Johnson & Johnson

Enterprise Risk Management Framework

Our Credo

We believe our first responsibility is to the doctors, nurses and patients, to mothers and fathers and all others who use our products and services. In meeting their needs everything we do must be of high quality. We must constantly strive to reduce our costs in order to maintain reasonable prices. Customers' orders must be serviced promptly and accurately. Our suppliers and distributors must have an opportunity to make a fair profit.

We are responsible to our employees, the men and women who work with us throughout the world. Everyone must be considered as an individual. We must respect their dignity and recognize their merit. They must have a sense of security in their jobs. Compensation must be fair and adequate, and working conditions clean, orderly and safe. We must be mindful of ways to help our employees fulfill their family responsibilities. Employees must feel free to make suggestions and complaints. There must be equal opportunity for employment, development and advancement for those qualified. We must provide competent management, and their actions must be just and ethical.

We are responsible to the communities in which we live and work and to the world community as well. We must be good citizens – support good works and charities and bear our fair share of taxes. We must encourage civic improvements and better health and education. We must maintain in good order the property we are privileged to use, protecting the environment and natural resources.

Our final responsibility is to our stockholders. Business must make a sound profit. We must experiment with new ideas. Research must be carried on, innovative programs developed and mistakes paid for. New equipment must be purchased, new facilities provided and new products launched. Reserves must be created to provide for adverse times. When we operate according to these principles, the stockholders should realize a fair return.

Johnson & Johnson

Introduction

In order to deliver value to our consumers, patients, caregivers, employees, communities and shareholders, we at Johnson & Johnson (J&J) must understand and manage the risks faced across our entire organization. Risks are inherent in our business activities and can relate to strategic threats, operational issues, compliance with laws, and reporting obligations.

This document provides an overview of our enterprise-wide approach to risk management (the "J&J Enterprise Risk Management Framework") and illustrates examples of how this approach is implemented within the organization.

The purpose of the J&J Enterprise Risk Management Framework is to describe

- Categorization of risk
- The common framework used to identify and manage potential events that may affect the enterprise
- Accountability for risk management
- Governance and oversight of risk management activities

Contents

J&J Strategic Framework

J&J is a company of enduring strength that has been privileged to play a role in helping millions of people the world over be well and stay well through more than a century of change. As the science of human health and well-being has grown, we have been able to grow along with it. Even more important, we have helped shape and define what health and well-being means in everyday lives. Our products, services, solutions and our commitment to philanthropy now touch the lives of at least one billion people every day.

Our strategic framework captures the way all the elements of our business intersect to deliver value including the key drivers of our future success.

First and foremost, J&J is guided by Our Credo, a deeply held set of values that is our moral compass. Above all, Our Credo challenges us to put the needs and well-being of all the doctors, nurses, patients, and consumers who use our products first. It also speaks to the responsibilities we have to our employees, to the communities in which we live and work and the world community, and to our shareholders. From Our Credo, Our Aspiration emerges – by caring, one person at a time, we help billions of people around the world live longer, healthier and happier lives.

We build from this foundation a unique set of strategic principles—being broadly based in health care; using our reach and size for good; leading with agility and urgency; and investing for enduring impact. And we do all this through a unique culture that values and fosters the development of our people.

Finally, our growth drivers are the specific areas of focus that help ensure our robust growth for the future. We believe that it is essential to focus on these critical drivers of our future growth: to create life-enhancing innovation; to deliver excellence in execution; to generate value through partnership; and to empower and inspire our employees.

Ultimately it is through effective risk management that we enable the enterprise to implement this strategic framework and grow the business successfully in alignment with Our Credo and strategic principles amidst an evolving and challenging external environment.

What is Risk?

Risk can be viewed as the combination of the probability of an event and the impact of its consequences. Events with a negative impact represent risks that can prevent value creation or erode existing value. In order to deliver value to our stakeholders we must understand the types of risks faced by our organization and address them appropriately.

Generally, risks to the Company's success can be grouped into four categories: (1) Strategic, (2) Operational, (3) Compliance and (4) Financial & Reporting. Specific examples of each type of risk are included in the table below.

Risk Types	Examples
Strategic	▪ Reduction in business vitality (due to change in business strategy, customer spending patterns, product discovery & development, changing technology, etc.) ▪ Loss of intellectual property & trade secrets ▪ Competition for talent ▪ Negative impact to reputation/loss of public trust
Operational	▪ Disruption to product supply ▪ Counterfeiting ▪ Inefficient use of resources/increased product cost ▪ Physical property/damage/disruption ▪ Discontinuation of global data flows
Compliance	Violation of laws or regulations governing areas such as: ▪ Environmental ▪ Employee health & safety ▪ Clinical trial subject/patient safety ▪ Product quality/safety issues (violations of FDA and other Health Authority regulations, Pharmacovigilance) ▪ Selling and promotion of our products (including Health Care Compliance (HCC), Foreign Corrupt Practices Act (FCPA)/global Anti-Corruption laws, U.S. government contracts/programs) ▪ Protection of personal data in accordance with global data protection requirements ▪ Local tax and statutory laws
Financial & Reporting	▪ Currency exchange, funding & cash flow, credit risk ▪ Financial misstatement (including violation of the Sarbanes Oxley Act)

J&J Approach to Enterprise Risk Management

Effective risk management enables the enterprise to successfully grow the business in alignment with Our Credo and strategic principles.

Enterprise Risk Management (ERM) Defined

Enterprise Risk Management is a common framework applied by business management and other personnel to 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.

Through this approach to risk management, we can:

- Ensure prompt resolution of internally identified risk to compliance with laws and regulations to maintain the provision of quality products, protect patient safety and ensure appropriate relationships with customers
- Support "simplification" strategies to ensure effective use of resources, enable an optimized approach to auditing and identification/remediation of compliance issues and promote reporting and monitoring across compliance functions
- Enable improved decision making, planning and prioritization through a structured understanding of opportunities and threats
- Support value creation by enabling management to deal effectively with future events that create uncertainty, pose a significant risk or opportunity and to respond in a prompt, efficient and effective manner
- Support our growth drivers of creating life enhancing innovation, delivering excellence in execution, generating value through partnerships and empowering and inspiring our employees

Accountability

J&J business leaders are accountable for managing and mitigating risks affecting their business. Risk management functions are responsible for identifying, assessing, and presenting those risks to the business leaders for recommended actions. Risk management professionals continuously strive to innovate and develop solutions to identify and mitigate risk more effectively. Select risk management functions are listed below along with the areas of risk for which they have responsibility.

Select Risk Management Functions	Strategic Risk	Operational Risk	Compliance Risk	Financial & Reporting Risk
Corporate Internal Audit			X	X
Environmental, Health, Safety & Sustainability	X	X	X	
Finance	X		X	X
Chief Medical Officer	X		X	
Global Security	X	X	X	
IS Risk Management (ISRM)	X	X	X	X
Health Care Compliance & Privacy	X		X	
Human Resources - Human Capital Development	X			
Law Department	X		X	
Quality & Compliance		X	X	
Supply Chain	X	X	X	

Our Credo and Code of Business Conduct are the core of our business philosophy and set the tone and values of the organization.

Components of Enterprise Risk Management Framework

Our J&J Enterprise Risk Management Framework is made up of six process components derived from the Committee of Sponsoring Organizations of the Treadway Commission ERM Framework. Our Credo and Code of Business Conduct are the core of our business philosophy and set the tone and values of the organization. Objectives are set by the Executive Committee in alignment with our strategic framework and are cascaded throughout the organization.

1. **Event Identification & Risk Assessment:** As part of the strategic planning process and day-to-day management of the business, functional leaders identify internal and external events that may affect the achievement of our Company's objectives. Risk management function personnel help identify and assess these risks through their expertise, formal assessments and analysis of business intelligence and trends.
2. **Risk Response:** A response is determined based upon the overall risk exposure, considered as a function of likelihood and impact of the occurrence. Risk responses may include avoiding or evading, accepting, reducing, and sharing or transferring risk.
3. **Control Activities:** Control activities are established to ensure that risk responses are carried out effectively and consistently throughout the organization. This involves formalizing risk response in our Company policies, ensuring clear accountability, utilizing self-assessment and monitoring tools and designing controls into our systems and critical business processes.
4. **Information & Communication:** Information and communication channels are in place to make the organization aware of risks that fall into their area of responsibility and expected behavior and actions to mitigate negative outcomes.
5. **Oversight & Monitoring:** Management reviews, as well as assurance activities, such as testing, auditing and assessments, are in place to ensure that risks are effectively identified and assessed, and that appropriate responses, controls and preventive actions are in place.

While no risk management system can ever be absolutely complete, the goal is to make certain that identified risks are managed within acceptable levels.

Internal Environment and Objective Setting

Our Credo, alongside the Code of Business Conduct, sets the tone and values of our organization. It is through this lens that we view risk and define how we will respond to that risk.

Management encourages a risk culture that has individual accountability at its heart. This means that 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 decisions. We are all accountable for speaking up and escalating concerns to management about issues that may cause risk or potential harm.

Guided by Our Credo, the Executive Committee sets overarching strategic objectives as well as financial targets based upon the Enterprise growth priorities. These objectives are cascaded to our businesses across the globe ensuring alignment across the Enterprise. Senior management is accountable for meeting the set objectives. Business unit, functional and individual employee goals are aligned to the overall objectives of the organization and are consistent with the Company's overall mission, Our Credo and our strategic principles.

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

Event Identification & Risk Assessment

Internal and external events affecting our ability to achieve these set objectives are identified at various points in the business cycle. During strategic and business planning and review processes, business unit management assesses the market and competitive environment to identify risks and opportunities facing their business. The various risk management functions within or assigned to that business unit provide expertise, support and input into the process. Each of the risk management functions is represented on applicable management committees to enable effective risk identification and business partnership.

Throughout the year, risk assessments, scans and surveys are performed by the business and risk management functions to identify internal and external events that might affect achievement of the Company's objectives. Additionally, the various risk management functions scan the external environment for risk indicators through analysis of applicable business intelligence, including trends in external health authority and other government inspections and enforcement, legislative changes, and shifts in market, payer and consumer models, as well as relationships with external subject matter experts.

Finally, risk management functions review the output from internal monitoring and assurance activities to identify gaps and emerging risk areas.

Risks are analyzed, considering likelihood and impact of a given outcome, to determine how they should be managed.

For each risk identified, a response is determined and implemented by the business leaders in consultation with the applicable risk management functions.

Risk Response

For each of the risks identified, a response is determined by the business leaders in consultation with the applicable risk management functions. The activity or situation posing the risk may be avoided or evaded, accepted, reduced, shared or transferred, depending on the facts and circumstances. The specific response is determined based upon the overall risk exposure, considered as a function of likelihood and impact of the occurrence, coupled with our overall risk tolerance.

Control Activities

To ensure that the risk response is followed consistently throughout the organization, Enterprise risk management functions may set policies, issue guidance and/or minimum standards that apply to all J&J business units globally.

Risk management functions support the implementation of these policies and standards locally at business units and sites through development and deployment of self-assessment and monitoring tools that allow local management to understand where processes and controls are necessary, as well as where improvement may be required. Business unit management, in consultation with the appropriate risk management functions, will design and document 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 or “design in” compliance with these standards and other risk mitigation strategies.

Information & Communication

Information and communication channels are in place to make business leaders, as well as individuals, aware of risks that fall into their area of responsibility and the expected behavior to mitigate negative outcomes.

Formal and informal training is conducted with applicable personnel. Information is provided to new hires and employees transferring to new functions on key processes applicable to their role. For many areas of risk, mandatory training is conducted annually. Knowledge is also exchanged within 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 prevent similar events at other J&J business units or locations.

Formal 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 the proper authorities in a timely manner.

Additionally, our J&J Credo Hotline offers all employees a mechanism for reporting potential violations of safety, security, policy and ethical behavior anonymously (where local law permits).

Oversight & Monitoring

Critical to our J&J Enterprise Risk Management Framework is a review and reporting process to ensure risks are effectively assessed and appropriate risk responses and controls are in place.

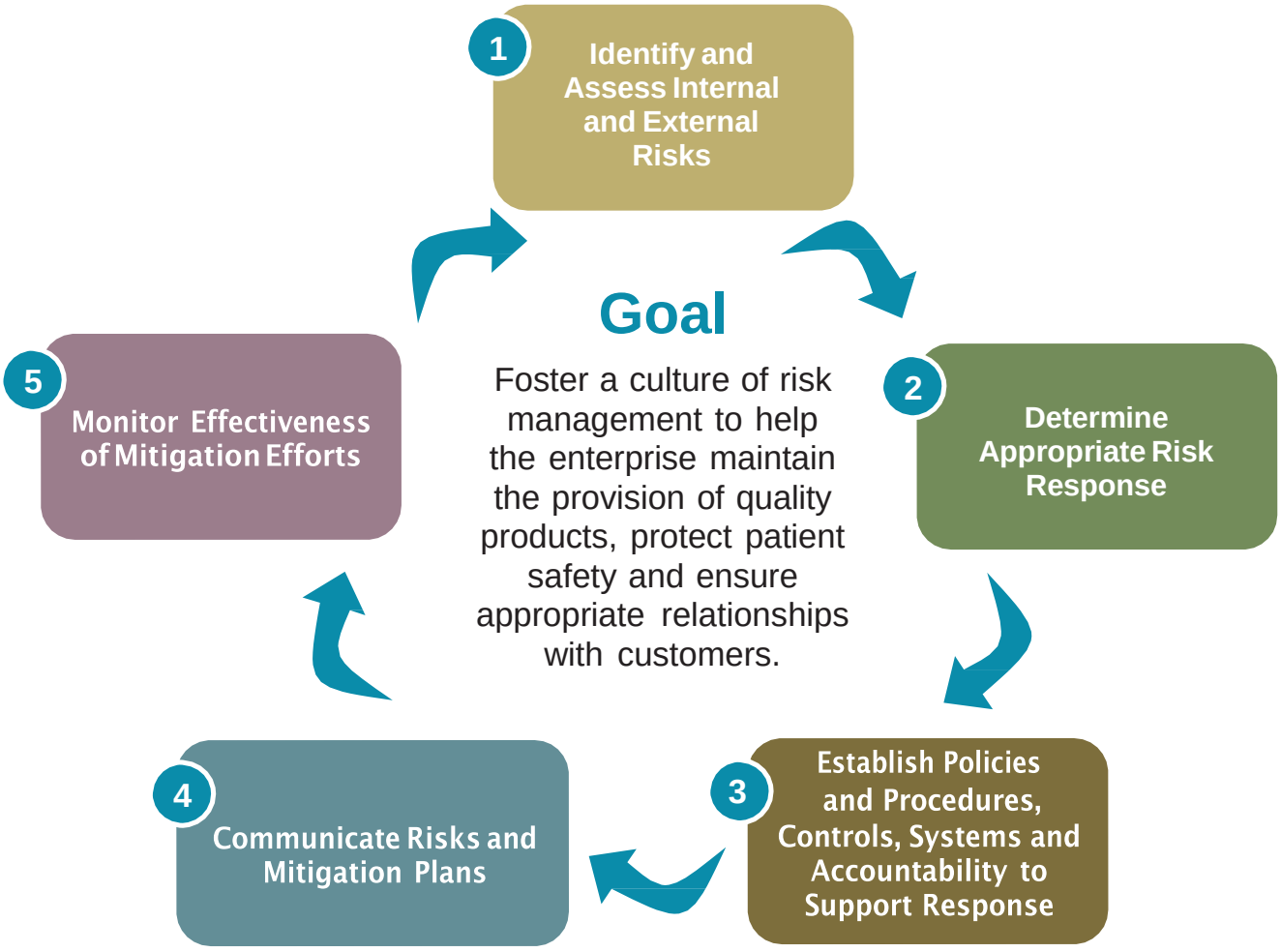
Testing, auditing and assessments are performed by independent, objective personnel to provide assurance that risk responses are consistently implemented, procedures are understood and followed, and appropriate controls are in place.

Risk management functional leadership and business unit management monitor the effectiveness of the risk mitigation activities as well as the overall program effectiveness through review of metrics and dashboards on a periodic basis. Additionally, these measures are reviewed with the J&J Compliance Committee or other Enterprise governance teams, the Executive Committee and the Board of Directors.

Each risk management function analyzes metrics, incidents, trends in auditing, testing and assessment results and other risk-related information to identify emerging risks, as well as ways to improve the risk management program including new controls, new or revised standards, or other initiatives.

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

J&J Enterprise Risk Management Framework Components



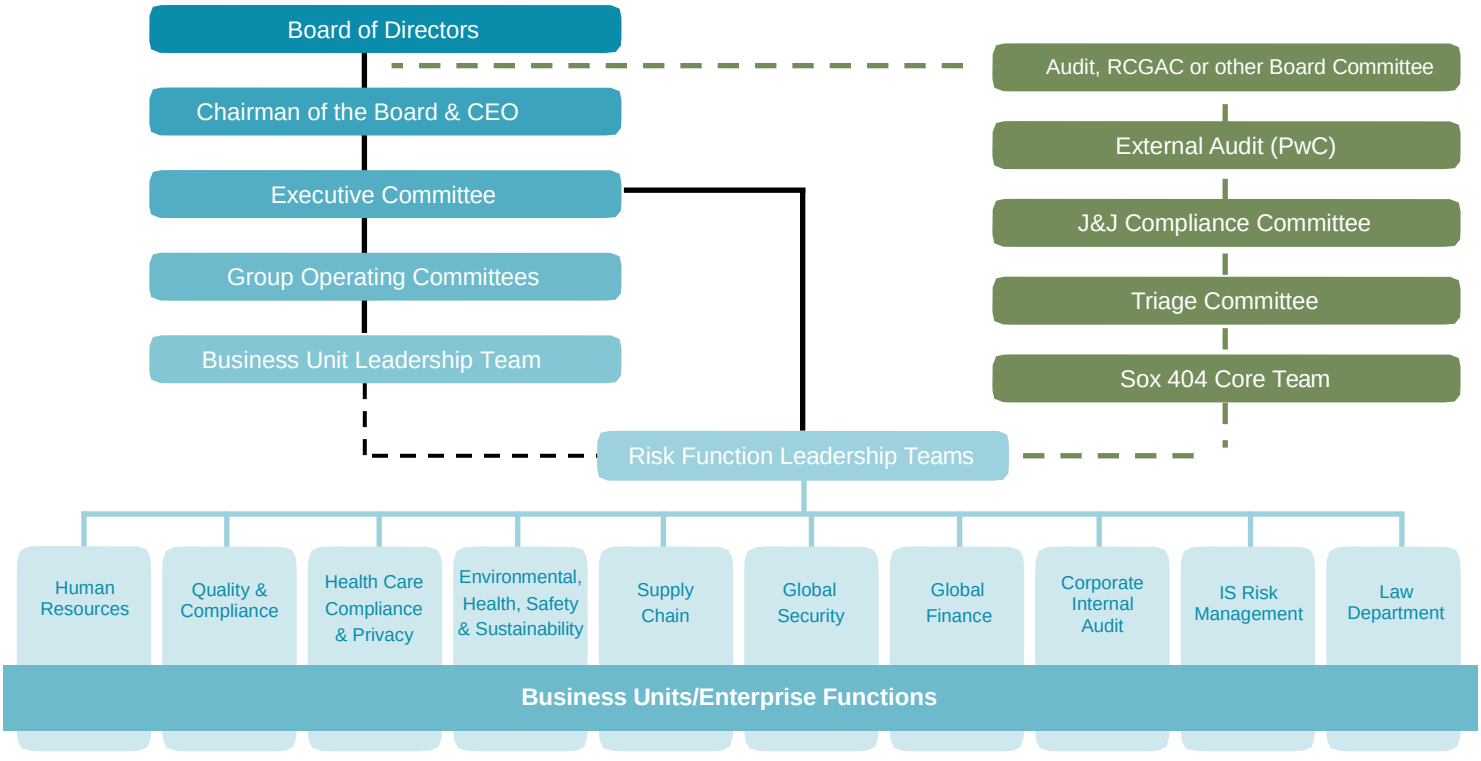
Governance & Oversight

Governance

As described above, each business unit and function communicates identified risks and associated response strategies to their leadership teams. As appropriate, issues are also escalated to their respective Executive Committee member or directly to the Audit or other appropriate Committee of the Board.

Individual risk management functions provide oversight and governance to 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 organization.

Finally, various councils and committees serve as cross-functional governance mechanisms to share emerging risks and common practices—especially for risks that require an integrated approach or may have complementary impact. For example, the J&J Compliance Committee serves as the primary governance structure for coordinating compliance-related risks across the core risk functions (such as Quality, Health Care Compliance, Finance, etc). And, the internal Triage Committee (comprised of senior leaders of Corporate Internal Audit, Health Care Compliance & Privacy and the Law Department) manages the investigation process for all escalated issues involving allegations of compliance, financial, legal or other similar policy violations.



Role of the Board of Directors

Our Board of Directors provides oversight of senior leadership's management of the various risks the Company faces. The Board meets regularly with key risk management functional leaders. It also receives regular reports from senior representatives of the Company's independent auditor.

For example, the Regulatory, Compliance & Government Affairs Committee (RCGC) of the Board reports to and assists the Board by providing oversight of regulatory, compliance, quality and governmental affairs matters that may impact the Company. The RCGC meets quarterly and holds separate private meetings at least semi-annually with each of the General Counsel, the Chief Compliance Officer, the Vice President for Corporate Internal Audit 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 Corporate Internal Audit and representatives of the Company's independent auditor.

Ultimately oversight of our risk management activities is one of the most important roles of the Board of Directors. The Board is dedicated and fully committed to its role in ensuring quality, compliance and effective risk management.

Conclusion

As a leader in health care, J&J serves billions of people worldwide by bringing value, expertise and innovation in line with Our Credo. Risk is inherent in our business activities. Our strong risk management practices allow us to strengthen our organization through informed strategic and business decisions, so we can continue to meet the needs of consumers, doctors, nurses, patients, mothers and fathers.