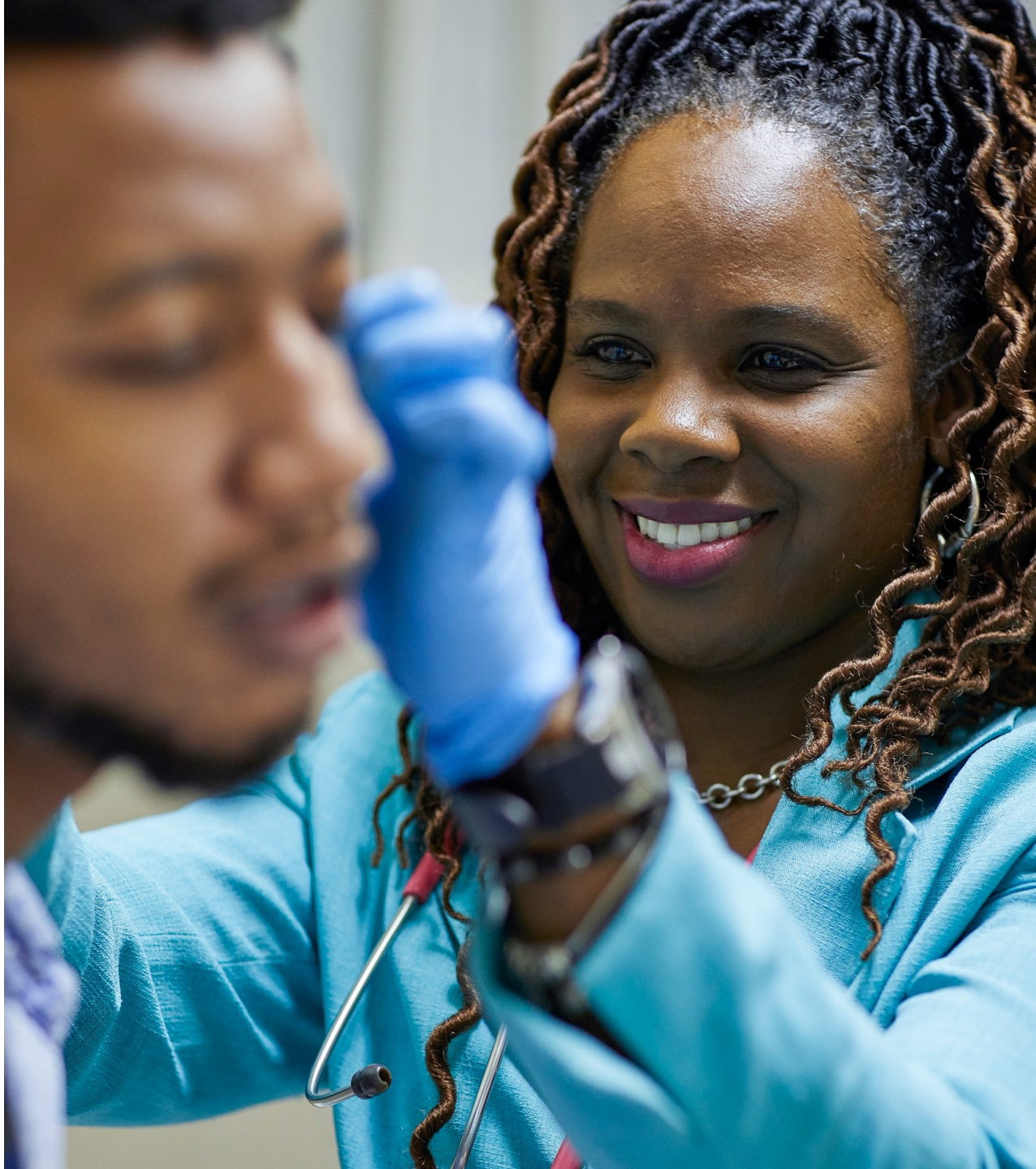
# Enterprise Risk Management Framework



Johnson&Johnson

Enterprise Risk Management Framework



Johnson&Johnson

# Introduction to our Enterprise Risk Management Framework

Johnson & Johnson serves hundreds of millions of people worldwide, aligned with a set of core principles known as Our Credo. Together with the Code of Business Conduct, Our Credo sets the tone and values of our organization. Each employee is encouraged to be open, candid and fact-based in discussing risk issues, making all relevant facts and information available so the company can consider possible options to make informed decisions. Risks are inherent in our business activities and can relate to strategic goals, business performance, compliance with laws and regulations, and the macro environment that may impact Johnson & Johnson.

This document provides an overview of the Johnson & Johnson Enterprise Risk Management (ERM) Framework and presents examples that illustrate how this approach is implemented within the organization. The ERM framework encompasses the following elements:

- Our approach to enterprise risk management
- Components of our ERM framework

**Our Credo and Code of Business Conduct are the core of our business philosophy and culture, and guide our business operations and decision-making.**

Johnson&Johnson

# Our approach to enterprise risk management

Our approach to ERM is informed by principles outlined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO defines risk management as "... the culture, capabilities, and practices that organizations integrate with strategy-setting and apply when they carry out that strategy, with a purpose of managing risk in creating, preserving, and realizing value."[1]

The Johnson & Johnson ERM framework helps identify potential events that may affect the Company, manage the associated risks and opportunities, and provide reasonable assurance that our objectives will be achieved.

Johnson & Johnson's vision is consistent, collaborative and forward-looking risk management that elevates risk awareness across all levels of the organization to:

- strengthen trusted relationships with patients, customers, regulators and business partners
- support strategic priorities
- protect and grow the business to deliver breakthrough innovation to positively impact patients' lives
- prioritize risks to enable appropriate allocation of time, talent and capital for greatest impact
- enable data-driven decision-making

**Enterprise risk management helps enable Johnson & Johnson to successfully grow our business in alignment with Our Credo values and fulfill our purpose to profoundly impact health for humanity.**

[1] COSO, ERM Framework – *Integrating with Strategy and Performance*, 2017.

Johnson&Johnson

# Components of our Enterprise Risk Management Framework

The Johnson & Johnson ERM Framework is comprised of five integrated components:

- Strategy & objectives
- Governance & oversight
- Risk identification & prioritization
- Risk management & monitoring
- Information, communication & reporting

While no risk management system can possibly address every risk, the goal is to ensure prioritized risks are managed within acceptable levels. Descriptions of these five components of our ERM framework follow.

# Strategy & objectives

## Enterprise risk management strategy and objectives

In today's global business environment, business leaders, investors and regulators seek assurance that companies will identify risks and manage operations in a way that balances business opportunities with risks in an integrated, holistic manner. Guided by Our Credo, the Executive Committee establishes overarching strategic goals and financial targets based upon our global growth drivers. These goals are cascaded to our businesses around the world, promoting alignment across the Enterprise. Senior management is accountable for meeting these goals and objectives. Enterprise, sector, business unit, function, and individual employee goals and objectives are aligned to those of the overall organization.

ERM goals and objectives are defined and form part of Johnson & Johnson's approach to managing the business. These goals and objectives are set annually and as needed to manage known risks and to provide risk information that will enable Johnson & Johnson to make informed strategic decisions.

## Enterprise risk management guiding principles

The Company's risk management process is steered by the following guiding principles:

- **Enterprise standardization –** Consistent approach to risk management
- **Integrated risk management –** Integrated view of risk and connected to our strategy
- **Enterprise-wide and Innovative Medicine / MedTech sector focus –** Management of risks at the appropriate level of the organization
- **Connected and enabled by technology –** Implementation of streamlined risk platforms across the organization
- **Clear prioritization –** Prioritization of risks to drive informed decision-making

# Governance & oversight

Strong governance is core to the management of Enterprise risks and supports individuals and organizations across the Company. Risk management is the entire Company's responsibility. The governance structure is intended to provide a high-level framework to enable a coordinated approach to risk management across the Company. In addition, the Enterprise Compliance & Risk Committee (ECRC), chaired by the Chief Technical Operations & Risk Officer, provides governance and oversight over risk management activities. The table below summarizes our five lines of responsibility (5LoR) governance model.

| Line of Responsibility | | Description |
|---|---|---|
| 5th Line | **Board of Directors** Governance and oversight | Provides oversight of management in the best interest of the Company and shareholders |
| 4th Line | **Executive Committee** Risk mindset and tone | Sets the Company's tone and approach to risk management to balance value creation opportunities and to enable efficiency and effective lines of responsibility (1-3 LoRs) |
| 3rd Line | **Independent Assurance** Adequacy and effectiveness | Global Audit & Assurance, reporting to the Audit Committee, works with other internal assurance functions, reporting to various Board Committees (e.g., the Regulatory Compliance & Sustainability Committee [RCSC]), to assess if Company policies and processes are designed adequately and the systems of internal controls are operating effectively |
| 2nd Line | **Risk and Compliance Functions** Policy setting, oversight and risk insights | Provides oversight, monitoring and reporting of operational management's activities to support performance, compliance and prudent risk-taking |
| 1st Line | **Operational Management** Day-to-day management of risk | Executes the day-to-day activities to manage performance and identify, assess and manage risk resulting from business activities, processes and systems for which they are accountable |

Johnson&Johnson

# Risk identification & prioritization

## What is risk?

In today's environment, the velocity of change is increasing and risks come in many different forms. Risk is defined as a potential uncertain event or condition that has an impact on business objectives.

Effective ERM supports the business by helping to identify, evaluate and proactively respond to potential business events or trends that could be either downside threats or upside opportunities that inform decisions and action across the organization. Johnson & Johnson's risks are categorized as strategic, operational, financial or compliance in nature.

## Risk identification & prioritization

Risk identification requires a broad understanding of internal and external factors that can impact the achievement of strategic and business objectives. To gain this understanding, Johnson & Johnson is committed to completing risk identification activities that include, but are not limited to, reviewing key performance indicators across the risk functions, interviews with key stakeholders, and emerging risk scanning. For more information, refer to the J&J Annual Report Risk Factors disclosure.

Risks are identified at various levels of the organization. To better organize and understand risks, they are further categorized into manageable components to help ensure appropriate accountability and leadership alignment. These risks are then prioritized using quantitative data and qualitative information. The prioritization of risks may evolve year over year as factors or risk information changes. Although it is difficult to define every specific type of risk, Johnson & Johnson works through periodic revision and review to maintain an accurate taxonomy of active risks that could affect business operations and objectives.

Johnson&Johnson

# Risk management & monitoring

## Risk management & monitoring process

Risk management and monitoring is a critical part of the risk management lifecycle. These activities are intended to enable early identification and proactive management of risks in the long-term interests of the organization.

Risk management involves understanding the risks and their components, identifying possible mitigation options to determine the most appropriate action for managing and monitoring a risk, and executing on these actions. The risk owners, risk managers, sectors and functions are responsible for the implementation and execution of the risk mitigation plans, where applicable.

Risk management functions develop risk governance and mitigation programs. These functions perform activities to monitor the effectiveness of the risk mitigation activities and provide challenge when needed. Risks are prioritized, and are presented and discussed at various leadership forums including senior leadership teams, functional and sector leadership teams, the Executive Committee and the Johnson & Johnson Board of Directors.

## Risk escalation

Incidents of non-compliance, adverse events, control failures or critical unmitigated risks are to be escalated internally per established policies and procedures, and where applicable, to the proper authorities in a timely manner.

Laws, regulations and internal risk functional policies define escalation paths and procedures. At Johnson & Johnson, all employees are accountable through the Code of Business Conduct and Our Credo to identify and escalate factors that would influence risk to ensure appropriate enterprise risk management.

# Information, communication & reporting

## Information & communication

Information and communication channels are in place so business leaders and employees are aware of risks that fall into their area of responsibility. Risk management functions meet regularly with the Johnson & Johnson's Board of Directors, the Executive Committee, sector leadership teams, functional leadership teams and other senior leadership teams to ensure visibility and ownership of risks.

Formal and informal training is conducted with applicable personnel. For new hires and employees transferring to new functions, information is provided regarding key processes applicable to their role.

Mandatory training is conducted for many areas of risk.

Knowledge and expertise are also exchanged within risk management functions through regular department meetings, short-term rotations through Enterprise or sector functions, and ad hoc cross-business unit assignments.

Other relevant information is disseminated through directed communications via our internal collaboration platforms.

# Information, communication & reporting

## Ethics & compliance reporting

The Our Credo Integrity Line is an integral component of the strong compliance culture at Johnson & Johnson. It provides a channel for all employees, contractors, customers, third-party agencies and other business partners to report potential violations of our Code of Business Conduct and other Company policies, applicable laws and regulations in the countries of operation, or to raise concerns about safety, security or ethical behavior. These issues are reviewed and investigated, and action is taken as appropriate. The channel includes strong protections for those who bring forward potential violations, helping to safeguard them from retaliation in the workplace.

## Risk reporting

In addition to its governance responsibilities, the Enterprise Compliance & Risk Committee (ECRC) serves as the main forum for risk information sharing, management coordination and management oversight. The ECRC supports the role of risk management in enabling Johnson & Johnson to achieve our strategic objectives and meet the expectations of all of Our Credo stakeholders.

The ECRC leverages its member experts to proactively review emerging areas, integrate external risks, opportunities, and risk mitigation plans and actions.

The ECRC also addresses broader cross-functional risk and compliance topics that are not ‘owned’ by any one function and require active cross-Company, cross-functional action, or have potential significant reputational impact. In addition, as appropriate, the ECRC will sponsor initiatives to advance risk management efforts across Johnson & Johnson.

Other senior management groups that have risk reporting responsibilities include the Executive Committee, sector leadership teams, functional leadership teams and other senior leadership teams.

# Enterprise Risk Management Framework

**Contact us:**

Email: Johnson & Johnson Office of the Corporate Secretary at WW-Corporate-Governance@its.jnj.com

One Johnson & Johnson Plaza
New Brunswick, New Jersey 08933
jnj.com

Johnson&Johnson