50 countries, having manufacturing facilities and marketing presence in India, UAE, Bangladesh, Sri Lanka, United Kingdom, Kenya and Nigeria.

Ashok Leyland is the first Commercial Vehicle company, outside of Japan, to have won the coveted Deming Prize for its manufacturing plants at Pant Nagar and Hosur. It has been ranked amongst the Top 40 best brands in India *(34th position in 2019)* by *Interbrand*, and one of India's finest workplaces by *ET Now (2017).*

People, Planet, and Profit for all stakeholders, is at the core of Ashok Leyland, which resonates with its philosophy of "AAPKI JEET. HAMARI JEET." (which means "In your success, lies our success").

Effectiveness of the Risk Management Framework

The Enterprise Risk Management framework at Ashok Leyland is inclusive, well integrated and standardized and encompasses all business units & functions, adopting the foundations of the COSO ERM framework & ISO 31000 standard. It enables the Company to strike an optimal balance between its growth and associated risks in pursuit of its strategic and operational objectives.

The Company's ethos of *"Aapki Jeet. Hamari Jeet."*, has been imbibed within the ERM framework as well. The culture of innovation in Ashok Leyland also extends to Risk Management, which is considered to be a way of life, rather than a compliance activity.

Ashok Leyland has in place a comprehensive ERM Framework document covering ERM Charter, ERM Vision & Mission, ERM structure, Risk Culture, Risk philosophy, Risk Appetite and Tolerances and ERM procedures. This serves as a guidance for implementing the risk management policy and strategy across the organization. Ashok Leyland's comprehensive ERM framework sets out the risk philosophy of the Company including the need to establish a sound risk culture (*ability to identify and seize relevant business opportunities and take risks based on informed decision-making practices*) across the organization.

Roles and Responsibilities of Organizational Risk Management setup

The ERM structure at Ashok Leyland is supported by robust Tone at the Top from the Board & Senior Leadership.

The Board, through the Risk Management Committee (RMC), provides oversight of the ERM framework and reviews the management of enterprise risks and the Company's exposure to residual risks.

The RMC ensures that the company has an appropriate and effective ERM process with well-defined policies and procedures. The RMC apprises the board on a periodic basis on the effectiveness of the ERM process and on the significant risks and its mitigants. The Committee reviews the risk posture of the company and ensures that the management is taking appropriate measures to mitigate the same, recommends changes to the Risk Management process and approves allocation of resources for Risk Management.

The ERM Steering Committee, the management-level Committee, is headed by the Chairman and comprises of members of Senior Leadership team. It is responsible for the overall ERM process, reviews the risk profile of the Company periodically and recommends necessary actions to manage the downsides, as may be applicable.

The Risk Management Committee / ERM Steering Committee is assisted by the Corporate ERM function, which facilitates the ERM process and ensures that the appropriate risk management procedures are adopted and adhered to. It consolidates and provides periodic risk updates to the Risk Management Committee / ERM Steering Committee.

Functional risk management teams are formed for each of the business verticals / functions, who are responsible for deliberation of the risk identification, risk evaluation and risk mitigation plan for each of the organizational objectives at the respective Business Unit level.

Periodic risk updates are provided by the Business verticals / Functions, which are further consolidated by the Corporate ERM function and submitted to the ERM Steering Committee (management-level committee) and Risk Management Committee including the report of key enterprise risks, risk heat maps, risk universe and risk tolerances.

Corporate ERM facilitates risk assessment for critical business projects / initiatives undertaken by the company, covering operational, regulatory / legal and financial risks. As part of this, the key risks pertaining to the projects are identified, assessed and mitigation plans / controls, as appropriate, are advised. These are reviewed and factored for risk mitigation as appropriate.

ERM Process

The Risk Management process, based on the components and principles of the COSO ERM Framework (2017) & ISO 31000:2018 standard, comprises of strategy and objective setting, risk identification, risk assessment, risk response, risk monitoring and risk reporting.

- **Strategy and objective setting:** At Ashok Leyland, Risk is integrated with strategy and planning and is factored in business decision-making. At the time of Annual Corporate Planning exercise, alongside the strategy setting, risk management strategy is also finalized, considering the acceptable risk appetite and tolerances. Further, management evaluates the alternate strategies and assesses the risks and opportunities of each option to ensure that the chosen strategies are aligned with the organization's vision, mission & core values.
  The Corporate ERM function also provides inputs in the form of a "Risk Outlook" report which comprises amongst other things – an analysis of external environment, macro-economic outlook, key emerging business risks identified by global risk surveys in addition to key industry and technology trends.
- **Risk Identification:** Risks critical to achievement of strategy and organizational objectives are identified and mitigation plans are devised through corporate initiatives/projects. Further, each of the business units and functions identify the risks for their respective functional objectives considering the internal (such as Operational, Financial, Compliance, People & Stakeholder expectations) and external (such as Legal & Regulatory, Political, Economic, Competitive environment at domestic and international levels) context.
  Common risk identification tools and techniques include structured workshops, brainstorming sessions, interviews, questionnaires and listing of potential events. Risks are also identified as part of day-to-day activities through measures which include budgeting, performance reviews and actual incidents. Emerging or newly developing risks, are also identified periodically, through industry wide scans, changes in business context and analysis of internal factors/trends.

- **Risk assessment:** Each risk identified is assessed in terms of its impact on the achievement of company's strategic and business objectives and likelihood of its occurrence. Risk rating is the product of impact and likelihood and is a process of prioritizing the risks identified for treatment. Apart from impact & likelihood, risks are also assessed using the dimension of their velocity, i.e., speed of onset of the risk. Risk assessments form the basis for selection of risk responses.
- **Risk responses:** Having assessed the relevant risks, appropriate risk responses are determined by the management considering the cost / benefit of the response to manage the risk within the business objectives, performance targets and risk appetite. The mitigation plan is implemented by the functional risk management team based on the agreed time frame and responsibilities. This is reviewed on a quarterly basis by the Function Head for its effectiveness.
- **Risk monitoring & review:** The progress and effectiveness of the risk mitigation activities are periodically monitored and where necessary, they are appropriately modified to bring the risk in line with the target performance and risk tolerances.
  Functional risk management teams periodically identify and assess any substantial changes in the internal and external environment that may affect the achievement of their strategy and business objectives. The ERM Steering Committee reviews the Key Enterprise Risks / High risks and Functional Risk Heat Maps on a quarterly basis.
  The Corporate ERM function conducts periodic monitoring to ensure that the Risk Management processes are being followed and provides assurance to the management regarding the overall effectiveness of the ERM program.
- **Emerging Risks:** Business units / functions continuously scan the external environment for any emerging risks, trends, new technologies, regulatory changes etc., These are closely monitored and where necessary, strategic initiatives are planned to manage the same.
  The Corporate ERM function also provides periodic emerging risk alerts in the form of a "*Risk Watch*" report, highlighting the key emerging risks and trends and the likely impact on the industry / company.
- **Information, communication and reporting:** The risk data and information are communicated to the various stakeholders, including the Risk Management Committee / Audit Committee, to provide relevant and timely information for use in decision making. Risk communication and reporting comprises of various aspects such as Risk Register, Risk Universe, Risk Heat Map, Report of Key Enterprise Risks.

SAP GRC Risk Management Solution

Ashok Leyland has successfully leveraged technology for risk management through implementation of SAP GRC Risk Management solution. The solution, extending across all business units & functions, has enabled automation of the ERM framework with real-time risk reporting, alerts, and dashboards.

A real-time risk register is maintained by each functional risk management team in SAP GRC Risk Management solution. This provides a single window view of the risks of each function / business vertical to the management.

Interface of Corporate ERM function with Internal Audit

Seamless collaboration of Corporate ERM function with Internal Audit is ensured through cross-pollination of inputs that feed into both verticals. Significant findings arising from Internal Audit reviews are shared with the Corporate ERM function. These are discussed with the business verticals / functions for inclusion in the functional risk register, as appropriate. The Risk Universe compiled by the Corporate ERM function is taken as one of the critical sources of input while developing the Annual Risk based Internal Audit Plan. Inputs on emerging risks, including global / country related risks, provided by the Corporate ERM function are also considered for the Internal Audit review.

Internal audit periodically conducts an independent evaluation of the risk management process, reporting and management of key risks to provide an assurance to the Board/Risk Management Committee on the effectiveness of ERM at AL.

Fraud Risk Management & Whistle Blower Policy

Ashok Leyland has established a robust fraud risk management framework across the Company.

The Company has defined a comprehensive Code of Conduct for its employees, Directors and Third parties, which outlines the values and principles of the organization which are the pillars for ethical conduct.

The Company has appointed a Corporate Ombudsman, whom the suppliers, employees or customers may approach for any references, complaints or grievances about the Company, its employees or its dealings. This further enhances the effectiveness of the Corporate Governance process.

The Company has also instituted various fraud deterrent measures including establishment of a Vigil mechanism / Whistle Blower Policy, to enable stakeholders to report unethical behavior, actual or suspected fraud, or violation to the Company's Code of Conduct. The policy comprehensively covers aspects pertaining to the role of a whistleblower, manner of making disclosures and undertaking investigations, reporting, protection of whistleblowers and secrecy or confidentiality of information. The policy is also disclosed on the website of the Company. The company seeks to ensure that no unfair treatment is given to a Whistle Blower and the appropriate care is taken to keep the identity of the Whistle Blower confidential and confidentiality of the protected disclosure is maintained. It also ensures that there is no kind of discrimination, harassment, victimization or any other unfair employment practice adopted against the Whistle Blower and complete protection is given against any unfair practices such as retaliation, intimidation and threat.

Most of the fraud risks are mitigated through robust internal controls which include having appropriate roles & responsibilities defined and segregation of duties. Internal Audit, as a part of its risk-based assurance reviews, evaluates potential risks of fraud within the processes being reviewed. Further, our Statutory Auditors also evaluate fraud risks, as part of financial statement audits.

Key Risk Indicators

Key Risk Indicators have been defined for key risks and are periodically monitored and reported. Wherever there is a breach in the defined threshold levels, the risks are re-assessed, and corrective action is taken, where necessary.

Alignment of Risk Process with ISO 31000

ERM framework at Ashok Leyland embodies the principles described in ISO 31000:2018 and is aligned to the risk management process as laid out in the standard. Ashok Leyland firmly believes that ERM practices integrate with all other aspects of business, including governance, strategy, performance management, and internal control practices. Integrating ERM with business activities and processes results in informed decision-making and enhanced performance.

Strategy for Managing Risks

Risk Management at Ashok Leyland is based on the tenet that risks and opportunities must be managed proactively, rather than being reactive. Given the cyclical nature of the domestic Commercial Vehicle industry, unpredictability of economic cycles coupled with ever increasing competitive pressures, and high level of operating costs, it is imperative that Ashok Leyland must be a cost leader regardless of market conditions. To this end, the Company has seeded a culture of cost-consciousness and continues to focus on pro-active cost reduction initiatives, aimed at bringing down the operating cost and break-even point, giving it the much need resilience to withstand the impact of the periodic industry / economic downturn.

Also, Risk management at Ashok Leyland, views risks as "Opportunities" for growing its business. The Company continues to focus on diversifying and growing its non-truck business through an overseas expansion strategy, pushing growth in non-truck business verticals and embarking on digital initiatives and customer solutions business. This would offset the risk of the domestic CV industry cyclicality by reducing the Company's business concentration risk in Trucks and complement its non-truck businesses, apart from tapping new business opportunities.

We, at Ashok Leyland, constantly strive to enhance our state of ERM maturity based on an understanding of external benchmarked practices which will enable us achieve our ERM Vision of becoming a truly "Risk Intelligent enterprise".

IIFL Finance Limited

Mumbai

Organizational Description

Started in 1995, India Infoline is India's leading integrated financial services group with diverse operating businesses, mainly, Non-Banking Finance, Housing Finance, Microfinance, Wealth and Asset Management, Financial Advisory and Broking, Mutual Funds and Financial Product Distribution, Investment Banking, Institutional Equities, Realty Broking and Advisory Services. India Infoline Finance Limited was incorporated in 2004 under the flagship of IIFL Finance Limited (formerly 'IIFL Holdings Limited').

IIFL Finance Limited is a systematically important, non-deposit accepting non-banking financial company catering to the rising credit requirements of underserved markets through its diversified retail offerings.

IIFL Finance Limited along with its subsidiaries is engaged in the financing business. The Company's diverse product suite, include Home Loans, Gold Loans, Business Loans (including Loans Against Property and MSME Financing), Microfinance, Developer and Construction Finance and Capital Market Finance, catering to a broad spectrum of retail customers.

The Company's wide physical network of 2,309 branches spanning across the length and breadth of the country along with a strong digital presence enables the Company to service to a vast customer base. Its small ticket retail focused products especially cater to the underserved sections of society.

Effectiveness of the Risk Management Framework

IIFL Finance has a very robust risk management framework that has evolved over a period of time. Being regulated by multiple regulators viz. SEBI, RBI, MCA, etc; we have an ongoing emphasis on building a process driven culture where there is strong emphasis on risk management, compliance and adherence to polices.

This is also reflective in our Vision – *"To be the most respected financial services company in India"* and 'Core Values' referred to as ***'FIT'.***

- Fairness - in our transactions with all stakeholders, bereft of fear or favor.
- Integrity - of the utmost nature, in letter, in spirit, and in all our dealings with people.
- Transparency - in all our dealings with stakeholders, media, investors, and the public.

Our integrated Enterprise Risk Management framework is a Top – Down and Bottom – Up approach, whose constituents include:

- Well defined business strategy of being a diversified retail focused NBFC. Our product offerings accordingly comprise of (a) Core Growth Segments, which includes Housing Loans, Business Loans to MSME, Gold Loans and Microfinance Loans; and (b) Synergistic Segments, which closely align to our Core Growth Segments and include Developer and Construction Finance and Capital Market Loans.
- Risk Tolerance Limits – for every activity and product offerings, whose adherence is monitored by the Board.
- Empowerment – of employees and branches to take decisions within defined framework, closely aligning with our culture of 'Owners Mindset'.
- 'Three Lines of Defense' model – where first line of defense is the makers viz. business / support functions; second line of defense are independent risk management and compliance functions and the third line of defense is Internal Audit who gives an assurance to the Board and Audit Committee.
- Reporting – to Board and Regulators. IIFL Finance being a listed entity believes in high level of transparency and reporting to its shareholders.

Risk Management framework is subject to periodic testing of its effectiveness through a 'Stress testing' and 'Audit' which is conducted by reputed independent external agencies.

Roles and Responsibilities of Organizational Risk Management set-up

Board of Directors: The Board of Directors has an overall responsibility for effective implementation of Risk Management framework and instilling a robust and transparent risk culture.

Based on the nature of Risk, the Board has defined various Board Committees that include:

- Risk Management Committee: comprising of Independent Directors, Whole Time Directors, CEO, CRO and CCO who monitor all facets of risk on a half yearly basis.
- Asset Liability Committee: comprising of Independent Directors, Whole Time Directors, CEO, CRO, CFO and Treasurer who monitors liquidity and market risk on a quarterly basis.
- Audit Committee: comprising of Independent Directors, Whole Time Directors, CEO, CRO, CFO and Head of Internal Audit who evaluates internal audit findings and validate financial statements on a quarterly basis.
- Information Technology Committee: comprising of Independent Directors, Whole Time Directors, CEO, CRO, Head of Internal Audit and Chief Technology Officer who monitor information security risks on a quarterly frequency.
- Compensation committee: comprising of Independent Directors and Chief People Officer who define compensation of key management personnel.
- Credit Committee: comprising of Independent Directors, Whole Time Directors, CEO, CRO and CCO who evaluates and monitor large funding proposals on an ongoing basis.

Risk Management Committee: Risk Management Committee (RMC) of the Board is tasked with the oversight responsibilities to monitor adherence to overall risk limits defined by the Board. RMC comprises of Independent Directors, Whole Time Directors, CEO, CRO and CCO who monitor all facets of risk. They meet at a minimum on a half yearly basis and in certain event specific scenarios at a shorter frequency. Its terms of reference include:

- Implementation of robust risk culture within the entire organization.
- Define and approve risk strategy and risk tolerance limits.
- Monitor compliance with regulatory and compliance risks.
- Report to the Board on key risks, risk management performance and the effectiveness of internal controls.

Operational Management: As the first line of defense, operational managers own and manage risks ensuring adherence to established policies & procedures for business operations.

Sourcing:

- Resilient business strategy with well-defined geography and sector –driven sourcing plan.
- Systematic & well- defined process for seamless customer onboarding.
- Strong fraud detection through referral checks leveraging local intelligence aided by technology.

Technology:

- End-to-end digitization through multiple innovations.
- Analytical algorithms to support faster credit decisions incorporating demographic and bureau parameters.
- Heightened branch security with sensors and exclusive vault access for gold storage and OTP based access.

Training:

- Training for sales personnel for appropriate customer identification.

- Learning sessions for branch personnel to avoid spurious and excess funding of gold loans.
- Proactive monitoring of early delinquencies for possible identification of sourcing issues.

Chief Financial Officer: CFO is key management personnel who have the overall responsibility of ensuring books of accounts and financial statements reflect a true and fair view of the affairs of the Company. He is the face of the organization to most regulators, rating agencies, bankers, shareholders and other external stakeholders.

Key Corporate Governance Risks

IIFL conducts an ongoing evaluation of all facets of risk. Based on the nature of the risk, a well defined mitigation strategy has been defined. Certain inherent risks in each of the areas are defined below:

Operational Risk: IIFL Finance being a retail organization having close to 4 million customers spread across nearly 2,000 branches, operational risk is one of the most critical risks. These would include:

- Failure of Internal Controls.
- Obsolescence of technology.

We have a robust operational risk framework that includes polices, standard operating procedures, risk control self-assessment, control testing, etc. which ensures risk incidents are identified, reported and resolved timely and effectively. Monthly Operational Risk Management Committee chaired by the CEO does an ongoing evaluation of risk incidents and process failures so as to enable timely escalation and quick fixes.

Market Risk: IIFL Finance being a financial services company in the business of lending, faces inherent market risk which includes abnormal market price movement effecting collateral cover, changes in borrowing / lending rates due to regulatory changes or changes in market dynamics. This risk is monitored on a continuous basis, and based on market specific events timely actions are initiated

Occupational Health & Safety Risks: IIFL Finance has over 20,000 employees spread across 600+ locations. Manpower is the single largest asset of the organization and significant investment is made in employee health and safety. IIFL has been nominated as a Great Place to Work for the current year.

Fraud Risks and Policy & Process for Prevention

IIFL has a zero tolerance policy for frauds and misconduct incidents. With this philosophy, IIFL has been investing in processes, systems, trainings and digitization to avert incidents of frauds and misconduct.

Being in the business of lending, risks associated with customer selection and staff fidelity are mitigated by strong processes and an oversight team, referred to as 'Fraud Control Unit'. Ongoing audits and vigilance is conducted to ensure that risks of frauds are identified, investigated and resolved timely.

Strong use of artificial intelligence, data analytics and various technology enabled integrated solutions have been put in place to ensure risks of fraud are nipped in the bud. Some of the technology solutions that have been implemented included the following: National Hunter, FinFort, Perfios, Probe 42. Additionally, in consultation with our in-house data analytics team we have implemented an 'Application Fraud scorecard 'incorporating likelihood of fraud occurrence. This ensures that incidents of identity theft and document forgery are completely eliminated.

Risk Management Process

The process of implementation of Risk Management policy includes following steps:

Identify Risk : It begins with recognizing and describing the risks that might affect a business or its outcomes. The results of risk identification are documented in a IIFL risk register, which includes a list of identified risks along with their sources, potential risk responses, and risk categories. This information is used for risk analysis, which in turn supports creating risk response.

While risk identification is majorly done in the beginning of a new product/ business, it's important to remember that risk identification is an iterative process wherein new risks can be identified throughout the life cycle due to changes to the business.

Assess Risk: Upon identification of risk, it is imperative to determine the priority, likelihood and consequence of each risk. Risk assessment is done for thorough lookout of workplace to identify those things, situations, processes, etc. that may cause harm. These assessments are very important as they form an integral part of risk management plan. Risk Prioritization is done with help of risk heat map. Ranking or prioritizing risks is one way to help determine which risk is the most serious and thus which to control first. Priority is then established by taking into account the exposure and the potential for incident which is then discussed in detail at Risk Committee.

Risk Mitigation Measures: Considering the complexity associated with product offerings, systems and operational processes, risk mitigation handling approaches initiated by the Company have been characteristically different. For certain risks which are dependent on external conditions, it is important to identify such risks with potential impact ensuring adequate capabilities (Natural disasters, unstable macro-economic conditions, etc.). Similarly, certain segment may not be advisable due to existing social, economic and political situations. The Company does an ongoing evaluation and modifies its processes and strategies in accordance with the treat. For the risks which have been identified and well within capabilities of the organization, our endeavor is on minimizing the impact of such activities. In case these risks are above the tolerance level, risk transfer is done through engaging with external agencies, subscribing to insurance policies, etc.

Policies and procedures specific to each business are implemented in line with the portfolio characteristics of the respective line of businesses. ORM framework provides guidelines on Risk Management & Monitoring mechanism for Operational Risk Events / Incidents. Various operational risk management tools include Risk Control Self-Assessment (RCSA), KRI, Process reviews, etc.

Monitor & Review: This includes review and monitoring of risk mitigation process. At IIFL there are separate teams for monitoring various risks.

- **Credit Risk:** This is evaluated and monitored by portfolio quality reviews on a monthly basis. Portfolio analysis and findings are shared and discussed with senior management based on which amendment to credit policies are undertaken.
- **Operational Risk:** Operational Risk Management framework includes continuous monitoring with help of analytics based early warning signals which are reviewed by senior management on periodic basis. Incident reporting is done based on independent root cause analysis fostering a risk culture
- **Fraud Risk:** For monitoring various Fraud Risk tools such as Karza, Finfort are used. For identification of frauds (eg fake documentation) fraud based score cards are implemented in underwriting to make smart credit decisions along with contact point verification.
- **Liquidity, Interest Rate and residual Market Risk Monitoring**: ALM team manages the Liquidity Risk through various limits & triggers including Maturity Gap Analysis / Cash-flow gap limits; Liquidity coverage; Limits on commercial paper borrowings; Short term to total borrowings ratio and Liquidity Stress testing.

Risk Reporting: Ongoing monitoring of actual performance v/s policy caps, early warning Indicators, key takeaways from Portfolio Quality reviews, Monthly Review Meetings, customer/site/competition visits etc are reviewed monthly, exceptions, if any, are reported in related committee, and acted upon as advised by the committee.

Key Risk Indicators

As part of the organizations Operational Risk Management (ORM) framework we have defined KRIs for key operational risk areas. KRIs are being monitored by the senior management as part of the periodic review with the respective departmental heads. An illustrative list of KRI is provided below.

Compliance with regulations: Customer selection, evaluation and on-boarding bypassing the mandatory Know Your Customer (KYC) norms.

Credit appraisal of loans: Manual errors / mistakes in loan appraisal and determination of credit eligibility (e.g. deviations from credit policy norms not obtained, details of past adverse credit record not specified, etc.)

Operations: Department wise trending of operations error resulting in (a) customer dissatisfaction; (b) Increase in TAT; (c) revenue loss; (d) erroneous reporting; (e) System malfunction

Accounting & finance: Erroneous data entry into incorrect ledger heads

KRIs are updated during every RCSA walkthrough or at the time of root cause analysis of OR Incident reported wherein newly identified risk is updated to the risk register.

Alignment of Risk Process with ISO 31000

ISO 31000 is a guidance on good practices in risk management which is at a high level and is intended to promote harmonization with existing and future "risk" related standards.

We have established the principles as per ISO 31000 framework across IIFL by integrating risk management with organization decision making process to address uncertainty systematically with best available information with a transparent & inclusive outlook which is sensitive to change management for driving continual improvement & creating value.

In IIFL, we have established a common framework with a specific mandate & commitment from the Top Management by establishing:

- Risk management policy
- Defining accountability
- Proper identification of Resources
- Establish internal/external communication and reporting mechanisms

Whistle Blower Policy

In accordance with the prescribed regulations, IIFL has adopted a Whistle Blower Policy.

Accordingly, this policy details:

- Procedure to disclose any suspected unethical and/or improper practice taking place in the Company;
- Protection available to the whistleblower;
- Anonymous disclosure of complaints;
- Mechanism for auctioning and reporting on such disclosures to the relevant authority within the Company; and
- Relevant authority and its powers to review disclosures and direct corrective action relating to such disclosures.

Strategy for Managing Risks

Board approved Risk Management Framework is in place to foster a strong risk culture across the organization. It aims to build a profitable and sustainable business with proactive risk management practices. Regulatory guidelines have been put from a systemic stability perspective. In recent past, increased regulations are being introduced for NBFCs (e.g. NPA recognition norms, SMA, Fraud Risk, Liquidity Risk). IIFL Finance has in place a robust and well defined risk assessment and control policy. It is so structured that it caters to both product/business specific guidelines and works within the overall risk framework for the organization. The risk framework has been implemented at various levels in the organization that govern the functioning of the organization both at macro and micro levels as every employee (including departmental heads) is actively responsible for risk management.

For any new product/offer launch a detailed study covering all aspects of risks and their mitigation. During annual business planning process, the business departments / functions submit an assessment of key risks and the mitigating measures. Scenario testing is done for various scenarios factoring in the external and emerging risks.

Risk Mitigation Techniques

Tools and techniques used for risk mitigation:

- **RCSA:** For Risk identification and control, IIFL uses RCSA that are filled by various department heads. They have to describe impact of risk associated with each process, determine their likelihood and risk level. This is done with help of risk score matrix & rating scale index communicated to senior management and the Board on periodic basis.
- **Assessment of KRIs:** As part of the ORM framework we have defined KRI for key operational risk areas. KRI is being monitored by the senior management as part of the periodic review with the respective departmental heads.
- **Internal & External Audits (Concurrent & quarterly audits):** Internal Audit provides comprehensive assurance based on the highest level of independence and objectivity within the organization. Additionally, the reviews undertaken by external audit firms engaged are also discussed with senior management.
- Liquidity Contingency Plan is in place as a sound risk management practice to ensure fulfilling contractual obligations on a timely basis, ensure an adequate liquidity level under any market condition and ensure all contractual obligations fulfilled even in contingent situation.
- Early Warning Signals in credit risk monitoring framework with policy limits and caps for each product segment is in place including Vintage Analysis, bureau analytics, collections scorecard, etc.

Magma HDI General Insurance Company Limited

Mumbai

Organizational Description

Magma HDI is a joint venture between Magma Fincorp group and HDI Global SE. Magma Fincorp Limited (Magma), parent company is a Non-banking Financial Company (NBFC), registered with the Reserve Bank of India (RBI). HDI Global SE is part of the Talanx Group, 3rd largest German Insurance group by premium income. Magma HDI General Insurance Co Ltd is into Insurance business offering more than 60 products, issued more than 11.74 lakhs policies, and settled claims of 43,375 during the FY 2018-19. The first policy was underwritten on 28th Sept, 2012.

Vision

To be the most preferred, vibrant, and responsible general insurance company, fulfilling the aspirations of all its stakeholders.

Mission

The company will strive to understand the insurance needs of the consumers and translate it into affordable products that deliver value for money.

Effectiveness of the Risk Management Framework

The risk governance structure of the Company lays down the foundation for effective Risk Management. It encompasses the three lines of defense. The first line of defense is the owner of the process, second line of defense is the facilitator which include Enterprise Risk Management team and 3rd line of defense is the validator which include Internal Auditor. The Risk Management Committee oversees the process which operating management identifies and assesses risks and determine appropriate responses. The Chief Risk Officer (CRO) works with operating management in establishing effective ERM in their areas of responsibility. CRO has direct access to the Board through RMC.

The activities under CRO include Enterprise Risk Management, Operational Risk Management, Fraud Control Unit, Information Security Management and other special projects such as Data Leakage Prevention, Natural Catastrophe (NATCAT) management, driving risk culture within the organisation. The Enterprise Risk Management team assists concerned operating management in execution of their ERM activities and responsibilities. The framework adopted within the company is as given below:

- **Risk Identification**: Interview programs, Historical data analysis, learning from experience, Feedback mechanism or risk survey conducted.
- **Risk Analysis**: Assess to their potential severity of loss and probability of occurrence.
- **Risk Evaluation**: the various stakeholders internal as well as external and their views on risks are considered and evaluated.
- **Risk Treatment:** It includes
    - Risk Avoidance and Risk Retention
    - Risk Transfer
    - Risk Improvement and mitigation
    - Periodic Risk Review
- **Risk Monitoring and Review:** Determination of whether risk-steering measures were / can be implemented at the planned time and whether the planned effect of the measure is sufficient.

Roles and Responsibilities of Organizational Risk Management set-up

Board of Directors: The Board provides oversight with regard to risk management. The Board of Director of the company consist of Eight Directors.

- 4 Independent Directors including (1) Woman Director;
- 3 Non-Executive Directors;
- 1 Executive Director

The Chief Executive Officer of the Company, who is also the Managing Director is an executive member of the board. All other Directors including the chairman are Non-Executive Directors and none of the Independent Directors are relative of any other Director or employee of the company.

Risk Management Committee: The RMC oversees the process which operating management identifies and assesses risks and determines appropriate responses. It addresses enterprise-wide risks, and sets performance measure goals and key risk indicators for those risks. The Risk Management committee of the company consist of 6 members.

- Chairman, Non-Executive Director
- Non-Executive Director
- MD & CEO
- 3 Independent Directors

Operational Management: Operational Management in charge of organizational units has primary responsibility for owning and managing risks related to the objectives of their respective area.

Chief Financial Officer: Assists in formulating the company's future direction and supporting tactical initiatives while considering various risks involved.

Key Corporate Governance Risks

ERM team conducts annual survey wherein key management employees provides inputs to identify key risks and opportunities. Survey risk analysis and evaluation involves rating of risks in order to identify the top risks within the company.

Risk Survey was last conducted in Q4 FY 18-19 for key risks likely to be faced by the company in FY 19-20. The below given is the list of risk based on priority.

- People Risk
- Sales & Distribution Risk (incl business achievement)
- Regulatory Risk
- Premium Risk
- Operational Risk
- Information & Cyber Security Risk
- Concentration Risk
- Fintech Risk
- Fraud Risk
- Strategic Risk
- Catastrophe Risk
- Market Risk
- Reputational Risk
- Political & Governance Instability Risk
- Reserve Risk
- Business Continuity Risk
- Terrorism and Insurgency Risk

Fraud Risks and Policy & Process for Prevention

During the FY 2018-19, the below were the top 3 fraud categories identified during the period:

- Fake/Tampered policies
- Misuse of Pre-inspection rights
- Data Leakage

Anti-Fraud policy has been adopted by the Company to detect, monitor and mitigate occurrence of such insurance frauds within the Company. This framework includes measures to protect the insurer from the threats posed by the following broad categories of frauds:

- Internal Fraud
- Policy Holder fraud and/ or Claims Fraud
- Intermediary Fraud

The below is the Framework to prevent, detect and respond to fraud:

- Prevention of Fraud
- Detection of Fraud
- Response to Fraud
- Fraud Investigation
- Reporting of Fraud

The Company has implemented the below activities, to improve the efficiency of the framework.

- Dedicated e-mail id wherein employees can report any suspicious fraudulent activity.
- Dedicated team for identification and investigation of fraud cases.
- Fraud risk assessments of various functions to identify, mitigate and control various internal as well as external fraud risks.
- Regularly review fraud triggers to keep abreast with the current trends.
- Perform various analysis to check and identify fraud lying within the system and take appropriate measures.

Risk Management Process

The following are the stages in the Risk Management Process

Risk Identification:

The focus is to identify new or modified risk with the help of risk champions which is nominated by the functional heads. The ERM team assist in risk Identification process. Risk Identification Approach:

- Risk identification is done through questionnaires and interviews with senior management;
- Evaluations of internal audit reports related to risk management systems;
- External insights such as recognized industry know-how;
- Operational loss events reported.

Risk Analysis:

Risks are assessed on an inherent basis, considering the likelihood and impact of the risk without taking into account the controls in place in the firm. This helps to understand the importance of controls in mitigating risk.

Risk Evaluation:

It is based on the outcomes of the risk analysis. For Each Risk Identified Identify the existing control, assess the effectiveness of the control, and assess the Residual Risk.

Risk Treatment:

Techniques adopted by the company for Risk Treatment:

- Risk Accept
- Risk Manage
- Risk Transfer
- Risk Eliminate

The process to identify and accept residual risk and to define the strategy for eliminating or minimizing the impact of these risks as well as the mechanism to effectively monitor the same is captured in template "Risk Acceptance Form"

Risk Monitoring:

The overall risks are monitored against the Risk Appetite statements approved by the Board and RMC. Key risks identified during annual Risk Survey are categorized in 6 buckets i.e. Insurance Risk, Operational Risk, Strategic Risk, Market Risk, Reputational Risk and Regulatory Risk and measured against the defined parameters

Risk Reporting:

- Risk Management Survey are presented to the RMC and monitored by ERM team.
- These risks are periodically monitored by the ERM team and presented to RMC along with key inputs from functional stakeholders on changes made during the quarter/year in mitigation strategies for addressing key risks.
- Risk Control Self-Assessment (RCSA) results for the overall function comprising the overall residual risk rating assigned to the overall control environment along with key gaps are presented to RMC.
- Scorecards for evaluating the control environment at the branches are published on a monthly.

Key Risk Indicators

Yes, KRI's have been identified for the key risk/ risk areas with threshold being Green, Amber and Red.

Premium Risk

- CoR deviation from plan
- Loss Ratio deviation from plan

Solvency Risk

- Deviation from planned Solvency

Fraud Risk

- Financial Impact

IT & Cyber Risk

- System downtime instances
- System Attack and Hacking
- Data Leakage Incidents

Market Risk

- Portfolio yield to Budgeted yield
- High concentration to particular company/group

Reputational Risk

- Instances for frauds identified

Regulatory Risk

- Instances for delay in regulatory reporting
- Number of cases for non-adherence to laid guidelines.

Alignment of Risk Process with ISO 31000

ISO 31000 proposes a three stage process for risk management:

Stage 1: Establishing the context
Stage 2: Risk Assessment
Stage 3: Risk treatment

Complementary processes: In addition to the three core stages of the risk assessment process, ISO 31000 recognizes that there are two equally important complementary processes that should occur at every stage of the assessment: communication and consultation, and monitoring and review. Organizations conducting an assessment should keep stakeholders informed throughout the process and conduct monitoring to ensure the process is effective.

All the stages defined above have been considered in the risk management process under ERM framework of the company.

Whistle Blower Policy

In line with the Company's commitment to the highest possible standards of professionalism, honesty, ethical, moral and legal behavior for conduct of affairs of the Company towards the employees and outsiders, in fair and transparent manner and its commitment to open communication, "**Breach of Integrity and Whistle blower Policy** " has been formulated to provide a mechanism to the directors, employees, senior management personnel and/or professionals serving in any functions and attached to any roles and stakeholders of the Company to approach and report to the Disciplinary Committee and/or Officer dealing with Frauds as may be designated for this purpose or any unethical or improper practices in the Company. The Policy also seeks to protect the Whistle Blower from any retaliatory action taken by anyone in the Company including its managerial personnel.

A Whistle Blower, in exceptional circumstances, may also report any violation, to the Chairman of the Audit Committee whose address is mentioned in the policy, who shall cause investigation into the same at his own discretion or may refer the matter to the Disciplinary Committee for investigation.

Strategy for Managing Risks

The strategic initiatives to implement a consistent, efficient and economical approach for managing risks are as follows:

- **ERM Framework:** It is a structured process that enables the enterprise to address risks emanating from its various activities and functions.
- **Operational Risk Management Process**: Risks/Loss occurring due to the inadequacy or failure of people, process and system are monitored and controlled primarily by means of processes and procedures within the internal control system.
- **Loss Event Data Management:** Loss Event Data Management process requires functions to identify, notify, escalate and rectify incidents in a transparent and practical way, assisting to minimize losses, promptly rectify incidents and assess the effectiveness of controls.

- **Risk & Control Self-Assessment (RCSA):** Operational risk and control assessment provides a structured approach for the functional heads in identifying, assessing and accepting risk and evaluating relevant controls for appropriateness, effectiveness and efficiency.
- **Other Special Projects:**
  - **Data Leakage Prevention:** Framework of detecting and preventing data breaches within the company.
  - **Monitoring of Natural Catastrophe Events:** The Objective of this monitoring is to ensure information among the team is shared efficiently, and various departments are ready for various Natural Catastrophe scenarios.
  - Proposed **Personal Data Protection (PDP):** Risk team is creating awareness on the steps to be taken to ensure that we can comply with the proposed PDP bill.

Risk Mitigation Techniques

There are various tools are used to identify and mitigate risk. The below is one of the example of tool used within the Company.

Example: We use Earthquake modelling tool, from RMSI, to model our Net exposure. Modelled output from RMSI predicts various loss scenarios for Earthquake on return period basis i.e. for an event of 1 in 200 years, amount of loss the Company will have. Reviewing the output given by model on most prudent basis we purchase Catastrophe Reinsurance (CAT) to protect our Net account from Natural or man-made calamities.

Max Bupa Health Insurance Company Limited

New Delhi

Organizational Description

Joint venture between True North, a leading Indian private equity firm, and the UK based healthcare services expert, Bupa.

Effectiveness of the Risk Management Framework

There are many forces, both internal and external, that shape future of organizations ultimate success and failures. This makes it challenging to measure success of ERM effectiveness.

Successful ERM helps a business achieve its objectives constantly. But often, irrespective of its design and execution, ERM does not guarantee an organization full success.

Risk management is the conscious balance of goals with the quality of output. It is therefore critical to strategically align ERM with business performance and effectively measure its effectiveness.

Risk management effectiveness at Max Bupa is measured against the seven (7) criteria's namely: Risk based decision making; Risk appetite; Risk strategy; Risk governance; Risk responsibilities; Risk capabilities; and Risk culture.

Roles and Responsibilities of Organizational Risk Management set-up

Board of Directors: Board is responsible for setting the entity's risk appetite and monitoring the establishment and operation of prudent and effective controls in order to assess and manage the risks associated with the entity's operations.

Risk Management Committee: The Risk Committee has been established to assist the board in its oversight of risk and risk management across the organization. The Risk Committee reviews MBHI's risk appetite and future risk strategy and makes recommendations on risk appetite to the board.

Operational Management and Chief Financial Officer: The Chief Executive Officer and, under the CEO's supervision, the Executive Leadership Team (ELT), and CFO are responsible for dealing with strategic, financial, business and risk policy issues of entity wide relevance, including ensuring adherence to and further development of the Max Bupa's Enterprise Risk Management Policy.

Fraud Rsks and Policy & Processes for Prevention

As policy, Max Bupa follows fraud risk mitigation framework which takes guidance from IRDAI fraud management framework to put in place supporting policies and procedures. As a process, Max Bupa adopts PDR (Prevention, Detection & Response) philosophy:

- **Prevention** – Training & Communication program on ethical conduct, MAP (Management Action Plan) procedures to ensure fraud learning's are looped back in processes, continuous review and revision of policies & procedures basis fraud risk assessments
- **Detection** – Robust investigation team to ensure timely investigations and closure, Deployment of detective tools, reviews and mechanisms to ensure minimum surprise on fraud.
- **Response** – Max Bupa adopts zero tolerance policy on fraud and all such incidents are handled through defined consequence management framework which is applicable to all internal and external parties in business with Max Bupa.

Risk Management Process

The Risk management process includes Risk identification, Risk categorization, Control identification and assessment, risk rating and prioritization, residual risk rating and remediation action.

Key Risk Indicators

The MBHI Risk management framework has the KRI's defined at the enterprise level as per the risk appetite. MAX Bupa has identified six key risk domains as set out below and a subset of more granular specific risks which fit into these risk domains.

- Financial Risk
- Legal & Compliance Risk
- Reputation Risk
- Operational Risk
- Reputational Risk
- Strategic risk

As part of the approach to develop the Company's Risk Appetite Statement, qualitative risk appetite statements and their limits which describe the level of risk the Company is willing to tolerate within each particular risk category are defined.

Whistle Blower Policy

MBHI has a whistle blower policy approved by the Audit Committee. Policy is reviewed annually. The policy has the underlying guiding principles to ensure whistle blowers identity is kept anonymous. Max Bupa is committed to maintaining confidentiality of the Complaint and undertakes that, except to the extent required to give effect to the implementation of this Policy, the identity of the Whistle Blower is kept confidential and is not communicated, published or made known to the public, press and media in any manner.

Strategy for Managing Risks

The Organization has a documented risk management strategy which is part of the Risk management framework and is approved by the board. The elements of the risk management framework namely; Strategic Risk Assessment, Risk and Control Self-Assessment, Risk Strategy & Appetite; Risk reporting and Risk Framework Design and effectiveness review form the annual plan. The plan with its targets is annually tabled and approved by the board.

Risk Mitigation Techniques

The Risk Mitigation process for the identified risks is through a governance at operational and management level. The operating level governance of ensuring the risk mitigation plans are defined and are implemented is between the risk manager and the risk owner. The CEO chairs the Management Risk Committee (MRC) which meets quarterly at the management level. The Back testing of the mitigation plans are conducted and an assurance report is presented to the management through the working risk committees (WRC) meetings chaired by the CEO. The Information Security Committee (ISC) is convened every quarter to assess the Information Security Risk, which is chaired by the CRO. The Cyber security risk assurance framework is presented in the committee. The Board Risk Committee meets quarterly to assess the agenda papers submitted by the CRO.

Wipro Limited

Bengaluru

Organizational Description

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 170,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

Effectiveness of the Risk Management Framework

Wipro's risk management framework enables to identify, assess, quantify, manage, and monitor the enterprise wide risks using one integrated system. Enterprise Risk Management (ERM) will perform an independent audit of InfoSec Risk and Data Privacy area referring to Wipro internal controls framework focusing.

- Testing of the design adequacy of controls
- Testing of the operating effectiveness of controls
- Audit procedures to enhance implementation of controls

Compliance Assurance Team (CAT) performs a risk based assessment carried out by an independent qualified assessor, independent of core operations, to ensure key risk areas are appropriately vetted periodically for all internal controls & processes.

Roles and Responsibilities of Organizational Risk Management set-up

Board of Directors: Audit, Risk & Compliance Committee of the Board: is an independent committee of the Board of Directors that has, as its sole and exclusive function, responsibility for the risk management policies of the Organizations global operations and oversight of the operation of the enterprise risk management framework.

Risk Management Committee(s): Risk Steering Council, chaired by General Counsel, meets every month to have oversight over all the material risks identified by the ERM team. This council communicates risk policies and processes for our organization. In addition, a Risk & Governance Committee, meets on a quarterly basis to oversight org wide risk inventory and the associated governance in place.

Operational Management: Their direct responsibilities include managing both the operations processes, embracing design, planning, control, performance improvement, and operations strategy across Business Units for Wipro global operations, our products & associated services.

Chief Financial Officer: Responsible for Corporate Finance, Business Finance, Business Planning, Treasury, Taxation, Secretarial, Controllership, Assurance and Procurement. Oversee financial risk management, monitoring and evaluation of the entity's major risk exposures, including operational, legal, regulatory, business, financial, strategic, credit, & liquidity and reputation risks. Act on behalf of the Board of Directors in approving organization financial policies and procedures that allow the use of brand, value, reputation and financial derivatives for identified purposes.

Key Corporate Governance Risks

Current major risks tracked and reported are stated below:

- Information Security risks
- Data Privacy and Regulatory Compliance

- Functional and Operational risks
- Service Delivery Risks
- Workplace Environment, Safety & Security

Fraud Risks and Policy & Process for Prevention

Wipro's risk & governance committee has an oversight over the Anti-fraud policy and our fraud risk management is completely aligned to the globally accepted classification published by the Association of Certified Fraud Examiners (ACFE). These risks are broadly illustrated below:

Misappropriation of organizational assets, financial statement misrepresentations, Corruption and Bribery, Intellectual Property/Confidential Information theft/misuse.

Breach of IT systems, Conflicts of interest, skimming frauds/Fraudulent disbursements.

Following are the excerpts from the organizations Anti-fraud policy –

"Wipro does not tolerate any malpractice, impropriety, abuse or wrongdoing or fraud of any kind. The organization encourages employees to come forward and voice their concerns. Wipro assures that such concerns would be enquired into by designated persons independently and fairly. Wipro has well-articulated Code of Business Conduct (COBC) supplemented by other segment specific policies. Every Wiproite is expected at all times, to abide by these policies and when in doubt seek suitable clarifications. The policy documents the overall framework for dealing with any fraud at workplace which may adversely affect the interests of the organization and its key stakeholders (internal/external)."

The process of enabling prevention, detection and remediation of frauds is illustrated in the following example:

A comprehensive risk assessment is performed as part of GRC program for every SAP Application user. This serves as a preventive control, where access risk management function is carried out for every request received, performing risk analysis for access & Segregation of Duty (SOD), checking access requests for severity of low/medium/high. Any request resulting in High SOD require special approvals and are controlled and monitored on an ongoing basis and immediate revocation of access controls after separation of the employee from Wipro.

Another example of fraud detection and remediation is illustrated in the following example:

Wipro has implemented SAP Fraud Management System (FMS) for operationalising Fraud Risks assessments. The system is also configured to check duplicate invoice processing. In all aforementioned cases of alarming transaction, alerts are generated and Governance teams take necessary corrective actions (including disciplinary actions).

Risk Management Process

Risk management at Wipro is an enterprise wide function backed by a qualified team of specialists with deep industry experience who develop frameworks and methodologies for assessing and mitigating risks. Key stages of Risk Management process are as follows –

Risk Identification and Analysis: Risks applicable are identified based on Business process/function. Risks are analyzed based upon probability of occurrence and impact, probable cost of risk as estimated loss incurred if the event occurs, tentative occurrence date of the identified risk etc.

Risk Evaluation & Treatment: Wipro's risk evaluation criteria comprises of three layers of defense process. Contract self-assessment (CSA), Compliance assurance review (CAT Assessment), and Comprehensive audit by corporate internal audit team. Risk treatment process consists of risk avoidance, reduction, transfer and acceptance criteria as per the organization risk appetite, with an understanding that every risk should be brought to the acceptable level after the evaluation for senior management decision making.

Risk Monitoring: This activity involves monitoring, reviewing, reporting risks periodically. Risk tracking is monitoring of action items from risk register and involves identification of need to evaluate new risks, re-evaluation of changes to previous risks, action items arising out of risk register. Risks are escalated where risk

mitigation plan is NOT implemented by due date. Risks are converted into Issues on occurrence and reported to relevant stakeholders for necessary actions. When risk is no longer valid, relevant stakeholder closes the risk.

Key Risk Indicators

#	Risk Areas	Key Risk Indicators (KRI)
•	Information Security risks	1) Security training & awareness, 2) Cyber security threat intelligence
•	Data Privacy and regulatory compliance	1) Privacy obligations 2) Incident reporting
•	Functional and Operational risks	1) Segregation of duties 2) Fraud indicators
•	Service Delivery risks	1) Deal risk analysis 2) Cost of delivery
•	Work place environment, Safety and Security	1) Health & Safety awareness 2) Code of business conduct

Material risks identified during CAT assessments, Mock audits and Corp Internal audits are reviewed/ updated in the Functional Account Risk Registers and top of the house risks in Org wide Risk Inventory.

Alignment of Risk Process with ISO 31000

As described in the ISO 31000 standard, Wipro has "Information Security Risk Management Procedure" & we focus on enterprise level information security risks for critical IT Infrastructure, Processes & Services managed by Wipro. While anyone may identify a risk, however the same is evaluated, context established, prioritized, mitigation is discussed & owner to monitor & resolve is mapped to each risk. Our risk management process involves periodic review with relevant stakeholders including client, business and functional teams as appropriate. Accordingly, risks are communicated to relevant stakeholders for their further attention & support.

Whistle Blower Policy

Policy Description - Wipro is committed to the highest standards of openness and accountability. An important aspect of openness and accountability is a mechanism to enable employees, business partners, customers of the company, and other members of the public to voice concerns in a responsible and effective manner. When reporting an issue, we strongly encourage you to identity yourself and to provide as much detail as possible regarding your concern. Your privacy will be maintained in accordance with applicable data protection laws. Wipro does not tolerate any malpractice, impropriety, abuse or wrongdoing and encourages employees to come forward and voice their concerns. The Whistle Blower Policy (referred to as Ombuds Policy) has been introduced by the Company to enable employees and other individuals connected with the Company to not overlook any concern but instead raise it at an early stage and in the right manner, without fear of retaliation, victimization, subsequent discrimination or disadvantage at workplace. The Ombuds Policy has been introduced by the Company to enable employees and other individuals associated with the Company to not overlook any concern but instead raise it at an early stage and in the right manner, without fear of retaliation, victimization, subsequent discrimination or disadvantage at workplace.

Strategy for Managing Risks

Wipro's risk management framework enables us to identify, assess, quantify, manage, and monitor our enterprise risks using one integrated system. Wipro has a three layered defense model for risk identification and controls selection. Core Operations as a Primary defense, accountable for Process and System Controls, Maker-checker, Segregation of Duties, Review mechanism. Enterprise Risk Management as Second layer of defense, accountable for Development of Risk Control Frameworks, Anomaly detection rules, Organization wide initiatives, Compliance assurance reviews, mock audits, Theme based assessments and external benchmarking. Internal Audit as third layer of defense, accountable for in-depth management assurance in high-risk areas. Over and above, Contract Self-Assessment by operation teams and contractual obligations management review by Legal team, Best practices audits by External auditor and Customer audits across Business units, contribute in identifying significant risks and controls selection.

Risk Mitigation Techniques

ERM is the custodian of Org wide Risk Inventory and accountable for publishing the single view of the risk across consistently maintained Account Risk Register updated by Core operations, Information Security/Cyber security Risk maintained by CIO/CISO org.

We have internal tools to report compliance on various parameters related to BGV, mandatory Training compliance, Open Source, IP compliance, End Point compliance, Contractual Obligations compliance, etc.

- An in-house developed tool has been used as a central tracker for all CAT assessment, Customer audits and the associated findings closure.
- ICertis has been used for Contract Obligation management.
- In-house developed tool is used for the Onboarding-Off boarding status tracking.
- SOX/ICOFR-Internal Controls over Financial Reporting, Risk and Controls for SAP systems as part of preventive and detective fraud control activities and Segregation of Duty (SOD) risk analysis, SAP Fraud Management System (FMS).

ERM also publishes the Org wide Risk Inventory to Risk & Governance Committee, Risk Steering Council and Audit, Risk & Compliance committee of the board in the agreed format on a periodic and ongoing basis.