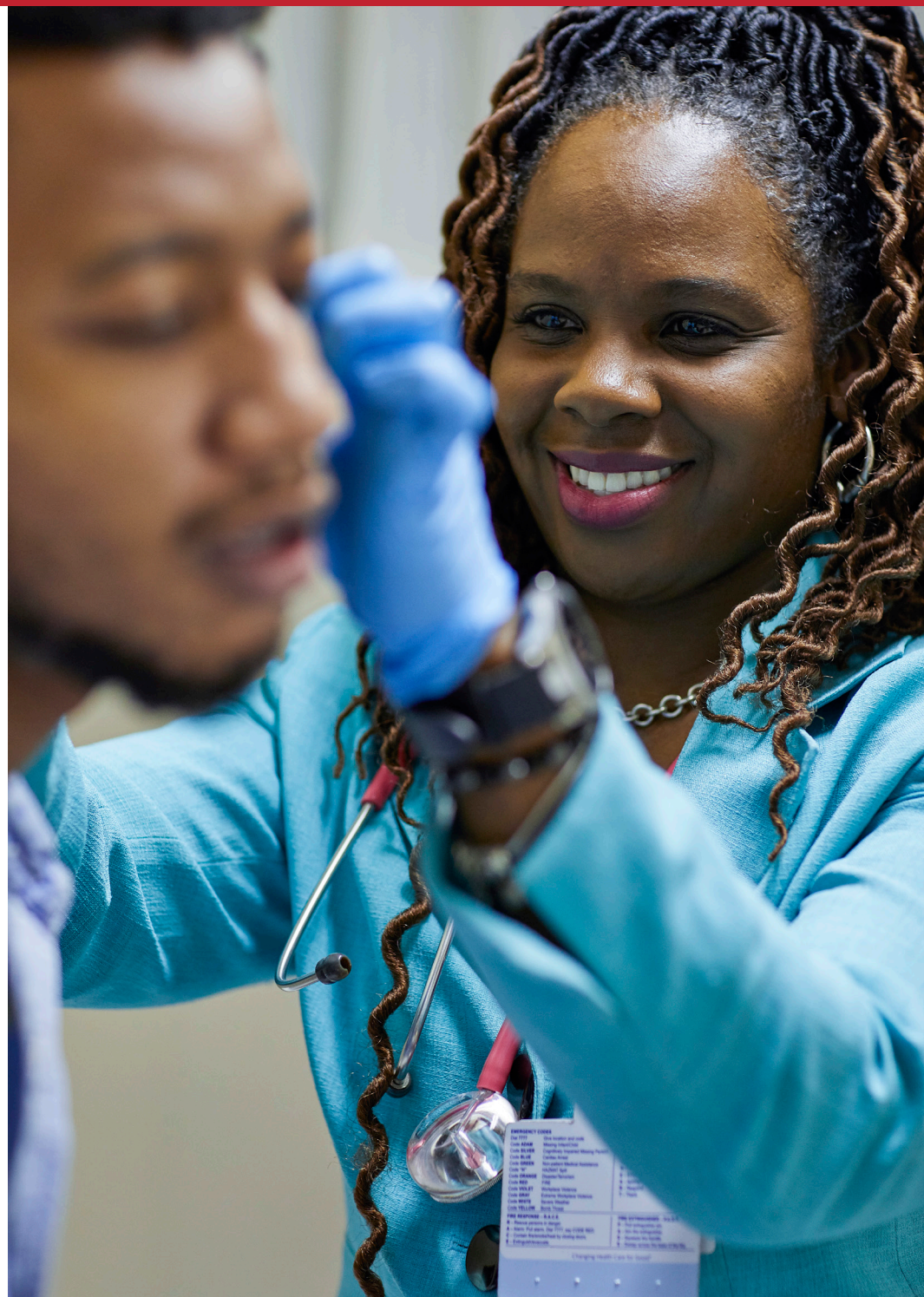
Johnson & Johnson

Enterprise Risk Management Framework



Introduction to ERM Framework 2
How We Define & Categorize Risk 3
Our Approach to ERM 5
Components of Our ERM Framework 6
Strategy & Objective-Setting 6
Performance 7
Review & Revision 8
Information, Communication & Reporting 9
Governance & Oversight 10

Introduction to Enterprise Risk Management Framework

As a leader in healthcare, Johnson & Johnson serves billions 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 all possible options and make informed decisions. Risks are inherent in our business activities and can relate to strategic goals, business performance, and compliance with laws and regulations; and there are also risks specific to environmental, social and governance (ESG) priorities.

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. It encompasses the following elements:

- How We Define & Categorize Risk
- Our Approach to ERM
- Components of Our ERM Framework

Our Credo and Code of Business Conduct are the core of our business philosophy and culture.

Introduction to ERM Framework 2
How We Define & Categorize Risk 3
Our Approach to ERM 5
Components of Our ERM Framework 6
Strategy & Objective-Setting 6
Performance 7
Review & Revision 8
Information, Communication & Reporting 9
Governance & Oversight 10

How We Define & Categorize Risk

Risk management requires a broad understanding of internal and external factors that can impact achievement of strategic and business objectives. Historically, risks to the Company's success have been categorized as Strategic, Operational, Compliance, and Financial & Reporting. However, as the world in which we operate becomes more complex and unpredictable, the corresponding risks and their potential impact have increased (the World Economic Forum Global Risks Report). To ensure the Johnson & Johnson ERM Framework appropriately incorporates the evolving risk landscape, our risk categories now also address environmental, social and cybersecurity risks. Additionally, the Compliance risk category has been expanded to explicitly include legal and regulatory risk.

Our thinking about risk categories is also informed by the results of internal risk assessments and risk assurance work, as well as insights from various industry sources such as the Gartner Risk Management Leadership Council, the World Economic Forum Global Risks Report, the Global Reporting Initiative Standards, the Carbon Disclosure Project and the Task Force on Climate-related Financial Disclosures. Although it is difficult to define every specific type of risk, select examples of risk that exist in our industry are listed in the following table.

Introduction to ERM Framework 2
How We Define & Categorize Risk 3
Our Approach to ERM 5
Components of Our ERM Framework 6
Strategy & Objective-Setting 6
Performance 7
Review & Revision 8
Information, Communication & Reporting 9
Governance & Oversight 10

Risk Types	Examples
Strategic	• Reduction in business vitality due to competition, healthcare reforms and increasing pricing pressures • Loss of intellectual property and trade secrets • Increasing geopolitical barriers to trade in the form of protectionism and nationalism • Barriers to affordable quality care, including suboptimal healthcare systems that limit access to medicines or products • Negative impact to reputation/loss of public trust
Operational	• Breakdown in movement of goods and information within the organization and/or with suppliers and consumers • Loss of business continuity or resilience • Procurement and supplier risks, including those related to human rights • Availability of key materials and/or labor • Inefficient use of resources/increased product cost
Compliance	• Increasing regulatory changes and enforcement in areas such as: - Clinical trial subject/patient safety - Protection and handling of personal information in accordance with data protection/data privacy requirements - Employee health and safety - Selling and promotion of products, including healthcare compliance, Foreign Corrupt Practices Act/global anti-corruption laws, U.S. government contracts/programs • Product quality, safety and effectiveness concerns • Significant legal proceedings, including product liability
Financial	• Poor financial results or economic performance • Changes in tax laws or exposures to additional tax liabilities • Fluctuating currency exchange rates; inflation and currency devaluation • Financial misstatement • Credit risks
Environmental	• Increased severe-weather events such as storms and flooding • Increased pollution due to inadequate waste management • Use of unsustainable materials in the product lifecycle
Social	• Human capital development risks, including leadership sustainability, management succession and capability, employee engagement and accountability • Unfair labor practices, including collective bargaining, freedom of association and grievance processes
Cybersecurity	• Data breach or fraud • Impact to availability of critical information systems • Security incident at critical third party affecting business operations

Introduction to ERM Framework 2
How We Define & Categorize Risk 3
Our Approach to ERM 5
Components of Our ERM Framework 6
Strategy & Objective-Setting 6
Performance 7
Review & Revision 8
Information, Communication & Reporting 9
Governance & Oversight 10

Our Approach to ERM

Our approach to ERM is informed by principles outlined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) which defines ERM as "the culture, capabilities, and practices, integrated with strategy-setting and performance, that organizations rely on to manage risk in creating, preserving, and realizing value" (COSO, ERM Framework – *Integrating with Strategy and Performance*, 2017).

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

Our approach to risk management:

- Looks to promptly resolve internally identified risks to compliance with laws and regulations to maintain the provision of quality products, protect patient safety and ensure appropriate relationships with customers
- Supports strategies to ensure effective use of resources; enables an optimized, proactive approach to auditing and identifying/remediating compliance issues; and promotes reporting and monitoring across Enterprise compliance functions
- Helps enable improved decision making, planning and prioritization through assessments of opportunities and threats
- Helps drive value creation by enabling management to respond in a prompt, efficient and effective manner to events that may potentially create uncertainty and represent a significant threat or opportunity

ERM helps enable the Enterprise to successfully grow the business in alignment with Our Credo values.

Introduction to ERM Framework 2
How We Define & Categorize Risk 3
Our Approach to ERM 5
Components of Our ERM Framework 6
Strategy & Objective-Setting 6
Performance 7
Review & Revision 8
Information, Communication & Reporting 9
Governance & Oversight 10

Components of Our ERM Framework

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

- Strategy & Objective-Setting
- Performance
- Review & Revision
- Information, Communication & Reporting
- Governance & Oversight

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 & Objective-Setting

Guided by Our Credo, the Executive Committee (EC) establishes overarching strategic goals and sets financial targets based upon our Global Growth Drivers. These goals are cascaded to our businesses around the world, ensuring alignment across the Enterprise. Senior management is accountable for meeting these goals and objectives. Business unit, Enterprise function and individual employee goals and objectives are typically aligned to those of the overall organization.

Introduction to ERM Framework 2
How We Define & Categorize Risk 3
Our Approach to ERM 5
Components of Our ERM Framework 6
Strategy & Objective-Setting 6
Performance 7
Review & Revision 8
Information, Communication & Reporting 9
Governance & Oversight 10

Performance

Internal and external issues and events affecting our ability to achieve established objectives are typically identified at various points in the business cycle. During planning and review processes, business unit management assesses the marketplace and competitive environment, including megatrends, to identify risks and opportunities facing their business. The various Enterprise risk management functions provide expertise, support and input into the process, as needed.

Business leaders, in partnership with the applicable Enterprise risk management functions, determine the appropriate way to address identified risks. The activity or situation posing the risk may be avoided, accepted, reduced, shared or transferred, depending on the facts and circumstances.

To help ensure risk responses are consistently implemented, Enterprise risk management functions may set policies, define minimum standards and/or issue guidelines that apply to Johnson & Johnson business activities.

Enterprise risk management functions help support the implementation of these policies, standards and guidelines through monitoring tools, including self-assessments, that enable local leaders to understand where controls are necessary, as well as where improvement may be required.

Business unit management, in partnership with the appropriate Enterprise risk management functions, develops action plans to implement or strengthen risk-mitigating activities, as applicable. Increasingly, as a best practice, systems and critical business processes are designed and implemented to automate and build in compliance with policies, standards and other risk mitigation strategies.

For example, to increase business resilience, our Supply Chain has implemented Business Continuity Management (BCM) processes with clear requirements tailored to different sites. These processes help ensure that social, political and environmental changes do not negatively impact our ability to service customer orders and safeguard our employees. Our BCM processes also promote maintenance and testing of business continuity plans.

Throughout the year, risk assessments, scans and surveys may be performed by the business and/or Enterprise risk management functions to identify internal and external events that might affect achievement of the Company's objectives. These include analysis of applicable business intelligence, such as trends in external health authority and other government inspections and enforcement, legislative changes, and shifts in market, payer and consumer models.

Introduction to ERM Framework 2
How We Define & Categorize Risk 3
Our Approach to ERM 5
Components of Our ERM Framework 6
Strategy & Objective-Setting 6
Performance 7
Review & Revision 8
Information, Communication & Reporting 9
Governance & Oversight 10

Review & Revision

Critical to our ERM Framework is a review and reporting process to ensure risks are effectively assessed and appropriate risk responses and controls are in place.

Testing, auditing and assessments are typically performed by personnel who don't report into the business in order to provide independent assurance that risk responses are being implemented, procedures are understood and followed, and appropriate controls are in place.

Enterprise risk management functional leadership and business unit management monitor the effectiveness of the risk mitigation activities through review of metrics and other data on a periodic basis. Additionally, key risk metrics are reviewed with the Johnson & Johnson Board of Directors, the EC, business segment and other senior leadership teams, as well as at the Johnson & Johnson Corporate Compliance Committee and Enterprise Governance Council.

Introduction to ERM Framework 2
How We Define & Categorize Risk 3
Our Approach to ERM 5
Components of Our ERM Framework 6
Strategy & Objective-Setting 6
Performance 7
Review & Revision 8
Information, Communication & Reporting 9
Governance & Oversight 10

Information, Communication & Reporting

Information and communication channels are in place so business leaders and employees are aware of risks that fall into their area of responsibility. Key Enterprise risk functions meet regularly with the Johnson & Johnson Board of Directors, the EC, each business segment leadership team and select additional senior leadership teams to ensure visibility and ownership of critical risks.

Formal and informal training is conducted with applicable personnel. For new hires and employees transferring to new Enterprise functions, information is provided regarding key processes applicable to their role. For many areas of risk, mandatory training is conducted annually. Knowledge is also exchanged within Enterprise risk management functions through regular department meetings, short-term rotations through Corporate or Enterprise functions and ad hoc cross-business unit assignments.

Other relevant information is disseminated through directed communications and via intranet sites available to all employees. Rapid alerts or formal memos summarizing key learnings from incidents, common audit findings or other identified trends may be distributed across the impacted community to help prevent similar events at other Johnson & Johnson business units or locations.

Policies and procedures are in place that require incidents of non-compliance, adverse events, control failures or critical unmitigated risks to be escalated to senior management and, if appropriate, the proper authorities in a timely manner.

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 partners to report potential violations of our Code of Business Conduct and other Company policies, or the 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 appropriate actions taken, if required. The channel includes strong protections for those who bring forward potential violations (whistleblowers), helping to safeguard them from harassment in the workplace.

Monitoring and reporting help ensure risks are effectively assessed and appropriate risk responses and controls are in place.

Introduction to ERM Framework 2
How We Define & Categorize Risk 3
Our Approach to ERM 5
Components of Our ERM Framework 6
Strategy & Objective-Setting 6
Performance 7
Review & Revision 8
Information, Communication & Reporting 9
Governance & Oversight 10

Governance & Oversight

Our Board of Directors provides oversight of senior leadership's management of the various risks the Company faces. The Board meets at regular intervals with EC members, other senior business leaders and leaders of Enterprise risk management functions to discuss risk factors related to the Company. It also receives regular reports from senior representatives of the Company's independent auditor.

For example, the Regulatory Compliance & Sustainability Committee of the Board reports to and assists the Board by providing oversight of quality, privacy/data security, cybersecurity and other key regulatory areas that may impact the Company. The Regulatory Compliance & Sustainability Committee meets quarterly and holds separate private meetings at least semi-annually with each of the following: the General Counsel, the Chief Compliance Officer and the Chief Quality Officer. The Audit Committee also meets quarterly to provide oversight of our financial compliance, as well as in private sessions with the Chief Financial Officer, the Vice President of Global Audit & Assurance and representatives of the Company's independent auditor.

The EC establishes overarching strategic goals and oversees the business segments as well as the Enterprise risk functions, which are functionally independent from commercial interests.

Johnson & Johnson business leaders are accountable for managing risks affecting their respective business segments and the overall Enterprise. Enterprise risk management functions are responsible for identifying and assessing risks to business leaders and collaborating with them to find effective ways to manage identified risks.

Risk management professionals also strive to innovate and develop solutions to identify and mitigate risk. Each Enterprise risk management function provides oversight and governance to help ensure standards are met and that risks are mitigated effectively. The leaders of these functions develop strategic plans and direction for their organization to effectively align the mitigation support to the objectives and priorities of the Enterprise.

Various councils and committees serve as cross-functional governance mechanisms to share emerging risks and common practices, especially for cross-functional risks that require an integrated approach or may have complementary impact. For example, the Corporate Compliance Committee (CCC) serves as the primary governance structure for information sharing and coordination on compliance-related risks across core Enterprise risk functions such as Health Care Compliance, Privacy, Quality & Compliance, Information Security & Risk Management, the Law Department and Global Audit & Assurance.

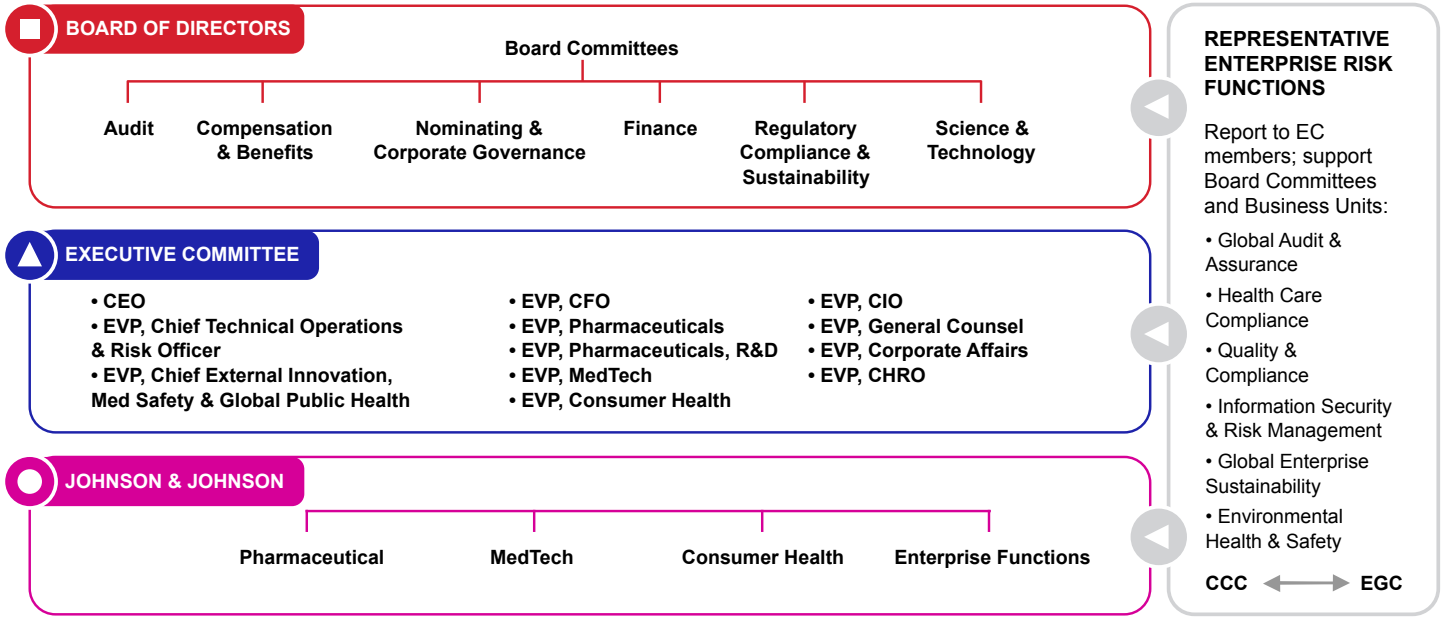
Introduction to ERM Framework 2
How We Define & Categorize Risk 3
Our Approach to ERM 5
Components of Our ERM Framework 6
Strategy & Objective-Setting 6
Performance 7
Review & Revision 8
Information, Communication & Reporting 9
Governance & Oversight 10

Similarly, the Enterprise Governance Council (EGC) serves as a community of experts who work cross-functionally to drive alignment and coordination on efforts related to key environmental, social and governance (ESG) topics. Both the CCC and EGC have overlapping representation of the Enterprise risk functions that facilitates common visibility and coordination between the two bodies. The EGC provides a venue for identifying and understanding significant emerging ESG topics, issues and trends that may impact the Company's overall business strategy and reputation.

During the course of the year, risk assessments are performed by the business and Enterprise risk management functions to identify internal and external events that might affect achievement of the Company's objectives.

Introduction to ERM Framework 2
How We Define & Categorize Risk 3
Our Approach to ERM 5
Components of Our ERM Framework 6
Strategy & Objective-Setting 6
Performance 7
Review & Revision 8
Information, Communication & Reporting 9
Governance & Oversight 10

Governance Flowchart



BOARD OF DIRECTORS

Throughout the year, the Board and its Committees receive updates from management and key Enterprise risk functions regarding ERM issues and risks related to our businesses, including active and potential litigation as well as reputational risk.

EXECUTIVE COMMITTEE

The EC establishes overarching strategic goals and sets financial targets based on our Enterprise Principles and Global Growth Drivers. These Goals are then cascaded to our business worldwide, ensuring Enterprise alignment.

BUSINESS UNITS/ENTERPRISE FUNCTIONS

Operational management establishes internal controls and executes procedures to identify, assess and manage events that may pose a risk to their business units. Corresponding Enterprise risk functions are engaged to analyze risks and determine how they should be addressed.

CORPORATE COMPLIANCE COMMITTEE

The CCC serves as the primary governance structure for information sharing and coordination of compliance-related risks across core Enterprise risk functions.

ENTERPRISE GOVERNANCE COUNCIL

The EGC serves as a community of experts working cross-functionally to drive alignment and coordinate efforts related to key environment, social, and governance topics.

Enterprise Risk Management Framework

Contact us:

Johnson & Johnson Enterprise ESG Program Office
WW-Corporate-Governance@its.jnj.com

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