**Fortis Healthcare Limited**

# Enterprise Risk Management Policy



**Type: Governance Document**
**Effective Date: January 2021**
**Communication Plan: Web**

**Owner: Risk Committee**
**Review Schedule: Annual**
**Privacy Classification: Open General**
**Version: 9.0**

**Custodian: Chief Internal Audit & Risk Officer**
**Last Review: September 2024**
**Doc. No. FHL/ERM/Sept 2024**

## 1. Overview

Fortis Healthcare Limited (‘hereinafter referred to as the ‘Company’ or ‘FHL’ or ‘Group’) is a public listed company and including but not limited to requirements under Companies Act, 2013 (including subsequent amendments) and SEBI (Listing Obligations and Disclosure Requirement) Regulations 2015, is required to have an effective risk management framework.

This document constitutes a policy for the oversight and governance of enterprise risks at the Fortis Healthcare Limited as a holding company overseeing a group of subsidiaries.

Risk is defined as the chance of something happening, measured in terms of likelihood and impact, which may adversely affect the achievement of business objectives.

It is acknowledged that ‘risk’ (or risk-taking) is imperative to the organization’s growth, the Board and Management of FHL also recognize the need to manage the risk exposure in a responsible and disciplined manner. A key factor for a Company’s capacity to create sustainable value is the risks taking ability (at strategic and operational levels) and its effective management.

FHL is committed to an effective system of enterprise risk governance which provides for the sound and prudent management of the organisation in meeting the above objectives within acceptable levels of risk. ERM is recognized as a proactive management tool for anticipating emerging risks and putting in place pre-emptive actions to minimize the effects of uncertainty on the organisation success.

The establishment of a formalized risk framework and risk management process enables the appropriate allocation of resources and support the formulation of strategies for risk optimization and response (which may include risk avoidance, reduction, transfer, etc.). Through its linkage to organizational objectives and business processes, ERM supports the maximization of potential for success.

This document describes the Company’s ERM Policy which refers to the minimum standards (principles) by which the Board and senior management oversee the Group’s ERM Framework. It provides details of the structures, processes, and delegated authorities which the Company has in place to implement the ERM principles across the organisation.

## 2. Objectives

While risk management already exists as an integral part of FHL's business operations and decision making, Enterprise Risk Management ('ERM') serves to put existing practices into a more structured, disciplined, coherent, systematic, and documented framework.

ERM enables management to create and sustain a risk-conscious culture, where there is a high degree of organization-wide awareness of risks, but not averseness to risks. Risk features as a key consideration in business planning, decision, and day-to-day operations.

By clearly defining terms and outlining roles and responsibilities, ERM promotes accountability and processes of self-assessment and continuous improvement.

The key objectives of the ERM policy are to:

- Create common language and understanding of the risks
- Facilitate informed decision making where business opportunities are assessed without exposing the business to an unacceptable risk
- Provide a comprehensive ERM framework to have visibility on company's risk profile (internal & external) through effective identification, assessment, treatment, and monitoring
- Establish common Terms of Reference including the structure, methodology, roles and responsibilities and processes for implementing ERM
- Methodology, process and systems are in place to monitor and evaluate risk(s)
- Improve compliance with applicable laws & regulations



## 3. Scope and Applicability

Business strategy, objectives, initiatives, operations across locations, partnerships, collaborations and outsourcing, management activities determine the scope for the ERM.

The applicability of the ERM Policy are as follows:

i. **Board of FHL**: The adoption of the ERM Policy by the Board and custodianship by the board level Risk Committee (RC) clearly demonstrates a high degree of emphasis and commitment.

ii. **Management of FHL**: The ERM Policy provides guidance to management on their position in managing strategic and business risks. Management will use the ERM Policy as a basis for decision making at strategic, tactical, and operational levels.

iii. **Employees of FHL**: The ERM Policy underpins the development of a productive risk culture in FHL. Rightfully, it should complement other existing policies (e.g. Code of Conduct) in guiding the thought-process, actions, and behaviours of all employees.

iv. **Business Partners:** This refers collectively to business partners, outsourcing partners, or any external entities with the ability to significantly impact FHL's business and operations. Whilst the ERM Policy may not be directly adopted by Key Business Partners, it is expected that these entities/ organizations have similar policies/practices to adequately safeguard FHL's interests.

## 4. ERM Principles

### 4.1 Board and Management Commitment

(a) The Board will provide an effective governance oversight over the adoption and implementation of the ERM Policy, including structure, oversight, and reporting.

(b) The Board will formalize a Board risk committee to provide focused support and expertise in managing its ERM accountabilities. The Board risk committee mandate, composition and operational procedures will be appropriately authorised, defined, documented, and overseen effectively by the Board

(c) The Management of FHL is committed to the effective adoption and implementation of the ERM Policy with defined process, roles, responsibility, accountability throughout the organization.

### 4.2 ERM Strategy

(a) Derive tangible and sustainable benefits for the organization.

(b) Create a culture that embraces confident risk-based decision making, albeit in a transparent and accountable manner. All decisions to be assessed and evaluated per risk appetite and tolerances.

(c) Adopt collaborative approach to manage risks in an integrated, holistic, and inclusive manner.

(d) Adequate and effective control and oversight exercised respectively by the Board and senior management that is consistent with their respective roles

(e) Integrated systems and controls to ensure sound, effective and prudent management of the business without inappropriate risk taking or assuming risks without taking account of the potential consequences

(f) Institute reasonable processes to reduce the likelihood, impact, and possible duration of disruption to the continuity of operations and have in place appropriate arrangements to ensure that business continue to function and meet its business, legal and regulatory obligations in the event of anticipated or unforeseen disruption.

(g) Transparent communication and disclosures to external parties (shareholders, regulators, etc.), to the extent deemed appropriate and relevant.

### 4.3 ERM Framework

(a) Implementation of a framework for managing enterprise-wide risks in a structured manner.

(b) All risk management-related activities and processes implemented at corporate, subsidiary and Unit levels shall be aligned to the framework.

(c) Review ERM framework annually to ensure relevance to FHL's operating environment. The review will be led by the Risk & IA function, and endorsed by the management, reviewed by the board Risk Committee, and approved by the Board of FHL.

### 4.4 ERM Oversight Structure

(a) To facilitate informed decision-making on risks, a governance structure with clearly defined roles and responsibilities for all ERM activities shall be defined.

(b) Risk oversight structure shall operate as an integral part of the existing management and board governance structure.

(c) The board Risk Committee acts as the body to oversee the risk management process as per the Terms of Reference approved by the board.

(d) Risk & Internal Audit department is responsible to facilitate the development, implementation, and continuous improvement of the ERM framework. While the risks are owned and manged by business, risk function will collaborate with risk owner(s) for identification of current and emerging risks to formulate risk mitigation solutions.



(e) The Risk Oversight Structure will drive and facilitate risk ownership and accountability. Risk owners supported by other functional owners to take accountability for FHL's key risks and mitigation.

# 5. ERM Policy

## 5.1 ERM Architecture

An Enterprise Risk Management (ERM) Architecture has been defined which will serve basis to implement risk management process. All risk management related activities and processes at Corporate, Functional and Unit levels will be aligned with the principles and guidelines set out in the ERM Architecture.

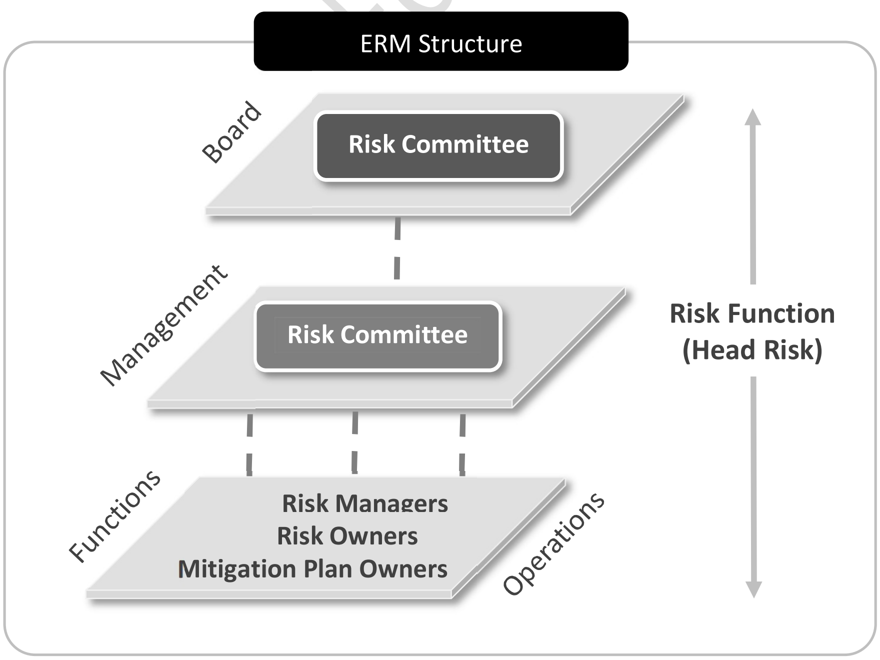
The FHL risk management architecture framework outlines the series of activities and their enablers to identify, assess, mitigate, and monitor risks across the organisation.

The ERM Architecture at FHL comprises essentially of 2 elements:

- Risk Management Structure i.e. the enablers that are created to operationalize the process. These take the form of roles & responsibilities, reporting etc.
- Risk Management Process i.e. the process to identify, prioritize and managed risks in the Company;

## 5.2 Risk Management Structure

For effective implementation of the policy, an ERM structure has been defined with mandate, role, responsibility, and reporting requirements.



The role of each component in the risk management structure is listed below:

**a. The Board**

The board sets the strategic plan for the business, ensures that resources are in place to meet its objectives, and reviews management performance. Board facilitates optimal framework for risk management to,

- Protect Company brand & reputation
- Ensure approach to risk management is consistently applied
- Ensure management assure that risk has been identified, assessed and all reasonable steps taken to manage it effectively and appropriately; and
- Endorse risk related disclosure documents.

The Board of Directors of FHL shall constitute a board level Risk Committee and mandate the roles and responsibilities of the committee and delegate monitoring and review of the risk management plan to the committee.

Board may delegate additional functions as deemed necessary from time to time.

**b. Board Risk Committee**

- To review and amend risk management plan and enterprise risk management policy and procedures
- To monitor the Company's risk profile covering all risks
- To obtain reasonable assurance from the Management that all known and emerging risks have been identified
- To review and provide inputs on the measures/ action plan taken by the management to mitigate the key/material/ emerging risks
- To review and assess the effectiveness of the Company's risk assessment process and recommend improvement wherever appropriate
- To ensure that an appropriate risk reporting structure is established to facilitate reporting of risks to the Board
- To recommend to the Board its findings and propose course of actions to be taken to ensure controls are put in place to address the identified risks
- To communicate with Audit Committee at least once a year to exchange information and coordinate on issues related to risks and internal controls.

**c. Management Risk Committee**

- Oversee execution of ERM program across organization
- Define organization risk appetite and tolerance levels
- Provide inputs on the risks identified across functions and operations and its measurement
- Facilitate identification and assessment of emerging risks
- Support risk identification and assessment for operating strategy, new programs and initiatives
- Assess adequacy of the risk mitigation plans
- Provide oversight on implementation of risk migration plans
- Oversight on documentation of identified risks as per risk register template
- Review and recommend changes to the risk management policy
- Provide an update to the board risk management committee

**d. Function / Operations Head**

Function / Operations Head is responsible for risk management in their area with the responsibility to:



- Comply with risk management policies and procedures
- Support risk function in promoting risk management culture
- Identify risks in line with business and operating strategy considering external and internal factors
- Scan the functional and operating landscape to identify emerging risks
- Assess the risk as per the ERM framework to prioritize the risks
- Report on risk performance targets / indicators
- Report risks and mitigation strategies

**e. Risk Owner**

Each risk is assigned to a 'Risk Owner'. The Risk Owner has the responsibility for ensuring that the risks are within the defined risk appetite. The role of the risk owner includes:

- Identify risk specific root causes and existing mitigation strategies
- Identify gaps in the mitigation strategies and develop improvement plan
- Document the risk mitigation strategy with accountability and timelines

- Review implementation status of mitigation plans with Mitigation Plan Owners and recommend corrective action where required
- Provide a formal assessment on risk mitigation

**f. Mitigation Plan Owner**

Risks may have one or more risk response strategies. The implementation of the mitigation strategy/plan is entrusted to the Mitigation Plan Owners ('MPO'). The MPO is responsible for:

- Contribute to design of the mitigation plans
- Own implementation of mitigation plans
- Provide update on the effectiveness/stage of implementation of the mitigation plan to the Risk Owner; and
- Provide inputs to identify new risks.

**g. Risk Function (Head Risk)**

Risk function is responsible for initiating and coordinating activities for operationalising the risk management framework.

FHL has designated Head – Risk & Internal Audit to coordinate the deployment of risk management framework, he is supported by risk management committee, functional Heads & risk owners. The Functional Heads & Risk Owners have the primary responsibility to manage the risks in the organization. The role of risk function is support to the risk management committee, functional heads & risk owners in:



- Maintain and update the ERM Policy as per risk committee direction
- Implement ERM policy & process across the organization
- Engage with risk committee and management to identify emerging risks and obtain inputs on the critical risks
- Participate in management discussion to understand internal and external factors influencing risk exposure
- Facilitate and manage ongoing risk identification and prioritisation across company operations & functions
- Engage with risk committee and management to identify emerging risks and obtain inputs on the critical risks
- Facilitate documentation of risks register (including mapping of risks to the categories as per the risk classification framework)
- Support Functional Head to finalise the risk register

- Facilitate the risk assessment exercise including risk prioritization
- Facilitate Functional Head/Risk Owners to document the risk mitigation plan, to include assessment of adequacy of defined mitigation plans and self-assessment of adherence to defined mitigation plans.
- Consolidate results of risk assessments across the functions to be presented to the Management/Board Risk Committee
- Provide independent assessment on the adequacy and effectiveness of the risk mitigation plans

### 5.3 Risk Management Process

The enterprise risk framework is based on the COSO ERM framework and include following components:


a. Setting the Context

Strategic business intent is integral to the risk management program to set the right context for risk identification and assessment.

The focus is on establishing relationship to the FHL overall strategic plan – why are we in this business and what is our purpose. This step involves understanding the vision, goals, business strategy and structure of the organisation to identify its objectives and areas that it seeks to safeguard.

The risk function shall obtain an understanding of the business objectives and management priorities through discussions with the Executive Management, Functional Heads, inputs from risk committee, review of strategy documents.

Scan of internal and external factors which influence movement in our strategic direction set the context for identification of relevant risks, and it may include, among other:

- Understanding long/medium/short terms plans,
- Key drivers of business strategy,
- Specific business initiatives which will have impact on organization strategic direction
- Country specific economic/regulatory/policy/political outlook
- Healthcare industry specific growth/regulatory outlook
- AOP & budgets

b. Risk Identification

Risk identification is the process of finding, recognising, and describing risks based on objectives. It is an exercise to identify potentially significant events that may prevent the achievement of objectives as unidentified risks which may pose major threats at an organization/ functional/ process level.

The process is enabled through at creating/updating risk definitions to ensure understanding of the potential threat across all levels of the organization and have commonality of the understanding.



Based on the business factors, risks shall be identified/revalidated at an entity/ functional / operating level. Existing risk library, operation data, AOP, business Intelligence and internal audit report serve as an input for risk identification.

For effective risk program, it is important to identify and assess most relevant risks in view of the external & internal operating environment, strategic direction, strengths, and weaknesses.

i. Risk Category

Under the ERM framework, following risk categories have been defined. All identified risks shall be categorised in one of the risk categories.

- Strategic
- Operational
- Clinical Quality & Patient Safety
- Financial
- People & Culture
- Cyber & Technology
- Government & Regulation
- Workplace Safety & Health
- Environment, Social & Governance (ESG)
- Black Swan

ii. Risk Classification

Risk Classification Framework shall be used to create a common understanding of risks and to differentiate between the risk, its causes, and eventual effects. The risk classification is provided in the *Appendix 1*.

iii. Risk Universe

To support functional and operating management in risk identification, a risk universe has been documented to provide with an inventory of the theoretical risks. Risk universe only serves as a guide to the management to identify the risk environment. Continuous inputs from the business will keep the risk universe dynamic and relevant.

The quality and completeness of the risk identification is the responsibility of the management, respective function and operating leaders and reviewed by the Executive Management. All risks need to be assessed comprehensively to determine its relevance to the organization.

Each identified risk shall be assigned a risk owner responsible for overall risk management of the identified risk.

Risk function shall facilitate the risk identification exercise, work along with the management to identify risks relevant to the organization.



c. Risk Assessment

Identified risks shall be assessed for the probability of occurrence and its impact (severity) on the organization. The probability and impact assessment criteria are defined as:

| Probability | Impact |
|---|---|
| Almost Certain | Severe |
| Likely | Major |
| Possible | Moderate |
| Unlikely | Minor |
| Remote | Insignificant |

Guidance on the risk assessment criteria is provided in the *Appendix 2*.

i. Risk Appetite

The risk appetite is the amount of risk to be taken in the pursuit of its strategic business objectives. The risk appetite determines what risks are acceptable and is intrinsic to the evaluation criteria used to measure identified risks.

What is considered as an acceptable level of risk has been determined through a consideration of the expectations/concerns of key stakeholders, both internal and external. These are then expressed in the risk assessment criteria outlined in the likelihood and impact matrix in *Appendix 2 & 3*.

Risks should be managed to an 'acceptable' level, defined by risk appetite. The defined risk appetite is intended to be a guide. The Management will evaluate all its business decisions and weigh all considered risks against the expected returns.

The following statements of risk appetite are intended to direct any decisions that are being made about enterprise risks and opportunities. They represent the key areas that the risks and opportunities will impact and are articulated in the form of the outcomes expected from the level of risk company is prepared to take.

The company operates within a low overall risk range. The lowest risk appetite relates to patient safety and compliance objectives, with a marginally higher risk appetite toward its strategic, and operations objectives. Reducing to reasonably practicable levels the risks originating from various medical systems, products, equipment, and our work environment while meeting our legal obligations will take priority over other business.



Strategic Risk Appetite: Not to accept risks that will impair company's ability to respond to changes in the external environment and /or impair its ability to develop and maintain positive stakeholder relationships to support brand and reputation. This includes any external factors relating to industry changes or events. Proactive management of internal and external factors are critical to minimize unintended consequences.

Governance Risk Appetite: Manage the risks arising from its decision-making structures to ensure that it maintains positive stakeholder relationships, appropriate information flows and effective change management to minimise the variance between expected and actual group performance targets

Financial Risk Appetite: To manage the risks of its business activities so as not to impair its ability to continue as a going concern whilst optimising shareholder returns within forecast profitability targets.

Operational Risk Appetite: To maintain highest standards for patient and staff safety and have zero tolerance for the non-reporting of patient and staff safety incidents. It will maintain zero tolerance for the non - reporting of compliance breaches with safety and security regulations.

Manage the risks of business activities so that operations are maintained to ensure the delivery of quality services to support its forecast profitability targets, compliance with legislative, regulatory and safety standards.

ii. Risk Prioritization

Risk assessment will assist in prioritizing the risks based on its probability and impact and shall be classified into:

| | |
|---|---|
| Serious: | Close attention required |
| Significant: | Rare but need contingency Plan |
| High: | Further action required to bring down the risk |
| Medium: | Risk is manageable and within acceptable level |
| Low: | No action required |

The guidance on the risk assessment matrix in given in the *Appendix 3*.

d. Risk Treatment

Risk treatment options (4Ts) are as follows:

- Terminate: deciding not to proceed with the activity that introduced the unacceptable risk, choosing an alternative more acceptable activity that meets business objectives, or choosing an alternative less risky approach or process
- Tolerate: making an informed decision that the risk rating is at a tolerable level. No further action is taken to treat the risk. However, ongoing monitoring of the risk should be done to ensure it is within acceptable limits
- Treat: implementing a risk action plan to either treat and reduce the likelihood or consequence of the risk to an acceptable level; and
- Transfer: – deciding to transfer the risk with a third-party service provider when the organisation does not have the in-house expertise or competency and/or purchase insurance to share part of the risk exposure.



Respective risk owners to:

- Finalize risk treatment option for each risk
- Propose and identify risk mitigation plan(s) with ownership and implementation timelines
- Plan target residual risk rating by taking into consideration the proposed risk action plan (including the existing risk controls)

e. Risk Mitigation

To manage the prioritize risk, appropriate response plan shall be prepared and documented. The existing controls in place to manage the identified risk shall be documented and may also include the additional mitigation steps required to manage the risk and bring the severity to an acceptable level as per the defined risk appetite.

To identify the reasons/drivers for the risk intensity root cause analysis shall be performed with respect to organization design, assessment of existing processes and controls, management controls. Additional mitigation plans shall be developed to address the open risk position with defined ownership and implementation plans.

The Risk Owner has the overall responsibility and ownership for the quality and completeness of the mitigation plans. Respective "Risk Owners" in consultation with process owners (within or across functions) will identify the root cause; assess existing management controls and improvement opportunities.

"Risk Owners" will document the mitigation strategy (considering existing and proposed activities) with timelines and responsibilities.

f. Risk Register

Identified and prioritized risks shall be documented in a Risk Register. The risk register details the risk, its classification, assessment its potential area of impact, ownership and functions that may play a role in managing it.



Format of the risk register is provided in the *Appendix 4*.

g. Risk Monitoring

Risks that have been identified, assessed, and measured, progress towards objectives needs to be tracked. Monitoring must be on-going and can prompt re-evaluation of the risks and /or changes in responses. Monitoring is carried out proactively and is wider than just reporting.

The risk monitoring assist in identifying emerging risks which can adversely impact the business objectives, extent of implementation of the mitigation strategies and efficacy of risk mitigation.

i. Key Risk Indicators (KRIs)

An effective tool for monitoring risks is the development and implementation of key risk indicators (KRIs). KRIs are metrics used by the Group to provide an early signal of increasing risk exposures.

In some instances, they may represent key ratios that management track as indicators of evolving risks, and potential opportunities, which signal the need for actions that need to be taken.

KRIs are distinct from key performance indicators (KPIs) which are designed to provide a high-level overview of the performance of the organisation and its major operating units. KPIs, generally, do not provide an adequate "early warning indicator" of a developing risk because they mostly focus on results that have already occurred.

h. Risk Reporting

The frequency of risk reporting shall be in line with risk monitoring activities and other business reporting such that KRIs.

All risk information shall be reported as per the defined frequency and reporting. The reports shall provide:

- critical entity level risks facing, or potentially facing
- major risk events/loss experience, issues identified and intended remedial actions
- the status and/or effectiveness of actions taken; and
- exception reporting (covering among others authorized and unauthorized deviations from the ERM Policy and likely or actual breaches in predefined thresholds for risk exposures and losses).

i. Key Risk Escalation Criteria

To ensure that the ERM process structure operates efficiently, a risk escalation process shall be in place to provide an early notification to management of:

- Risks that have been identified as demonstrating a materially adverse trend
- Newly identified material risks which are likely to materialise in the short term
- Significant risks that have materialised
- Significant risk control failures
- Breaches of Policy, including breaches of risk appetite limits; or
- Significant risk losses incurred or likely to be incurred.

The risk escalation process is also used to determine which risks require management at a higher level through a set of risk escalation criteria based on the impact of the risk.

## Appendix 1: Risk Classification Framework

| Primary Risk Category | Secondary Risk Category | Tertiary Risk Category |
|---|---|---|
| Strategic Risk | Community / Consumers | Demand shift |
| | | Needs/ Preference Change |
| | | Public Health |
| | Economic | |
| | Market Share | Business portfolio |
| | | Business model/ strategy |
| | | New/ Unexpected Competitor |
| | | Marketing Strategy |
| | | Investment Evaluation |
| | Technology | Disruptive technology |
| | | Changes / Trend shifts |
| | Reputation | Branding |
| | | Stakeholder perception |
| | | Intellectual property |
| | Organisation Structure | Merger Integration |
| | | Leadership Change |
| | | Resource allocation |
| | | Planning |
| | | Change readiness |
| | Globalisation | Partnering |
| Operational Risk | Catering & Food Hygiene | Food Delivery |
| | | Food Safety & Hygiene |
| | | Food Supplies & Storage |
| | | Premises equipment |
| | | Preparation & Production |
| | | Washing / Sanitising |
| | Hospital Security | Information Security |
| | | People Security |
| | | Property Security |
| | Housekeeping Services | Cleaning |
| | | Disinfection |
| | | Pest Control |
| | Laundry & Linen | Compliance with regulation & hospital policy |
| | | Washing detergent / chemical |
| | | Delivery Timeline |
| | Supplier Risk | Key Supplier |
| | | Competitiveness of pricing |
| | | Delivery Timeline |
| | | Accuracy of invoicing |
| | | Supplier Performance |
| | Supply Chain | Market Dynamics |
| | | Product / Service |
| | | Supply Chain disruption |
| | | Technological trends |
| | Pharmacy | Formulary |
| | | Forecasting clinical needs |
| | | Product quality |
| | | Supply continuity |
| | | Supplier Performance |
| | | Medication Storage |
| | | Product Scoring |
| | Third Party Vendor Management | Contract commitment / scope of service |
| | | Performance gap |
| | | Blunders / Mishaps / Lapse in services |
| | Project / Renovation Risk | Major Capital Works |
| | | Major IT Project |
| | | Project Management - timeliness, cost, quality |
| | | Contract administration |
| | | Regulatory / Authority approval |
| | | Compliance with regulatory / ESH / hospital policy |
| | | Interruption of hospital services |
| | Communication & Reporting | Internal mandatory reporting |
| | | Miscommunication / communication breakdown |
| | | External reporting |
| | Facility & Engineering | Maintenance |
| | | Engineering and Building Systems |
| | | Utilities |
| | | Equipment Breakdown |
| | | Medical Equipment/ Devices Technology |
| | | Medical Equipment/Devices Utilisation |

| | | |
|---|---|---|
| | Diagnostics (Lab/Radiology) | Image/Specimen quality / suitability |
| | | Image/ Specimen Integrity |
| | | Result Reliability / Accuracy |
| | | Management and notification of critical findings |
| | | Report turnaround time |
| | Logistic & Support | Delivery accuracy & timeliness |
| | | Parking |
| Clinical Quality & Patient Safety Risk | Access to Services | Bed Management |
| | | Clinical Service Planning / Capacity |
| | | Waiting time / triage / queue management |
| | | Telemedicine |
| | Care Delivery | Appropriate Care |
| | | Timeliness |
| | | Assessment |
| | | Clinical Outcomes |
| | | Community Care |
| | | Consent |
| | | Diagnostic |
| | | Discharge |
| | | Missing / absconding patients |
| | | Nutrition / Catering |
| | | Pain / Sedation |
| | | Patient Transfer / Clinical Handover / Communication |
| | Patient Needs | Language and Communication |
| | | Patient Experience |
| | | Patient rights |
| | | Grievance Management |
| | | Special Needs |
| | Patient Safety | Blood / blood products |
| | | Clinical Deterioration |
| | | Clinical Complications / Adverse outcome |
| | | Hospital acquired conditions/ Injuries |
| | | Medical Device Related Complication (non infectious) |
| | | Medication Safety |
| | | Patient behaviour |
| | | Patient identification |
| | | Falls |
| | | Restraint related injuries/ complication |
| | | Surgical Safety |
| | Prevention and Control of Infection | Hospital Acquired Infections |
| | | Surgical Site Infection |
| | | Outbreak |
| | | Medical device related infection |
| | Continuity of care | Social determinants of health (discharge planning) |
| | | Referrals |
| | | Transition of Care |
| | | Follow-up/education |
| | Record keeping | Documentation |
| | | Digital Recording |
| | | Filing & compiling of records |
| | | Retrieval & access to Medical Record |
| | Case Management | Investigation |
| | | Patient/Family Engagement |
| | | Service Recovery |
| | Quality Standards | Clinical Accreditation |
| | | Other Accreditation |
| | Research | Clinical trials |
| | | Ethics |
| | Medico-legal | Medical Errors / Negligence |
| | | Vicarious liability |
| Financial Risk | Financial Accounting | Accounting Systems |
| | | Assets |
| | | Billing / Pricing / Bad Debts |
| | | Financial Reporting |
| | | Income/ Expense |
| | | Liabilities |
| | | Debtor/creditor management |
| | | Payroll Accounting |
| | Financial Planning | Funding /Loan |
| | | Reserves/Cash Pooling |
| | Insurance | Coverage / Claims |
| | Management Accounting | Budget / Forecast Utilisation Control |
| | Treasury | Bank Accounts |
| | | Cash Flow Management |
| | | Interest Rates |

| | | |
|---|---|---|
| | | Foreign Exchange |
| | Taxation | Corporate Tax / Indirect Tax and Transfer Pricing |
| People & Culture Risk | Talent | Labour Market |
| | | Performance gap |
| | | Physician Engagement |
| | Performance Measurement | Information for Decision Making |
| | | Monitoring Performance |
| | Staff Development | Professional Staff development & qualifications |
| | | Training and development |
| | Staff Engagement | Staff grievances |
| | | Staff relations / Communications |
| | | Staff welfare |
| | Workforce Management | Recruitment |
| | | Remuneration / Benefits/ Recognition |
| | | Competency |
| | | Leadership Development |
| | | Resignation / dismissal / Retirement / redundancy |
| | | Retention |
| | | Workforce / Succession Planning |
| | | Workforce Scheduling |
| Cyber & Technology Risk | Communication | Telecommunications (ie phones) |
| | | Messaging (SMS, Whatsapp, etc) |
| | Information Management | Application Systems |
| | | Accessibility/ Availability (Redundancy) |
| | | Interoperability |
| | | Disruptions / Disaster Recovery |
| | | Data Centre |
| | | Data Integrity / Loss |
| | | Hardware |
| | | Infrastructure / network |
| | | IT Governance |
| | | Software |
| | | Technology |
| | | Cloud |
| | Cyber Security | Data Privacy |
| | | System security breaches |
| Workplace Safety & Health | Occupational Health & Safety | Electrical Safety |
| | | Injury (Physical, Chemical, Clinical, etc) |
| | | Manual handling/ Ergonomic / Occupational |
| | | Radiation Safety |
| | | Slips / Trips / Falls |
| | | Infection Risk / Biological |
| | | Psycho-social |
| | | Work Environment |
| | Facility Security & Safety | Facility Safety |
| | | Medical Equipment Safety |
| | | Fire Safety |
| | | Security Technology |
| | Hazardous Material & Waste | Conservation / Pollution |
| | | Hazardous substances |
| | | Hospital waste |
| | Renovation | Safety |
| | | Noise / Air Quality / Vibration |
| | Physical Environment | Buildings |
| | | Grounds |
| | Contingency Planning | Internal Disaster Planning |
| Government and Regulation Risk | Contractual | Administration |
| | | Product Liability |
| | | Overlooked deadlines/ expiration |
| | | Terms and Conditions |
| | Litigation | Medical malpractice |
| | | Directors and Officers Liability |
| | | Adverse publicity leading to reputational impact |
| | | Public Liability |
| | Statutory and Regulatory Requirements | Professional Code of Practice / Conduct |
| | | Corporate compliance |
| | | Facilities and Services Legislation |
| | | Tax compliance |
| | | Service Deed |
| | Accountability | Performance Reporting |
| | Copyright and trademarks | Branding Value Protection |
| | Data protection | Use of data |
| | Integrity | Internal Fraud |
| | | Illegal Acts |
| | | Ethics/Morale/ Behaviour |

| | | |
|---|---|---|
| | Bribery & Corruption | False claims for payments |
| | | Bribery of Government Officials / Authorised Bodies |
| | | Procurement fraud |
| | | Bribery or excessive hospitality to secure business opportunities |
| | | Obtaining excessive corporate contributions & sponsorships |
| | | Obtaining inducements |
| | | Asset misappropriation by employees |
| | | Misuse of rank, authority, or position |
| | | Compliance with ABC Policy |
| | Political Climate | Change in laws, regulations, and government policies |
| Environment, Social & Governance Risk | Stakeholder Management | Stakeholder pressure |
| | | Supplier Related |
| | Leadership | Corporate Direction |
| | | Board of directors |
| | | Clinical Leads & Physician Alignment |
| | Authority | Delegation of Authority |
| | | Matters reserved for Board |
| | Environment | Greenhouse Gas (GHG) Emission |
| | | Air Quality |
| | | Energy Management |
| | | Waste & Hazardous material management |
| | | Water Management |
| | | Climate change |
| | Social | Human Rights & Community Relations |
| | | Customer protection |
| | | Customer welfare |
| | | Labour practices |
| | | Diversity |
| | | Inclusion |
| Black Swan | Business Continuity and disaster recovery (External disaster) | Pandemic/ Disease outbreak |
| | | Catastrophe (Mass Casualty) |
| | | Natural Disaster (Flood/Fire/Etc) |

## Appendix 2: Risk Assessment Framework

The following criteria serve as a guide. Management and Risk Owners are to select the most appropriate criteria, depending on the risk being assessed.

Risk Probability Assessment Criteria

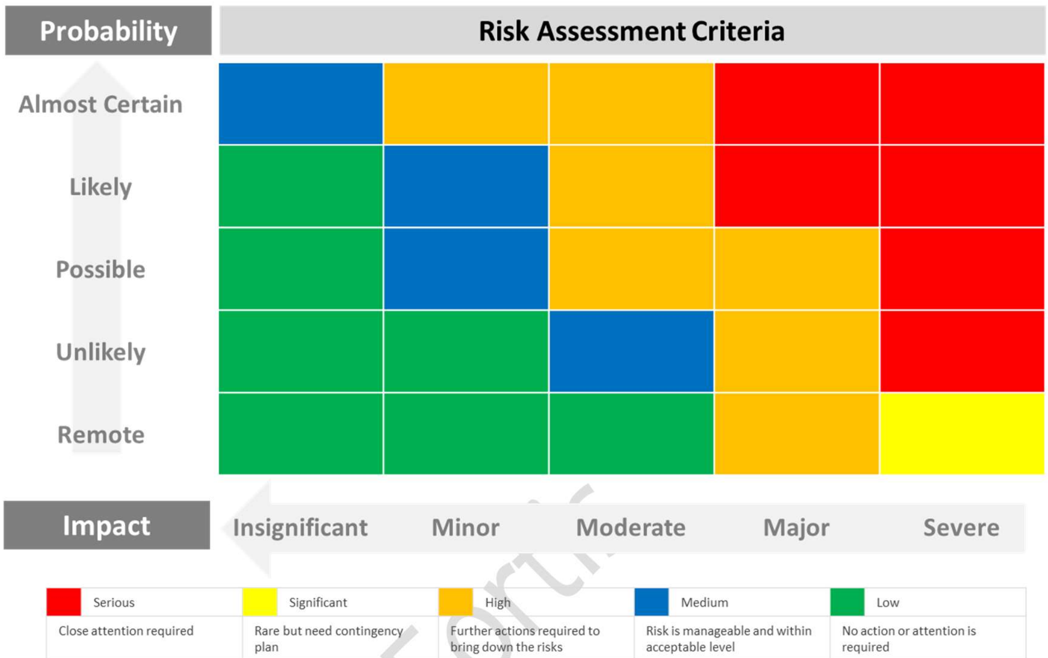
| | Remote | Unlikely | Possible | Likely | Almost Certain |
|---|---|---|---|---|---|
| **Probability (chance) of occurrence** | <10% chance of occurrence within the next one year | 10 – 20% chance of occurrence within the next one year | 20 - 50% chance of occurrence within the next one year | >50% chance of occurrence within the next one year | >75% chance of occurrence within the next one year |
| **Frequency of occurrence** | Occurrence is rare | Occurs exceptionally | Occurs occasionally (from time to time) | Occurs quite frequently (a few times a year) | Occurs very frequently (several times a year) |
| **Time to Failure** | Not expected to occur within the next 5 years | Within 3 – 5 years | Within 3 years | Within 1 – 3 years | Already occurring |
| **Other qualitative considerations** | Not conceivable; has not occurred before | Conceivable but no indications or evidence to suggest occurrence in the near term | Has occurred before, and some indications to suggest possibility of re-occurrence in the near term | Some evidence to suggest expected occurrence in the near term | Strong evidence to suggest occurrence in the near term |

Risk Impact/Consequence Assessment Criteria

| | Insignificant | Minor | Moderate | Major | Severe |
|---|---|---|---|---|---|
| **Strategic Impact** | No impact to FHL strategic goals | Minor 'road bumps' but FHL is generally still on-track to achieve its strategic goals | Moderate diversion of efforts and resources are required to bring FHL back on track to achieve its strategic goals | Substantial efforts and resources are required to bring FHL back on track to achieve its strategic goals | FHL's ability to achieve its strategic goals are significantly impaired; fair to say FHL has failed in fulfilling its mission and vision |
| **Financial Impact** | No impact on EBITDA | <5% hit on target EBITDA (immaterial to financials) | 5 – 10% hit on target EBITDA (material to financials) | 10 – 20% hit on target EBITDA (or profit warning announcement required) | >20% hit on target EBITDA |
| **Medical Impact** | No injury or increased level of care or length of stay | Increased level of care or length of stay required, unrelated to the natural course of the illness and differing from the expected clinical outcome | Temporary reduction in bodily functions (sensory, motor, physiologic, or psychological) unrelated to the natural course of the illness and differing from the expected clinical outcome | Permanent reduction in bodily functions (sensory, motor, physiologic, or psychological) unrelated to the natural course of the illness and differing from the expected clinical outcome | Death of patient |
| **Operational Impact** | Business-as-usual | Isolated and temporary disruptions to operations | Isolated and prolonged disruptions to operations | Widespread but temporary disruptions to operations; substantial and coordinated effort is required to resume and/or maintain normalcy | Widespread and prolonged disruptions to operations; business is almost crippled |
| **Regulatory Impact** | No regulatory impact | Verbal warnings from authorities | Written warnings from authorities ("knuckle-raps") | Regulatory actions taken on FHL – official investigation on company and/or its Directors and Officers; fines or sanctions, publicized reprimand, etc. | Severe regulatory actions taken on FHL and/or its Directors and Officers – suspension or termination of operating licenses, delisting, etc. |
| **Reputation / Brand Impact** | No visible impact on FHL's reputation | Minor reduction in confidence in FHL by stakeholders | FHL is under scrutiny from a small group of stakeholders; some management effort is required to manage this group of stakeholders<br><br>No visible impact on the 'Fortis' brand yet | Negative media coverage (published in mainstream media) isolated to 1 country<br><br>Negative news on FHL has started appearing on the Internet<br><br>'Fortis' is not viewed as a desirable healthcare brand | Negative international media coverage (published in mainstream media of 2 or more countries)<br><br>Negative news on FHL has gone 'viral' on the Internet and reached a wide audience<br><br>Customers, employees, and partners do not wish to be associated with FHL |

**<u>Appendix 3: Risk Assessment Matrix</u>**

Risks are assessed based on their 'Likelihood of Occurrence' and 'Magnitude of Impact'. Functional Heads & Risk Owners should apply these criteria as closely as possible, but may opt to 'override' the criteria with qualitative judgment where it makes sense to do so (i.e. where the measurement criteria or definition does not appropriately reflect the risk analysis or assessment).



## Appendix 4: Risk Register Format

| | | | | | |
|---|---|---|---|---|---|
| **Risk Category** | | **Risk Owner** | | **Probability** | |
| **Risk Statement** | | | | **Impact** | |
| | | | | **Inherent Risk** | |
| **Elements of Risk** | | | | | |
| **Current Mitigation Framework** | | | | | |
| **Residual Risk** | | | | **Response** | |