

GSK Policy		Title: Risk Management and Compliance	
Official Short Title: Risk Management and Compliance			
Key Points			
<ul style="list-style-type: none"> ➤ For specified business units designated by the ROCC, the CET member is responsible for establishing an appropriate risk management and compliance infrastructure within their Business Unit to oversee and ensure the identification and implementation of internal controls for significant risks. ➤ Risk management activities and compliance controls must be embedded within normal business operations ➤ Each business has the responsibility to implement and oversee monitoring activities for risks that are inherently significant to that business. ➤ All GSK managers are expected to communicate significant issues promptly via line management and via GSK's internal control framework. 			
Why do we have this policy?			
<p>GSK is committed to having an effective risk management process. This enables management to operate a risk-based approach in establishing internal control systems within their organizations to effectively mitigate or control their significant risks. This is recognized as an integral part of good management practice and is required as part of GSK's compliance with Combined Code requirements. This policy outlines the framework for managing risk within GSK.</p>			
What does this policy say?		Who in GSK has general obligations under this policy?	
<div style="border: 1px solid black; padding: 5px; display: inline-block;">The Basics</div>	1. Purpose 2. Scope		All GSK Staff <input checked="" type="checkbox"/>
	<div style="border: 1px solid black; padding: 5px; display: inline-block;">Specific Requirements</div>	3. Responsibilities 4. Risk Management and Compliance Boards and the Risk Oversight and Compliance Council 5. Risk - Identification, Assessment and Treatment 6. Audit and Monitoring 7. Communication of Issues	
		Audit, Compliance, & Quality <input checked="" type="checkbox"/> Communications <input type="checkbox"/> Govt. & External Affairs <input type="checkbox"/> Finance <input type="checkbox"/> Global Procurement <input type="checkbox"/> HR <input type="checkbox"/> IT <input type="checkbox"/> Legal <input checked="" type="checkbox"/> Manufacturing & Supply <input type="checkbox"/> Marketing, Sales & Support <input type="checkbox"/> Medical <input type="checkbox"/> Research / Development <input type="checkbox"/> Supervisors & Management <input checked="" type="checkbox"/> Senior Management <input checked="" type="checkbox"/> Other <input type="checkbox"/>	
<div style="border: 1px solid black; padding: 5px; display: inline-block;">Glossary and Administration</div>	Glossary Waivers	Administration Related Documents	Contacts: Corporate Ethics & Compliance 1-866-GSK Ethics

The Basics

1. Purpose

GSK is committed to high standards of business conduct (See [Code of Conduct](#) – POL-GSK-001) and to an effective risk management process in order to protect patient safety, employees, the environment, company assets and reputation, help achieve business objectives, safeguard shareholder investment and ensure compliance with applicable legal requirements. This policy outlines the framework for managing risk within GSK.

In order to meet these objectives:

- Risk management and compliance must be an integral part of decision making;
- Risk management activities and compliance controls must be embedded within normal business operations;
- GSK aims to identify and treat risk on a proactive basis. The emphasis must be on prevention and improved performance, rather than reactive responses to realised events;
- A culture of transparency must be encouraged and reinforced through identification, reporting, disclosure and open dialogue, to promote sharing of risk management and compliance information and good practice.

2. Scope

This policy applies to all GSK managers.

This policy defines the roles and responsibilities of the organisation in relation to risk management and compliance processes.

The Specifics

3. Responsibilities

- 3.1.** Each Risk Management and Compliance Board (RMCB) is responsible for identifying, assessing, treating, monitoring and reporting on significant risks associated with their area.
- 3.2.** Risk Owners are accountable for ensuring appropriate management processes and/or internal controls are implemented to treat significant risks.
- 3.3.** Business Unit Risk and Compliance Officers and Compliance Champions facilitate the implementation of a sound system of internal controls and compliance and an effective approach to risk management within their assigned area.
- 3.4.** The Risk Oversight and Compliance Council (ROCC) is responsible for identifying the risks that are significant to GSK, assigning risk owners for GSK's significant risks, monitoring the effectiveness of internal controls implemented to manage those risks.

- 3.5. The role of the global audit groups is to provide an objective view, independent from line management, of the adequacy, effectiveness and efficiency of internal controls and GSK's risk management framework.

4. Risk Management and Compliance Boards and the Risk Oversight and Compliance Council

- 4.1. GSK must establish the Risk Oversight and Compliance Council (ROCC) to provide oversight of risk management activities for significant risks affecting GSK. Please refer to the [Corporate Governance Booklet](#) for the ROCC's Terms of Reference.
- 4.2. Specified business units designated by the ROCC must establish a high-level Business Unit RMCB, or other suitably designated committee, to oversee and ensure the identification and implementation of internal controls for significant risks.
- 4.3. For these business units, the CET member is responsible for establishing an appropriate risk management and compliance infrastructure reporting to the Business Unit RMCB.
- 4.4. The RMCB may be a part of the executive team or constituted as a separate, stand-alone committee and should meet at least semi-annually. The RMCB should be comprised of members representing the major activities of the area.
- 4.5. The Business Unit head should ensure that the Business Unit RMCB determines, on an annual basis, the scope of risks and associated controls that fall within its oversight and outline these in an annual presentation to the ROCC.

5. Risk - Identification, Assessment and Treatment

- 5.1. Each RMCB must periodically review the significant risks facing their business. This review should include identifying operational risk, legal compliance risks and risks to the achievement of strategic goals & objectives.
- 5.2. This periodic review must occur at least annually and should be embedded / aligned within the annual planning process to ensure that significant risks are identified with changes in management direction and the external environment.
- 5.3. For each significant risk, a Risk Owner must be assigned to oversee the implementation of appropriate management processes and/or internal controls to treat that risk.
- 5.4. Risk acceptance or mitigation decisions (risk appetite) for significant risks need to be made transparent to the appropriate RMCB or executive team.
- 5.5. On an annual basis, each Business Unit head must certify that there is an ongoing program to identify, assess, and treat significant risks faced by their Business Unit.

6. Risk Monitoring

- 6.1. Each RMCB has the responsibility to implement and oversee Level 1 and Level 2 monitoring activities (refer to Appendix A) for risks that are inherently significant to their area (e.g., compliance with laws and regulations and risks associated with patient safety). Monitoring activities must be rigorous and pragmatic, but ideally should be non-bureaucratic.
- 6.2. Level 2 monitoring forms an essential control process for significant risks and must be performed by a group or individual(s) who are independent of the operation or activity being monitored. The ongoing review should be performed against an established standard such as regulations, guidelines, and policies and procedures to measure compliance.
- 6.3. Results of this monitoring activity must be made available on a periodic basis to the respective RMCB and/or ROCC as appropriate.

7. Communication of Issues

- 7.1. All GSK managers are expected to communicate significant issues promptly (e.g., a significant compliance failure) together with associated root causes and corrective actions taken and follow up diligently. Communication will typically be through line management and/or functional groups, but should also be directed through the internal control framework and to appropriate higher levels of management as appropriate.

Glossary & Administration

Glossary

Risk: A potential event that creates uncertainty or could adversely affect the expected achievement of business objectives

Significant Risk: A risk, or combination of risks, to which the Business Unit/Corporate Function is exposed to that is significant in terms of severity of impact and likelihood of occurrence.

Risk Management: Risk management is the process of proactively identifying, assessing and implementing appropriate risk treatment for significant risks.

Risk Treatment: Risk treatment is the process of selecting and implementing measures to modify the significance of risk. Risk treatment measures can include risk avoidance, mitigation, transfer or retention.

Risk Appetite: Risk appetite is the amount of risk exposure, or potential adverse impact from an event, that the organization is willing to accept/retain. It is associated with the level of management process and/or internal controls that management is willing to implement to treat risks.



Significant Inherent Risks : These are risks are inherently impactful to the Business Unit/ Corporate Function however management may have implemented adequate and effective controls to mitigate them (e.g., patient safety, supply chain continuity, financial statements).

Administration

Approval: Corporate Executive Team (CET)

Owner: Simon M. Bicknell, Corporate Compliance Officer

Author: Nick Hirons, VP – Corporate Assurance

Approval Date: 19-MAR-2009

Effective Date 19-MAR-2009

History: 19-MAR-2009: POL-GSK-500 v02: Policy revision & Title change
24-SEP-2001: POL-GSK-500 v01 - Risk Management and Legal Compliance

Waivers

Any requirement of this Corporate Policy may be waived conditionally on a case-by-case basis in exceptional circumstances with written approval from the owner, the Corporate Compliance Officer or the CET. All requests for exceptions/exemptions should be directed to Corporate Ethics & Compliance (CEC).

Once approved, these exceptions will be recorded by CEC and posted on the Corporate Ethics & Compliance web community for visibility. The approved exception author/sponsor is required to notify all relevant GSK employees, contractors and third parties of the granted exception.

Related Documents

[Corporate Governance Booklet](#)

Appendix A – Audit and Monitoring in GSK

