Enterprise Risk Management Policy & Framework

Document Version No.:2.0

Release Date: 23rd Oct 26

REVISION HISTORY

Date	Version No.	Prepared By	Reviewed By	Approved By	Summary of Changes
23rd Oct 26	2.0	Aniket Kulkarni	Rajashree Laad	Uma Thomas	Added Section 3.3 Risk Prioritization

Table of Contents

1.0 Introduction 4
1.1 Objectives of the Policy 4
1.2 Scope of policy 5
1.3 Maintenance of Enterprise Risk Register 6
2.0 Risk Governance 6
2.1 Board Risk Management Committee 7
2.2 Ops Management Council (MC) 8
2.3 Chief risk officer (CRO) 8
2.4 Risk Owner 9
2.5 Risk coordinators 10
2.6 Risk reporting structure 10
3.0 Risk management approach 10
3.1 Risk identification 12
3.1.1 Risk categorization 13
3.2 Risk assessment 14
3.2.1 Detailed guidelines for assessing impact & probability 15
3.3 Risk prioritization 18
3.4 Risk mitigation strategy 18
3.4.1 Risk reduction/mitigation 19
4.0 Risk monitoring & review 22
4.1 Early warning indicators (EWIs) 22
4.2 Governance, assurance & management reviews 22
Combined view - Level of Défense 31
4.3 Communication & reporting 31
5. Climate Risk Management 31
6.0 Training & awareness 32
7.0 Annexure 34

1.0 Introduction

Hexaware Technologies has grown over the years with the core value of building transparent and lasting relationships. Our mission is to Transform how IT Services are delivered and to be the first IT services company in the world where half the workforce is digital. We strive to proactively seize opportunities that the market offers in order to achieve our strategic and business objectives. In this process, we are exposed to several external and internal risks which may affect our financial and non- financial results. Hexaware ("the company") is committed to recognize & manage its risks in a proactive, ongoing & positive manner with the adoption of risk management framework.

Requirements under the Companies Act 2013 advocates the implementation of an effective enterprise-wide risk management process. With this in perspective and to ensure reasonable assurance over the attainment of our business objectives, we have adopted this risk management policy to guide our risk management activities.

The objective of an Enterprise Risk Management (ERM) system is to ensure that risks are not treated in isolation. Risks from different sources across the organization are identified, analyzed and controlled within the enterprise risk management framework of the organization and risks are treated on a timely basis with robust risk mitigation strategies and early warning indicators formulated for these risks.

This Policy:

- Articulates the company's risk management objectives
- Defines various risks and establishes use of common risk language for the company
- Defines the governance model for execution of this policy as well as responsibility for risk decisions
- Defines authority structure for committees and business functions that have a role in risk management

The aim of the policy is to ensure that every effort is made by the company to identify, measure, evaluate, manage, and monitor risk to maximize potential opportunities and minimize the adverse effects of risk

1.1 Objectives of the Policy

The objective of this policy is to ensure sustainable business growth and to promote a pro-active approach in identifying, evaluating, reporting, and managing risks associated with the business.

In order to achieve the key business objectives, this policy establishes a structured and disciplined approach to risk management in order to manage risk related issues. The specific objectives of this policy are:

- To enable visibility and oversight of the Board on the risk management system and material risk exposures of the company.
- To ensure all risks across the organization are identified and evaluated through standardized process and consolidated across the organization to identify the key risks that matter to the organization to enable risk prioritization.
- To ensure mitigation plans for key risk are agreed upon, assigned to risk owners and reviewed on a periodic basis
- To ensure that risks are reported at all levels in the organization as per their relevance and significance.
- To ensure that risk governance structure is aligned with organizational structure and risk profile of the company with well-defined and delineated roles, responsibility, and delegation of authority.

- To enable transparency of risk management activities with respect to internal and external stakeholders.
- To enable compliance to appropriate statutory & regulatory requirements, wherever applicable, through the adoption of leading practices.
- To assist in defining the early warning indicators and the related leading measures associated to the top risks identified by the enterprise
- To establish and maintain the risk appetite of the organization within the defined threshold levels by tracking the early warning indicators
- Assist in safeguarding the value and reputation by avoiding unpleasant shocks and surprises.
- Validate the implementation of risks management practices and measure the effectiveness using the risk based internal audits
- To develop a “risk aware” culture which is crucial for long term success.

1.2 Scope of policy

The policy guidelines are devised in context of the organization’s growth objectives, its business and strategy plan, global ERM standards and leading industry practices. The **Scope of the Policy** shall cover:

- This policy will be applicable to all Hexaware entities.
- All functions at corporate /branch offices across territories
- All events, both external and internal which shall have significant impact on the objectives of the organization
- This framework is reviewed & approved by CRO
- This Framework is revised based on changes in the business environment/ regulations/ standards/ best practices in the industry by an outside consultant/ organization that would present their recommendations to the Chief Risk Officer annually or as per the

directives of the Board /Audit committee

- In case of non-adherence to the policy, the same shall be reported to the Ops Management Council (MC) & necessary action may be taken in this regard

1.3 Maintenance of Enterprise Risk Register

Centralized Risk register with their mitigation plan shall be maintained by CRO and shall be reviewed and updated as per the policy guidelines.

2.0 Risk Governance

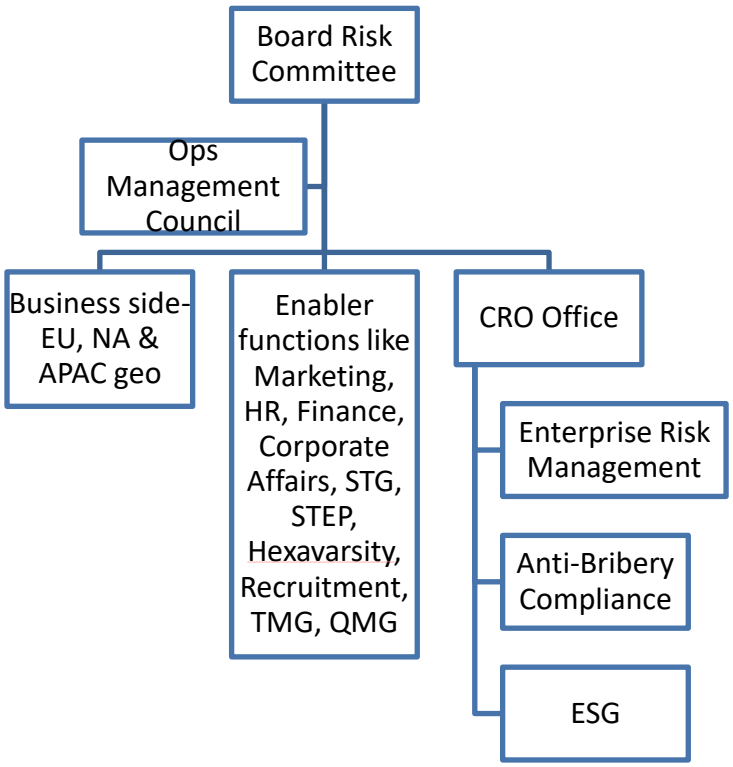
The company's vision for risk management is to have a culture in which risks are managed in an integrated manner that will enable it to:

- Be recognized as a leading organization with best practices; to achieve the vision and mission.
- Be seen as an organization of high ethics that manages its risks responsibly in addition to achieving operational and financial goals.

A well-defined risk governance structure serves to communicate the approach of risk management throughout the organization by establishing clear allocation of roles and responsibilities for the management of risks on a day-to-day basis. As part of Risk Governance, risk management related aspects get discussed in Board Risk Management Committee and Ops Management Council meetings. Ops Management council comprises of CXOs of the company. This ensures that the risk management activities are undertaken as per the policy.

CRO shall appoint Risk Owners from all relevant functions at Hexaware and the Risk Owners would be responsible for establishment and implementation of risk management process effectively in their respective functions.

The diagram below outlines the governance structure for Hexaware: -



Board committees include- Nomination and Remuneration Committee, Audit Committee, Stakeholders Relationship Committee, Corporate Social Responsibility Committee, Risk Management Committee, Environmental, Social and Governance Committee

Enterprise Risk Management is one of the agenda points of Ops Management Council (MC) meeting

2.1 **Board Risk Management Committee**

Composition of the Board Risk Management Committee:

1. Mr. Joseph Mclaren Quinlan, Independent Director (Chairman);
2. Mr. Kapil Modi, Non-Executive Director (Member); and
3. Mr. Alok Chandra Misra, Independent Director (Member)

The role and responsibility of the Risk Management Committee shall be as follows:

- Review, assess and formulate the risk management system and policy of the Company from time to time and recommend for an amendment or modification thereof, which shall include:
  (a) a framework for identification of internal and external risks specifically faced by the Company, in particular including financial, operational, sectoral, sustainability (particularly, environment, social and governance related risks), information, cyber security, compliance and ethics risks or any other risk as may be determined by the Risk Management Committee;
  (b) review of anti-bribery & anti-corruption framework
  (c) measures for risk mitigation including systems and processes for internal control of identified risks; and
  (d) business continuity plan;

- Ensure that appropriate methodology, processes and systems are in place to monitor and evaluate risks associated with the business of the Company;

- Monitor and oversee implementation of the risk management policy, including evaluating the adequacy of risk management systems;

- Periodically review the risk management policy, at least once in two years, including by considering the changing industry dynamics and evolving complexity, and recommend for any amendment or modification thereof, as necessary;

- Keep the Board of the Company informed about the nature and content of its discussions, recommendations and actions to be taken;

- Review the appointment, removal and terms of remuneration of the Chief Risk Officer (if any);

- To implement and monitor policies and/or processes for ensuring cyber security;

- To coordinate its activities with other committees, in instances where there is any overlap with activities of such committees, as per the framework laid down by the Board; and

- Any other similar or other functions as may be laid down by Board from time to time and/or as may be required under applicable law, as and when amended from time to time, including the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015."

The Risk Management Committee shall have powers to seek information from any employee, obtain outside legal or other professional advice and secure attendance of outsiders with relevant expertise, if it is necessary. The Risk Management Committee shall meet at least twice in a year, provided that the meetings of the Risk Management Committee shall be conducted in such a manner that on a continuous basis not more than two hundred and ten days shall elapse between any two consecutive meetings.

2.2 Ops Management Council (MC)

Risk Management topics which get discussed in Management Council meetings-

- Review the organization's risk profile periodically
- Review and assess the current & planned approach to manage key business risks
- Assess and evaluate the key risks anticipated and associated mitigation measures for the organization and suggest new mitigation measures as necessary.
- Ensure that effective risk mitigation plans are in place and the results are evaluated and acted upon.
- Evaluate the Early Warning Indicators for key business risks identified by the Risk Owners
- In case of exigencies / emergent conditions, ensure that the Board is apprised about the same

2.3 Chief risk officer (CRO)

The Chief Risk Officer (CRO) will work with members of Ops MC and risk owners in establishing and implementation of risk management process effectively in their areas of responsibilities.

Roles and Responsibilities of the CRO:

- Manage the establishment and ongoing maintenance of risk management policy pursuant to the organization's risk management vision
- Ensure all the relevant functions are represented in the Management Council
- Validate that the risk management policy is implemented in each department and that all significant risks are recognized, acknowledged, and effectively managed
- Discuss with risk owners and finalize the ownership of risk registers, thereby entrusting the person with the responsibility of completion of the risk register
- Coordinate with risk owners for periodic update of risk registers
- Support the Risk Owner in identifying and assessing risks, creating mitigation plans, and development of early warning indicators

2.4 Risk Owner

Risk Owners shall be the heads of respective function/department/location as decided by Management Council on time-to-time basis depending on the organizational structure and business imperatives so as to ensure that risks pertaining to all critical and significant functions/departments/locations are captured while identifying, assessing, and managing risks. Their name shall reflect as the owner of the respective risk register.

Role and Responsibilities of Risk Owners:

- Risk Owners should ensure that all the risks within their respective functions are identified, assessed, monitored, and managed effectively to ensure that risk management practices are implemented. They should also ensure that processes utilized are in compliance with the entity's enterprise risk management policies.
- Ensure that risks for their respective functions/department/location are identified and assessed
- Ensuring that the risk assessment is done as per the risk assessment framework
- Ensuring risks are managed on a daily basis
- Ensuring risk registers are maintained and updated on a monthly basis & shared with CRO function on a quarterly basis
- Facilitate the identification and implementation of risk mitigation plans
- Development of early warning indicators for key risks identified
- Define L2 EWI's and track them to measure the effectiveness of the mitigation plans
- Reporting the risks along with assessment and mitigation of the respective function to the CRO

Ownership of the most frequently identified risks

Risk	Owner
Information & Cyber Security risk	Chief Information Security Officer (CISO) & Head Cyber Security
Talent availability & retention	Chief People Officer (CPO) & Head Recruitment
Increased cost of services leading to margin erosion	Chief Operating Officer (COO)
Revenue Concentration	Chief Executive Officer (CEO)
Regulatory and Compliance risks	Company Secretary & Compliance Officer
IP infringement & risks related to contract management	Head Legal
Climate change & Sustainability risk	Chief Operating Officer (COO)
Disaster recovery and Business continuity	Chief Information Security Officer (CISO)
Ability to meet delivery commitments	Vertical/Channel heads/VDHs

2.5 Risk coordinators

Based on the needs risk coordinators shall be appointed by risk owners within their function (one or more than one) to assist in the risk management activities.

Role and Responsibilities of Risk Coordinators:

- Assisting the Risk Owner in initiating risk identification and assessments within their area of responsibility
- Taking timely inputs from Risk Owners
- Timely updating and maintaining the risk register for functions as per the inputs from Risk Owners.
- Assist the Risk Owners in development of early warning indicators and mitigation plans

2.6 Risk reporting structure

Risk Owners shall report quarterly to CRO with all the risks identified in their respective functions and the status of the Early Warning Indicators. CRO shall discuss org. risks with the Ops MC on a periodic basis.

3.0 Risk management approach

Risk Management as a process shall enable the organization to identify, assess and treat risks. It is the responsibility of everyone in the organization viz. board, management team and all Hexaware personnel. Risk Management applies to all functions, and operations within the organization.

The plan for managing enterprise level and operational risk is by communicating it to the stakeholders and establishing the connection between the risk management policy and the organization's strategic planning, assessment processes and procedures.

Based on the risk management process, security controls are evaluated for its applicability and effectiveness. Additionally, based on the changes in the environment or prior to any significant change, or after a serious incident, or whenever a new significant risk factor is identified, or at a minimum annually, the risk management process is to be triggered and updating of risk management policy is to be assessed.

In Hexaware, risk management is iterative. An iteration of the risk management process is triggered when e.g.:

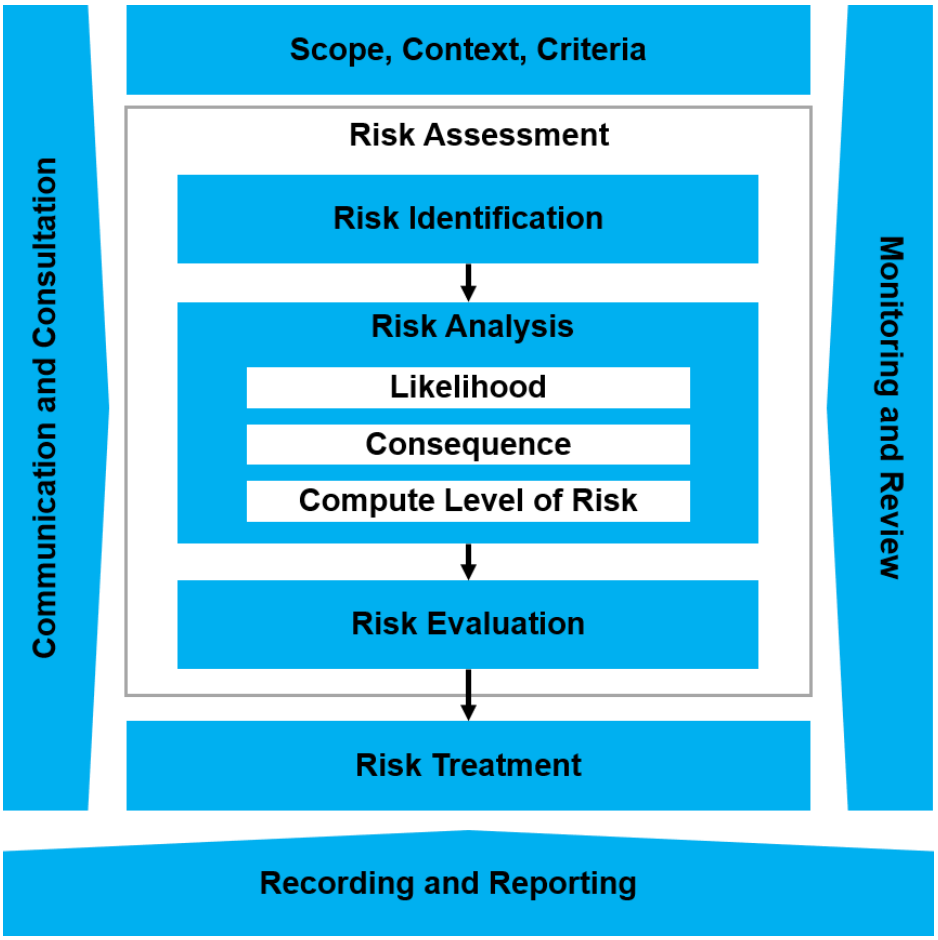
- The business develops a new goal, undertakes a project or investment, or considers its strategy for coming years
- Conditions exterior to Hexaware change significantly, e.g. regulatory or legal changes, major changes in competitive landscape, changes to key partnerships etc.
- Periodic requirements for risk reviews as required by Governing documents, Contracts, legislation, or other sources
- Organization changes/ M&A

The primary objective(s) of establishing a risk management process is to ensure that:

- Risks faced by the organization shall be identified and recorded in the risk register, enabling the top management to take a comprehensive view of the same
- Risks identified shall be assessed, mitigated, monitored, and reviewed on an ongoing basis.
- The level of acceptable risk in the critical infrastructure and business-specific risks is clearly stated.
- Acceptable risk appetite is set that balances risks and opportunities to contribute to the achievement of the organization's strategic objectives.
- Enable the audit committee to assess the effectiveness of the risk management systems which are in place and undertaking independent review of the risk mitigation plans which have been designed for material risks.

Hexaware's enterprise risk management practices are aligned to ISO 31000:2018 & COSO ERM 2017

The Risk Management Process is depicted below:



3.1 Risk identification

Risk identification sets out to identify an organization's exposure to uncertainty. This requires an in- depth knowledge of the organization, the market in which it operates, the economic, legal, regulatory, social, political, technological and cultural environment in which it exists, as well as the development of a sound understanding of its strategic and operational objectives, including factors critical to its success and the threats and opportunities related to the achievement of these objectives.

Risk identification shall be approached in a methodical way to ensure that all significant activities within the organization have been identified and all the risks flowing from these activities defined.

The following methodologies can be used to identify risks:

- Brainstorming
- Surveys /Interviews/Working groups
- Experiential or Documented Knowledge
- Risk Lists - Lessons Learned
- Historical risk event information

Please refer Annexure 1 for risk register template.

3.1.1 Risk categorization

Risk Categories are the defined risks that assist in organizing consistent risk identification, assessment, measurement, and monitoring across the organization. A standardized risk category would help determine the impact of each risk at aggregate/group level. However, this risk category would be updated regularly to incorporate new risks that may arise from time to time.

All the risks that have been identified shall be categorized under the following risk categories - Strategic, Operational, Reporting and Compliance risk.

- Strategic Risk - Risk of loss resulting from business factors. These are risks that arise from an organization's business strategy and objectives. For example, entering a new market or launching a new product/service may have strategic risks associated with them. These risks adversely affect the achievement of strategic objectives and may impair overall enterprise value.

- Operational Risk - Risk of loss resulting from inadequate or failed processes, people and information systems. These are risks that arise from an organization's day-to-day activities and processes. Examples include technology failures, employee errors or supply chain disruptions.

- Compliance Risk - Risk of loss resulting from legal and regulatory factors. These are risks that arise from an organization's failure to comply with laws, regulations or industry standards. Examples include contract disputes, intellectual property disputes, employment law violations, data privacy violations or noncompliance with environmental regulations. Risks related to Hexaware's internal compliance framework such as Anti-bribery & Anti-corruption framework are also covered under this tab

Reporting Risk – Risk arising out of wrong or inaccurate reporting

Other important types of risk

- Information & Cybersecurity risk: Information security risk is the potential for loss or harm to an organization's data and systems from threats exploiting vulnerabilities, impacting confidentiality, integrity, or availability (CIA), while cyber security risk specifically focuses on digital threats like attacks, breaches, and system failures, causing financial, operational, or reputational damage.

- IT/Technological Risk: the potential for negative impacts, like financial loss or operational disruption, arising from the failure, misuse, or security compromise of an organization's technology systems, data, or processes, encompassing areas like cyberattacks, software bugs, hardware failures, and human error, affecting confidentiality, integrity, and availability of information

- Reputational risk: the potential for negative public perception, whether factual or not, to damage an organization's brand, trust, and financial health, leading to loss of customers, revenue, and stakeholder confidence. It stems from various sources, including internal failures (ethical lapses, data breaches), external events (supplier issues, social media backlash), and the perceived response to a crisis, all amplified by instant digital communication.

- Third-party (or vendor) risk: the potential for an organization to suffer negative impacts, like data breaches, financial loss, or operational disruption, due to reliance on external partners (suppliers, vendors, contractors) that have access to sensitive data, systems, or processes. These risks arise because third parties may not have the same strong security or compliance standards, creating vulnerabilities that attackers can exploit to get into your organization

- Financial risk: the potential for loss or negative financial outcomes from investments, business ventures, or financial decisions, stemming from factors like market volatility, credit defaults, liquidity issues, or operational failures, affecting individuals, companies, and governments. It's the possibility of capital loss or failure to meet financial obligations

- Sustainability/Climate change risk: Sustainability risk is the broad potential for negative impacts on organizations from environmental, social, and governance (ESG) factors, while Climate Change Risk is a specific, major component of that, focusing on financial, physical, and transition risks from climate change itself, like extreme weather (physical) or policy shifts (transition) impacting assets, operations, and markets

3.2 Risk assessment

Risk assessment allows an entity to consider the extent to which potential events have an impact on achievement of objectives. Risk assessment is a continuous process. Continuous evaluation should be performed both qualitatively and quantitatively. The goal is to identify the interrelations and enable the management to prioritize the risks.

Regular risk assessment shall be conducted, along with mitigation of risks identified from risk assessment and threat monitoring procedures.

Risk is assessed whenever there are any major or significant changes. The risk management process is integrated with the change management process.

The table below captures the scoring methodology for measuring exposure for each risk at an initial level (unmitigated) and residual level (after mitigation strategies have been implemented). The final risk rating can be obtained from the table based on the values assigned against each of the risks identified.

Measure of Risk Exposure = Impact * Probability

Impact (Low, Medium High)	Probability (Low, Medium High)	Initial & Residual risk rating (Green (Low), Amber (Medium), Red (High))
Low	Low	Green
Medium	Medium	Amber
High	High	Red
Low	High	Green
Low	Medium	Green
Medium	Low	Green
Medium	High	Amber
High	Low	Green
High	Medium	Amber

3.2.1 Detailed guidelines for assessing impact & probability

The risk analysis can be performed qualitatively or quantitatively. The impact assessment can be decided based on the following parameters-

Risk Impact	Quantitative	Qualitative
Low	Less than Rs. 50 Lacs (or $ 66000)	No/ minimal impact on business reputation / operations. The impact of which can be absorbed through normal activity.
Medium	Between Rs. 50 Lacs (or $ 66000) to Rs. 3 Crore (or $ 400000)	Issues impacting the value or reputation / operations of the company. Damaged expected to be limited only to the short run. (Less than 6 months)
High	Greater than Rs. 3 Crore (or $ 400000)	Issues materially affecting the value or reputation / operations of the entire company or the group

Also, one can refer below detailed parameters for impact assessment.

The impact of a particular risk should be assessed on the following areas. If a particular risk impacts multiple areas, the highest rating will be considered.
For example, if a particular risk has a 'High' Financial Impact and a 'Low 'Regulatory Compliance Impact, the final impact rating for the risk will be 'High'

Impact Assessment Parameters			
Rating	High	Medium	Low
Financial	Financial impact (PBT) can be >2% of revenue for the previous year	Financial impact (PBT) could be between 0.5 % to 2% of revenue for the previous year	Financial impact (PBT) will be less than 0.5 % of revenue for the previous year
Business Continuity	Continuity threatened permanently	Continuity threatened temporarily	Continuity threatened for a minor period
Security	Major disruption/ considerable damage to project or operations	Temporary disruption/ some damage to project or operations	Manageable disruption/ no damage to project or operations
Regulatory/ Compliance	Prosecution of Senior Management of the company/ suspension of operations	Major fines and prosecution of the company	No prosecution but imposition of minor fines/ Minor technical non-compliance
Reputation/ Brand	Irreparable damage to company reputation and brand on national/ international level	Localized damage to company reputation and brand	Localized low-level impact to company reputation and brand

Information Technology	Any control issue in IT/systems that may lead to a major: - Breach of sensitive data - Loss of data Integrity - Impairment of Operations	Any control issue in IT/systems that may lead to a moderate: - Breach of data (not considered to be sensitive) - Loss of data Integrity - Impairment of Operations	Any control issue in IT/systems that may temporarily impact operations but will not lead to breach or loss of data integrity
Anti-bribery & anti-corruption	- Proven bribery involving top management, government officials, or large-scale collusion. Bribery risks in high-value procurement, dealings with government officials, or third-party intermediaries in high-risk jurisdictions.	Isolated bribery incidents or facilitation payments in mid-level processes. Risks in charitable contributions, sponsorships, or conflicts of interest without designated approval	Low-value gifts or hospitality breaches without intent to influence decisions.

Probability Assessment Parameters		
High	Medium	Low
• Event expected to occur in most circumstances • Definite history of occurrence • Frequency between once and ten times a year	• Event will probably occur in most circumstances • Probably occur once per decade • History of near miss	• Event may occur, but only under exceptional circumstances. • May happen once per lifetime • Probably occur once in more than a decade

3.3 Risk prioritization

A 3-tier risk prioritization system will be used to provide clarity, accountability, and agility in risk management. This is done to ensure that the most critical risks receive Board/Executive attention, while operational and emerging risks are managed at appropriate levels within the organization.

Tier	Definition
Tier 1	Strategic & Critical: Enterprise-wide risks threatening strategy, reputation, or survival. Business-critical risks with very high impact and high/medium likelihood, high urgency and high importance. Includes risks with potential regulatory, reputation, customer, financial, or enterprise-level impact for its operation. These risks typically exceed risk appetite/tolerance limits. These risks would proactively be discussed (immediately escalated) with Risk Committee of the Board for guidance/information.
Tier 2	Risks disrupting business operations, financial performance, or compliance (not existential) High risks with high/medium impact and likelihood, but managed by senior management-level review and governance . If the trend worsens or thresholds are breached, this would get promoted as tier 1 risk. These will get reported in regular risk committee meetings of the Board
Tier 3	Tactical or Watchlist risks. Localized, routine, or emerging risks managed at project/department level which are tracked in the risk register

3.4 Risk mitigation strategy

There are four common strategies for treating risk. There is no single "best" response strategy, and each risk must be considered on its own merits. Some risks may require a combination of strategies and multiple responses, whereas others may need only one strategy with a single response.

- Risk avoidance/ termination: This involves doing things differently and thus removing the risk (i.e. divestments). This is particularly important in terms of project risk, market risk or customer risks.

- Risk reduction/ mitigation: Reduce or Treat the risk. This is the most widely used approach. The purpose of treating a risk is to continue with the activity which gives rise to the risk but to bring the risk to an acceptable level by taking action to control it in some way through either:
  - ✓ Containment actions (lessen the likelihood or consequences and applied before the risk materializes) or;
  - ✓ Contingent actions (put into action after the risk has happened, i.e. reducing the impact. Must be pre-planned)

Risk acceptance: Accept and tolerate the risk. Risk Management doesn't necessarily mean risk reduction and there could be certain risks within the organization that it might be willing to accept and continue with its operational activities. The organization shall tolerate such risks that are considered to be acceptable, for example:

- ✓ a risk that cannot be mitigated cost effectively
- ✓ a risk that opens up greater benefits than loss
- ✓ uncontrollable risks

It's the role of function head to decide the tolerance level of a risk, and when such a decision is taken, the rationale behind it shall be fully documented based on the exposure impact, the vulnerability impact and effectiveness of the compensatory controls etc. In addition, the risk shall continue to be monitored and contingency plans shall be in place in the event of the risk occurring.

Risk transfer: Transfer some aspects of the risk to a third party. Examples of risk transfer include insurance and hedging. This option is particularly good for mitigating financial risks or risks to assets.

- The following aspects shall be considered for the transfer of identified risks to the transferring party:
  - ✓ Internal processes of the organization for managing and mitigating the identified risks.
  - ✓ Cost benefit of transferring the risk to the third party.

3.4.1 Risk reduction/mitigation

If the risk treatment mechanism selected is risk mitigation or risk transfer for an identified risk then the next step shall be to review and revise existing controls to mitigate the risks falling beyond the risk appetite and also identify new and improved controls.

Risk mitigation process:



Identify controls

New control activities are designed in addition to existing controls post assessment of risk exposure at current level to ensure that the risks are within the accepted risk appetite.

Control activities are categorized into Preventive or Detective on the basis of their nature and timing:

- Preventive controls – focus on preventing an error or irregularity.
- Detective controls – focus on identifying when an error or irregularity has occurred. It also focuses on recovering from, repairing the damage from, or minimizing the cost of an error or irregularity.

Evaluate Controls

The controls identified for each risk event shall be evaluated to assess their effectiveness in mitigating the risks falling beyond the risk appetite.

Implement Controls

It is the responsibility of the function head to ensure that the risk mitigation plan for their function is in place and is reviewed regularly.

Risk tolerance thresholds are defined for each category of risk. Risk reassessment is conducted to ensure management's stated level of acceptable risk is still valid.

In addition to this, the organization shall implement financial & non-financial controls to ensure effectiveness of Anti-Bribery & Anti-Corruption & Anti-Money Laundering framework which is aligned to ISO 37001 Anti-Bribery Management Systems

Some of the Financial controls are listed below*-

- Segregation of duties
- Delegation of authorities
- Revalidating the transaction for details
- Requiring the appropriate supporting documentation to be annexed to payment approvals
- Periodic and independent financial audits and changing, on a regular basis, the person or the organization that carries out the audit.

*The list is not exhaustive

Some of the non-financial controls are listed below*-

- Working with suppliers/third parties from approved supplier list only
- Conducting Due diligence of the third party before on-boarding
- Assessing whether the services were properly carried out by the third partyAwarding contracts, where possible and reasonable, only after a fair and, where appropriate, transparent competitive tender process between at least three competitors has taken place.

- *The list is not exhaustive

4.0 Risk monitoring & review

The Ops Management Council (MC) is the key group which shall work on an ongoing basis within the risk management framework outlined in this policy to mitigate the risks to the organization's business as it may evolve over time.

4.1 Early warning indicators (EWIs)

Early Warning Indicators are rule based quantitative or qualitative triggers based on multiple sources of information for early identification of potentially harmful scenarios. They have the following characteristics

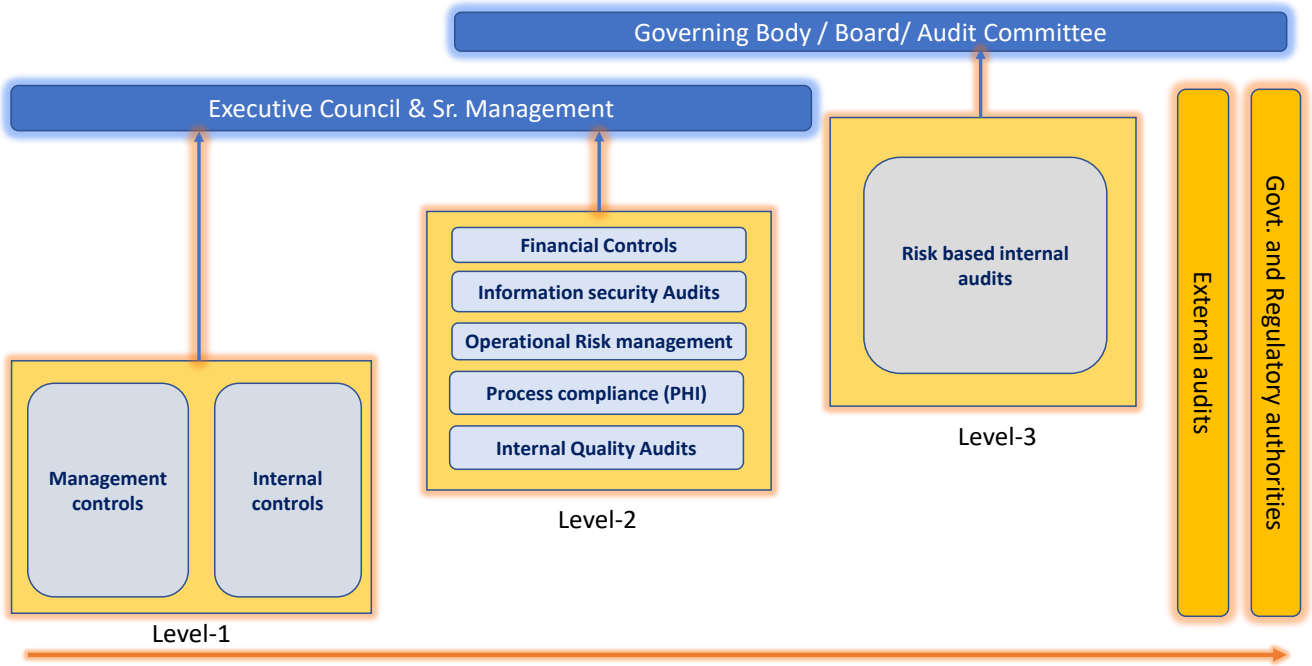
- Rule based triggers - These are triggers to flag risks early based on rules – that can be quantitative (like sharp increase in resource cost) or qualitative (like change in government policies)
- Multiple sources of information - The triggers could be based on internal information like supplies, labour issues, high attrition etc. or external information like changes in travel regulations, macro-economic developments etc.
- There are two levels of EWI's defined Level 1 (Strategic Level), Level 2 (Operational Level). Both the categories of EWI's are tracked using the format provided in Annexure - 3

4.2 Governance, assurance & management reviews

The Three Lines of Défense model distinguishes among three groups (or lines) involved in effective risk management:

Three Levels of Defense - Model

Three Levels of Defense - Model



Level 1: Functions that own and manage risks

As the first line of Défense, operational managers own and manage risks. They are also responsible for implementing corrective actions to address process and control deficiencies. Operational management is responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis.

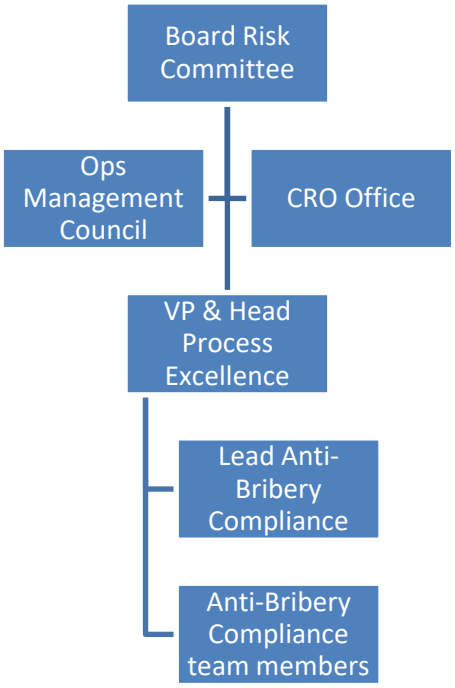
Operational management identifies, assesses, controls, and mitigates risks, guiding the development and implementation of internal policies and procedures and ensuring that activities are consistent with goals and objectives.

Level 2: Functions and processes to oversee risks

Management establishes various risk management and compliance functions to help build and/or monitor the first line-of-Défense controls. Management establishes these functions to ensure the first line of Défense is properly designed, in place, and operating as intended. These functions ensure that information about risks and their management is communicated to all stakeholders.

The Ops Management Council (MC) facilitates and monitors the implementation of effective risk management practices by operational management and assists risk owners in defining the target risk exposure and reporting adequate risk-related information throughout the organization.

CRO office Governance structure



Compliance function under CRO office handles internal compliance framework & external

(regulatory) compliance management.

Internal compliance framework covers aspects like Anti-bribery & Anti-corruption, Third Party management, Interaction with public officials, Gifts, Hospitality & Entertainment, Conflict of interest, Donation & Sponsorship, Conducting due diligences, etc.

In Regulatory compliance management, the compliance function monitors specific risks such as noncompliance with applicable laws and regulations. Hexaware uses "Compliance Manager Tool" which tracks & records applicable legislations, regulations & laws. Compliance owners identified report whether Hexaware is in compliance with the requirements and Compliance approvers identified review the submission of compliance owners. The compliances are classified as per the risk inherent in it. The classifications are-Extreme, High, Medium, Low.

The criteria to arrive at the classification is-

Country	Risk Rating			
	Extreme	High	Medium	Low
India	Extreme has been assumed for: i. Imprisonment/ Detention/ Criminal Liability ii. Closure of business activity (fully/ partially) iii. Cancellation of Permit/ License iv. Disallowing/ Discontinuation of Defaulting Business Activity v. Impact of non-compliance on Directors/ General Manager/ Representative of Company vi. Administrative Punishment	Monetary Fine has been assumed as more than INR 1,00,001/-	Monetary Fine has been assumed between 10,001/- to INR 1,00,000/-	Monetary Fine has been assumed up to INR 10,000/-
USA	Extreme has been assumed for: i) Imprisonment/ Detention/ Criminal Liability ii) Closure of business activity (Fully/Partially) iii) Cancellation of Permit/License iv) Disallowing/Discontinuation of Defaulting Business Activity v) Wrongdoings made public vi) Administrative Punishment	Monetary Fine has been assumed as more than 10,000 USD	Monetary Fine has been assumed as more than 2,000 up to 10,000 USD	Monetary Fine has been assumed up to 2,000 USD

Mexico	Extreme has been assumed for: i) Imprisonment/ Detention/ Criminal Liability ii) Closure of business activity (Fully/Partially) iii) Cancellation of Permit/License iv) Disallowing/Discontinuation of Defaulting Business Activity v) Wrongdoings made public vi) Administrative Punishment	Monetary Fine has been assumed as more than 200,000 MNX	Monetary Fine has been assumed as more than 20,000 upto 200,000 MXN	Monetary Fine has been assumed up to 20,000 MXN
Canada	Extreme has been assumed for: i) Imprisonment/ Detention/ Criminal Liability ii) Closure of business activity (Fully/Partially) iii) Cancellation of Permit/License iv) Disallowing/Discontinuation of Defaulting Business Activity v) Wrongdoings made public vi) Administrative Punishment	Monetary Fine has been assumed as more than 100,000 CAD	Monetary Fine has been assumed as more than 5000 up to 100,000 CAD	Monetary Fine has been assumed up to 5000 CAD
Australia	Extreme has been assumed for: i) Imprisonment/ Detention/ Criminal Liability ii) Closure of business activity (Fully/Partially) iii) Cancellation of Permit/License iv) Disallowing/Discontinuation of Defaulting Business Activity v) Wrongdoings made public vi) Administrative Punishment	Monetary Fine has been assumed as more than 10000 AUD	Monetary Fine has been assumed as more than 2000 AUD Upto 10000 AUD	Monetary Fine has been assumed up to 2000 AUD

UK	Extreme has been assumed for: i) Imprisonment/ Detention/ Criminal Liability ii) Closure of business activity (Fully/Partially) iii) Cancellation of Permit/License iv) Disallowing/Discontinuation of Defaulting Business Activity v) Wrongdoings made public vi) Administrative Punishment	Monetary Fine has been assumed as more than 300000 GBP	Monetary Fine has been assumed as more than 31500 GBP Upto 300000 GBP	Monetary Fine has been assumed up to 31500 GBP
Netherlands	Extreme has been assumed for: i) Imprisonment/ Detention/ Criminal Liability ii) Closure of business activity (Fully/Partially) iii) Cancellation of Permit/License iv) Disallowing/Discontinuation of Defaulting Business Activity v) Wrongdoings made public vi) Administrative Punishment	Monetary Fine has been assumed as more than 400000 EURO	Monetary Fine has been assumed as more than 31,500 upto 400000 EURO	Monetary Fine has been assumed up to 31,500 EURO
Poland	Extreme has been assumed for: i) Imprisonment/ Detention/ Criminal Liability ii) Closure of business activity (Fully/Partially) iii) Cancellation of Permit/License iv) Disallowing/Discontinuation of Defaulting Business Activity v) Wrongdoings made public vi) Administrative Punishment	Monetary Fine has been assumed as more than 100,000 PLN	Monetary Fine has been assumed as more than 30,000 upto 100,000 PLN	Monetary Fine has been assumed up to 30,000 PLN

Germany	Extreme has been assumed for: i) Imprisonment/ Detention/ Criminal Liability ii) Closure of business activity (Fully/Partially) iii) Cancellation of Permit/License iv) Disallowing/Discontinuation of Defaulting Business Activity v) Wrongdoings made public vi) Administrative Punishment	Monetary Fine has been assumed as more than 400000 EURO	Monetary Fine has been assumed as more than 31,500 upto 400000 EURO	Monetary Fine has been assumed up to 31,500 EURO
Belgium	Extreme has been assumed for: i) Imprisonment/ Detention/ Criminal Liability ii) Closure of business activity (Fully/Partially) iii) Cancellation of Permit/License iv) Disallowing/Discontinuation of Defaulting Business Activity v) Wrongdoings made public vi) Administrative Punishment	Monetary Fine has been assumed as more than 400000 EURO	Monetary Fine has been assumed as more than 31,500 upto 400000 EURO	Monetary Fine has been assumed up to 31,500 EURO
Japan	Extreme has been assumed for: i) Imprisonment/ Detention/ Criminal Liability ii) Closure of business activity (Fully/Partially) iii) Cancellation of Permit/License iv) Disallowing/Discontinuation of Defaulting Business Activity v) Wrongdoings made public vi) Administrative Punishment	Monetary Fine has been assumed as more than 1,000,000 JPY	Monetary Fine has been assumed as more than 500,000 upto 1,000,000 JPY	Monetary Fine has been assumed up to 500,000 JPY

Philippines	Extreme has been assumed for: i) Imprisonment/ Detention/ Criminal Liability ii) Closure of business activity (Fully/Partially) iii) Cancellation of Permit/License iv) Disallowing/Discontinuation of Defaulting Business Activity v) Wrongdoings made public vi) Administrative Punishment	Monetary Fine has been assumed as more than 1,000,000 PHP	Monetary Fine has been assumed as more than 50,000 PHP up to 1,000,000 PHP	Monetary Fine has been assumed up to 50,000 PHP
Singapore	Extreme has been assumed for: i) Imprisonment/ Detention/ Criminal Liability ii) Closure of business activity (Fully/Partially) iii) Cancellation of Permit/License iv) Disallowing/Discontinuation of Defaulting Business Activity v) Wrongdoings made public vi) Administrative Punishment	Monetary Fine has been assumed as more than 10,000 SGD	Monetary Fine has been assumed as more than 2,000 SGD up to 10,000 SGD	Monetary Fine has been assumed up to 2,000 SGD
Sri Lanka	Extreme has been assumed for: i) Imprisonment/ Detention/ Criminal Liability ii) Closure of business activity (Fully/Partially) iii) Cancellation of Permit/License iv) Disallowing/Discontinuation of Defaulting Business Activity v) Wrongdoings made public vi) Administrative Punishment	Monetary Fine has been assumed as more than 100,000 LKR	Monetary Fine has been assumed as more than 10,000 LKR Upto 100,000 LKR	Monetary Fine has been assumed up to 10,000 LKR

Dubai	Extreme has been assumed for: i) Imprisonment/ Detention/ Criminal Liability ii) Closure of business activity (Fully/Partially) iii) Cancellation of Permit/License iv) Disallowing/Discontinuation of Defaulting Business Activity v) Wrongdoings made public vi) Administrative Punishment	Monetary Fine has been assumed as more than 20,000 AED	Monetary Fine has been assumed as more than 5,000 AED up to 20,000 AED	Monetary Fine has been assumed up to 5,000 AED

Note- **There may also be risk criteria which may overlap i.e.an issue may pose a reputational risk as well as have a material financial impact.**

The following are the key activities of Risk & Compliance Functions in the ERM framework:

- Supporting management policies, defining roles and responsibilities, and work with different organization entities in setting goals for implementation.
- Identifying known and emerging issues.
- Assisting management in developing processes and controls to manage risks and issues.
- Providing guidance and training on risk management processes.
- Facilitating and monitoring implementation of effective risk management practices by operational management.
- Alerting operational management to emerging issues and changing regulatory and risk scenarios.
- Monitoring the adequacy and effectiveness of internal controls, accuracy and completeness of reporting, compliance with laws and regulations, and timely remediation of deficiencies.

Financial Controls: Corp. Finance function monitors financial risks and financial reporting issues

Project Health Index (PHI): This is performed on a monthly basis by the process consultants for all the projects. The scores are published to the leadership team. This process uncovers the key indicators that helps the Project Manager to identify and controls the risks. This report is reviewed every month as part of the monthly reviews by the vertical delivery heads. The organization level risks identified are shared with the CRO

Account Level Information Security and Governance Audits: This audit helps to identify the risks related to cyber security, data privacy and business continuity. This helps the Sr. management to take some timely measures for mitigating the risks.

Third-Party Vendor Risk Assessments: This assessment is performed once a year to identify the risks associated with third-party vendors and their services and tools implemented in Hexaware environment. The risks identified from this assessment are reported to the leadership team to take appropriate decisions and actions.

Internal Vulnerability & Assessment & Penetration Testing: The internal VAPT is performed on the critical devices / networks/ internet facing applications etc. The findings are classified as Critical, high, medium, and Low. The Internal scanning team ensures to close critical and high findings within the agreed SLA. This ensures an acceptable level of security posture of the organization.

Monthly Reviews- Support functions: The support function performs the self- assessment and publish their dashboard to the function head. Action plans for the critical risks identified are implemented with appropriate approvals from the leadership team. This review includes the compliance requirements as applicable to the respective functions.

As the risk exposure of Hexaware may undergo change from time to time due to continuously changing environment, the risks with their mitigation measures shall be updated on a regular basis.

Level 3. Functions that provide independent assurance Risk Based Internal Audits:

The Risk based internal audit brings in a higher level of independence and objectivity within the organization. This high level of independence is not available in the second line of Défense.

Internal audit provides assurance on the effectiveness of governance, risk management and internal controls, including the way in which the first and second lines of Défense achieve risk management and control objectives. Internal audit actively contributes to effective organizational governance fostering independence and professionalism.

The scope of this assurance function covers Hexaware and its subsidiaries, Business unit/verticals, support functions and their applicable business processes. It includes:

- A broad range of objectives, including efficiency and effectiveness of operations and controls.
- Safeguarding of organizational Hardware/Software assets & environment.
- Reliability and integrity of reporting processes & transactions within the entity.
- Compliance with laws, regulations, policies, procedures, and contracts.
- All elements of the risk management and internal control framework, which includes internal control environment; all elements of an organization's risk management framework (i.e., risk identification, risk assessment, and response); information and communication; and monitoring.

The Chief Risk Officer will ensure adequate coordination and communication between the risk management and Internal Audit functions. This includes discussions with the internal auditors on the scope and coverage and internal audit findings

Daily Status Reviews – Delivery

Hiding risks and/or denying problems can inhibit the future success of the company. Everybody should be encouraged to identify problems and new risks and therefore the project manager must have a positive attitude toward risk. Hexaware management has created a constructive environment / daily status review forum in which all employees feel free to raise concerns and admit mistakes.

External Audits & Assessments:

External auditors, regulators, and other external bodies reside outside the organization's structure, but they have an important role in the organization's overall governance and control structure.

External audits and security and other assessments are performed annually or as per the frequency defined in the standards. These audits and assessments are carried out to measure the effectiveness of the internal audit, assurance reviews and other internal assessments. The first, second and third level of Défense control's effectiveness is measured based on the outcome of these reviews.

Tailoring /Exceptions: In a few cases the second and third level of Défense related activities may be carried out by the same group due to the overlap in the operational responsibilities.

Combined view - Level of Défense



4.3 Communication & reporting

The outcomes of the risk management are published & communicated to the relevant stakeholders across the organization. The timely communication of the outcomes enables the Sr. Management and board to take appropriate decisions. The report is also helping the leaders from the middle management teams to take mid-course corrective actions to reduce the consequences.

Hexaware has open culture environment. Different forums such as Periodic CEO Town-Halls, Leadership Town-Halls, Team connect, HR connects where employees can understand the existing risks and voice out the new/associated risks/impacts if any to the leadership/management team.

5. Climate Risk Management

It is widely recognized that continued emission of greenhouse gases will cause further warming of the Earth and that warming above 1.5° Celsius (1.5°C), relative to the pre-industrial period,

could lead to catastrophic economic and social consequences. For managing climate related risks, Hexaware adheres to practices of "Task Force on Climate-related Financial Disclosures (TCFD)" which is a framework providing guidance on Climate Risk Management. The climate risks will be managed as per the Risk Management process detailed in Section 3. 0 Risk Management Approach.

Climate Risks as per our Risk Management approach

a) Physical Risks (Risks related to the physical impacts of climate change.)

Acute risks	• Cyclone • Floods • Wildfire
Chronic risks	• Heat stress • Water stress

b) Transition Risks (Risks related to the transition to a lower-carbon economy)

Policy & Legal	• Regulatory compliance in regions of operation • Emissions reduction targets of countries and regions of operation
Market	• Customer and investor demand for sustainable business services • Product/Service price variations • Energy efficiency in operations and shift to renewable energy sources • Supplier resilience and practices • Client preferences and standards
Technology	• Proliferation of climate-smart technology and equipment • Energy Efficiency and Performance Optimization
Reputation	• Stakeholder and investor preferences

6.0 Training & awareness

In order to increase the knowledge and competence related to enterprise risk management framework the following activities will be undertaken:

- The CRO shall identify the training needs for all employees and stakeholders from risk

management perspective

- Periodic awareness sessions and end of training assessments for the relevant stakeholders (Risk owners, key members of the support function etc.)
- Periodic Awareness mailers to all employees

7.0 Annexure

Annexure 1: Risk register format

Hex 5692- Enterprise Risk Management Risk Register

#	Risk Description	Risk Source (Internal / External)	Cause	Risk Treatment Category	Stakeholders		Initial Risk Assessment			Controls/ Mitigation plan /Action plan
					Owner	Supported By	Impact (Low, Medium High)	Probability (Low, Medium High)	Initial Risk Rating (Green, Amber, Red)	

Residual Risk after mitigation						Risk Status	Early Warning Indicators
Impact (Low, Medium High)	Probability (Low, Medium High)	Residual Rating (Green, Amber, Red)	Is Risk Treatment required for residual risks? (Yes or No)	Residual Risk Treatment Category	Proposed Action Plan		

Annexure 2: Definitions

Enterprise Risk Management (ERM)

COSO's (Committee of Sponsoring Organization of Treadway Commission) integrated framework defines ERM as:

"Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

Risk

One of the standard definitions of risk accepted worldwide in the domain of enterprise risk management has been framed by Committee of Sponsoring Organization of Treadway Commission (COSO) as a part of its 'Enterprise Risk Management – Integrated Framework' It defines risk as:

'Risk is the possibility that an event will occur and adversely affect the achievement of objectives.'

According to ISO 31000 standards, risk is the "effect of uncertainty on objectives" where an effect is a positive or negative deviation from what is expected.

In line with the above leading practices risk at HEXAWARE is defined as 'the possibility that an event will happen and adversely impact achievement of HEXAWARE's objective'.

Risk Owner

Risk Owner is the person with the accountability and authority to manage a risk.

Risk Coordinator

The risk coordinator is the person nominated by risk owner to assist the risk owner in managing the risk management activities within the domain of respective risk owner.

Risk Identification

Risk identification is the process of identifying the organization's exposure to uncertainty.

Risk Identification is the continuous process that helps the organization to proactively identify the parameters that can negatively /positively /both ways impact the organization / the specific entity of the organization to meet its business objectives.

The organization can use different techniques for identifying uncertainties that may affect one or more objectives. (Refer Risk management guidelines HEX-2224 to get more details on the Risk identification techniques)

Input	Tools	Output
✓ Information from the past ✓ Business /Strategic Plan ✓ Threats, vulnerabilities, capabilities, and opportunities affecting business ✓ Internal / External Factors ✓ Compliance reviews ✓ Risk based internal Audits	✓ Document reviews ✓ Information gathering Techniques (Brainstorming, Delphi, FMEA, etc.) ✓ Taxonomy based risk questionnaire	Risk Register

Key parameters

The following are some of the key parameters that denotes the characteristics of the risk

- Source: The elements/factors that may potentially increase the risk to the business objectives. The following are the key internal and external factors to identify the risk sources

#	Internal	External
1	business objectives, strategies, tactical plans, policies	political & economical changes
2	enterprise governance, organizational structure, roles and accountabilities	operational & socio-cultural factors
3	processes, standards, guidelines followed by the organization	innovations & technological changes
4	people skills and awareness	relationships, perceptions, values, needs and expectations
5	internal assets, systems, tools, applications, and configurations	contractual relationships and commitments
6	customer data handling /Information processed and information flows	external vendor/third-party dependencies
7	cyber security controls and data privacy controls	legal, regulatory implications
8	contractual relationships and commitments;	environment related parameters

- Event: Change of environment / change in regular operational circumstance
- Likelihood or probability: The chances of the risk occurrence
- Consequences or impact: The effect of the risk towards the business objectives (positively, negatively, or both)
- Appetite, Tolerance & Threshold: Appetite is the quantum /amount of risk that the organization is prepared to take / pursue. The threshold is the single point value/ goal/metric, and the tolerance is the variation /range/acceptable level in which the risk appetite can be pursued.
- Risk residuals: The threat a risk poses after considering the current mitigation activities in place to address it and can be an important metric for assessing overall risk appetite. A risk tolerance range for acceptable levels of residual risk is typically set by the committee responsible for risk management oversight.

This means that if a risk's impact on the organization, multiplied by its likelihood of occurring, multiplied by the effectiveness of current mitigation activities falls outside of the level deemed acceptable, then the risk factor is out of tolerance.

Business process owners must then adjust mitigation activities, procedures, or controls in order to keep the residual risk within the defined risk tolerance.

Setting enterprise risk tolerances is a calibration exercise, meaning you need to collect a number of risk assessments for areas known to have high and low risk.

This provides an opportunity to compare residual risk to measurements of known acceptability.

Risk Assessment

Risk assessment is the overall process of risk analysis and risk evaluation. It allows an entity to

consider the extent to which potential risk events have an impact on achievement of objectives.

Annexure 3: Format for reporting Early Warning Indicators (Illustrative)

In order to control the risks effectively, the frequency of monitoring plays an important role.

In order to enable this practice, the early warning indicators are defined with the following parameters

- Reporting frequency
- Source of Data
- Threshold
- Tolerance Range
- Actual value
- Current Status in -Red, Amber, Green

As per the frequency defined, the entity level SPOC's /managers must collect the actual data and measure the current status of the risk appetite.