Policy on Risk Management

POL-GSK-500

Why we have this policy

What does this policy cover?

We are committed to having effective *risk management* systems (including frameworks and processes) to ensure the *significant risks* we face have been appropriately identified, assessed, treated, monitored, and reported.

This is an integral part of good management practice and will help us to: protect patient safety, employees, the environment, company assets and reputation; and achieve our business objectives, safeguard shareholder investment and ensure we comply with legal requirements.

This policy helps ensure risk management is an integral part of decision making and is embedded in normal business operations.

GSK's Board of Directors is required to maintain sound risk management and internal control systems in order to comply with the UK Corporate Governance Code requirements.

Why should you read this?

This policy applies to all GSK employees and *complementary workers*.

This policy defines the roles, responsibilities and expectations of the organisation in relation to risk management systems.

What you need to know

The company must maintain the Risk Oversight and Compliance Council (*ROCC*) to oversee the risk management and internal control systems for our significant risks. This includes ensuring a robust process exists for the business to identify the *risks* that are significant to the company, assign risk owners, and monitor the effectiveness of internal controls implemented to manage those *risks*.

Significant risks in this policy are defined as potential events that create significant uncertainty or could significantly adversely affect the achievement of business objectives. Please refer to the Corporate Governance Manual for the ROCC's terms of reference.

Business units and Global Functions designated by the ROCC must set up a Risk Management and Compliance Board (*RMCB*) to ensure the implementation of appropriate internal controls for significant risks. The RMCB should meet at least semi-annually and be comprised of members representing the major activities of the area.

Each RMCB must review significant risks at least annually to identify operational, compliance and other risks that may affect the achievement of business unit objectives.

The relevant Corporate Executive Team (CET) member must report to the ROCC annually on the scope of its risks and associated controls that fall within his or her oversight.

Significant risks should be considered in the business unit's annual planning processes (e.g. strategy, financial) and management should consider the impact of executing its plans on its significant risks.

Each RMCB must assign Risk Owners to directly oversee the assessment and treatment of its significant risks and to periodically update the RMCB on the status of the risks. The treatment of a risk defines whether the risk will be mitigated, accepted, transferred, or avoided.

The relevant RMCBs and ROCC should determine its reporting expectations to fulfil the group's respective responsibilities.

The relevant CET member must set up appropriate risk management and internal control systems reporting into their relevant RMCBs.

Every year, each CET member must certify that they operate an effective system of internal control and have undertaken an exercise to identify and assess significant risks faced by their business unit.

The RMCB must ensure that appropriate controls are in place for its significant risks including:

- Management operations (level 1): controls that are embedded in processes, systems or products to ensure risks are appropriately managed. Examples include management approvals and self inspections.
- Control groups (level 2): ongoing monitoring against a defined standard (e.g. regulations, policy, guidelines and procedures) to measure compliance. This must be carried out by people or a group that is sufficiently independent of the activity being monitored.

Global Ethics and Compliance are responsible for facilitating the implementation of a sound system of risk management and internal controls. The role of Audit & Assurance is to provide an objective view, independent from line management, of the adequacy and effectiveness of the management of significant risks.

If you have a concern turn to page 2 for guidance

Speak Up

Policy on Risk Management

POL-GSK-500

If you have a concern

If you have a concern over this policy or know it has been breached you must inform a member of Global Ethics and Compliance or Global Risk Management.

To find your local Speak Up integrity line number or to report online, please visit: www.gsk.com/integrity

If you are out of compliance or feel you are unable to comply with the policy please contact your business unit Compliance Officer

Definition of terms in italics can be found in the *Glossary*

Additional information

Approval	Corporate Executive Team (CET)
Owner	Senior Vice President, Governance, Ethics and Assurance
Author	Senior Vice President, Head of Audit & Assurance
Approval Date	16-SEP-2013
Effective Date	15-OCT-2013

History

Current Version:
15-OCT-2013: POL-GSK-500 v03
Policy Simplification rewrite

Previous Versions:
19-MAR-2009: POL-GSK-500 v02
Policy revision & Title change

24-SEP-2001: POL-GSK-500 v01
Risk Management and Legal Compliance