Policy on Risk Management and Internal Control

Enterprise: VQD-POL-000847 (7.0)

Purpose

Implementing this policy ensures GSK's operations are conducted in a controlled, efficient and sustainable manner by outlining the critical elements in identifying, assessing, and managing risks that could impact operations, reputation, financial standing, and license to operate.

This policy defines minimum requirements for the governance and management of our risks and internal controls, and highlights expected risk management behaviours aligned to The Code.

Document audience scope: who needs to follow this policy?

Global Business/Function(s):	Specific audiences:
All GSK	All GSK employees, complementary workers, contracted third parties

What do you need to know / do

Our work really matters. People around the world count on us every day. We must take personal responsibility to be ambitious for patients and do the right thing to be a trusted company.

Challenge and encourage each other to be our best and deliver GSK's ambitions

The Code expects **all employees** to be our best and deliver GSK's ambitions, including:

- **Taking ownership of business activities**, considering risk when making decisions.
- **Learning from internal and external** incidents to accelerate continuous improvement.
- **Committing to risk mitigation,** managing risk and following through on actions.

Inspire great performance through leadership and teamwork

In living our Code, **Leaders** are expected to:

- Set a tone where **risk management is seen as integral to great business performance**.
- Invest in **identifying and understanding** risks within their organisation's **business activities** and **inspire** individuals to take **accountability** to manage these risks**.**
- Pursue opportunities to **discuss and recognise learnings** when incidents arise, fostering a safe environment for continuous improvement.

- **Hold teams accountable** to risk mitigation commitments, **recognising** when individuals uphold these commitments and acting with appropriate urgency when they do not.
- **Foster** an environment where people Speak Up when something is not right.

Speak up if things don't feel right

We have established Speak Up processes, enabling anyone to speak up if things do not feel right, and to report issues, concerns or potential breaches of laws, regulations or codes.

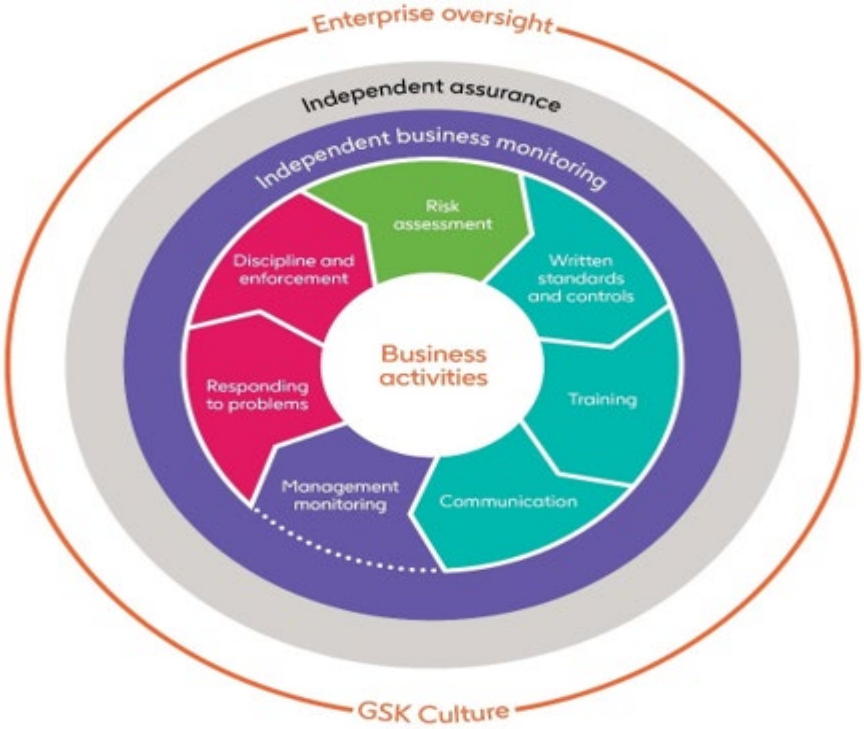
As a responsible company we manage risks effectively and take action if things go wrong

Risk management and internal control framework (ICF)

Our risk management and ICF enables GSK to be a trusted company, and includes the identification, assessment, management, reporting and oversight of risk at all levels of the organisation in a timely, proportionate, and transparent manner, supported by an effective hierarchy of governance forums.

Our ICF defines essential elements expected of our compliance and risk management programmes, aligned to industry standards and regulatory codes. It helps systematically design a set of checks and balances in a proportionate way to reduce the likelihood of risk arising.

✪Leaders should ensure elements of the ICF are in place.



Core elements of our risk management and ICF include:

- **Business activities**: Our business activities consider risk up front and throughout as activities change.
- **Risk assessment:** Assessment enables the business to prioritise and proportionately manage risk, considering the likelihood and impact. For Enterprise Risks, we use the Corporate Risk Rating Framework which considers strategic, operational, legal, compliance, and emerging risks in the external or internal environment, including those associated with third parties, during the conduct of our business activities.
- **Written standards and controls:** Our written standards and controls communicate the ideas, rules, and expectations of our company.
- **Training:** Training is provided to ensure our people operate and manage risks associated with their business activities aligned to our policies, laws, regulations, and risk appetite.
- **Communication:** We communicate risk information and learnings, promoting an environment where people feel free to speak up and protected from retaliation. We recognise when things go well, inspiring great performance with effective risk management, promoting a culture of doing the right thing.
- **Management monitoring:** Businesses and global functions ensure – ongoing - their own processes are followed, controls are effective, and gaps to strengthen controls are addressed.
- **Responding to problems:** We respond to problems by understanding the root cause or identifying relevant contributing factors and applying corrective and preventative action in a timely and appropriate way proportionate to risk, continuously learning, improving and ensuring business resilience and continuity.
- **Discipline and enforcement:** We take appropriate, proportionate and consistent disciplinary action where warranted and in alignment with local requirements for non-compliance with our Code and policies. We reward good risk management behaviour.
- **Independent business monitoring:** Independent reviews of activities and key risks aligned to legal or regulatory requirements, to continuously improve the quality of operations and ensure policies and procedures are effective and followed. Independent business monitoring is designed holistically with management monitoring and proportionate to risk.
- **Independent assurance:** Audit & Assurance provide independent assurance of the adequacy and effectiveness of our risk management and internal control environment.
- **Enterprise oversight:** Our risk governance hierarchy enables us to apply enterprise oversight in an organised and systematic way to ensure accountabilities are clear for decision making and escalation pathways. This ensures we can confirm all relevant parts of the risk management and ICF are effective or where improvements are needed. This is achieved through Risk Management and Compliance Boards (RMCBs), or other risk oversight boards, committees, or councils, reporting through to our Risk Oversight and Compliance Council (ROCC) and Board committees.

- **GSK Culture:** Our culture – Ambitious for Patients, Accountable for Impact, Doing the Right Thing - provides the management tone for the organisation, describes the spirit in which we operate and provides a reference point when we encounter difficult situations. The consistent demonstration of our culture by our leaders and people is essential in making risk management and the ICF effective. We recognise best practices for effective risk identification and management actions, and promote a strong proactive risk culture.

We are subject to external inspections and audits to assess framework adequacy.

Annually, our Businesses and Global Functions conduct a confirmation exercise to affirm leader accountability that key risks are well managed or that actions are in place to address gaps.

Enterprise and emerging risks

Annually, the Risk Oversight and Compliance Council (ROCC) assesses its significant risks to agree the corporate enterprise and emerging risks for the forthcoming year that require management attention and consideration by the Board. The Board agrees our corporate risk list. Additionally, we provide a summary of our enterprise risks in our Annual Report.

Each enterprise risk is assigned an Enterprise Risk Owner (ERO), a GSK Leadership Team member (GLT) or senior delegate accountable to an enterprise risk plan biennially which defines the risk, context, appetite, assessment, mitigation, key risk indicators aligned to reporting thresholds and governance. They define the ICF which identifies minimum controls to manage the risk across the company. The ERO provides quarterly reports to the ROCC which include any risks and mitigation, changes to the enterprise risk plans, external risk intelligence, key risk indicators and corresponding remedial actions. They hold appropriate governance forums to execute their responsibilities, including the approval of related global policies and procedures.

Emerging risks are appointed owners who provide updates to the ROCC when required.

Work to seize opportunities, solve problems, make informed decisions at pace

Risk governance hierarchy

The Chief Compliance Officer is responsible for supporting integration of risk management into businesses and global functions and provides regular updates to the Audit & Risk Committee (ARC) on the effectiveness of our risk management and internal controls. The Compliance function is responsible for supporting the development and implementation of practices to facilitate employee's compliance with laws, regulations, our policies, meeting high ethical standards and our corporate responsibility.

Risk Management and Compliance Board (RMCB)

GLT members must ensure appropriate risk management is being performed, supported by a hierarchy of RMCBs or other governance forums which promote the tone from the top, establish our risk culture, and oversee risk management effectiveness.

✪RMCBs are expected to meet at least quarterly to discuss risks, including emerging risks, specific to their business activities that could impact achievement of objectives.

Relevant enterprise risk plans and supporting ICFs are reviewed by RMCBs throughout the year and requirements implemented with relevant risks and issues escalated. Where appropriate, risks identified are reported to the ROCC quarterly and to the Board and its committees. Minutes of RMCB meetings are archived in accordance with GSK Global Record Retention Schedule.

Risk Oversight and Compliance Council (ROCC)

✪The ROCC is comprised of GLT and other senior executives authorised by the Board to oversee risk management and internal control activities. The ROCC and the aligned board committees review enterprise risk plans to assess risk management and ICF effectiveness. The ROCC reviews enterprise risks quarterly, along with significant or emerging risks or issues across GSK and reports outcomes to the Audit & Risk Committee (ARC).

Board and Committee Oversight

The Board is responsible for GSK's corporate governance framework, oversees our risk management approach and approves our risk appetite.

The ARC reviews the integrity of our risk management and ICF; the key risks inherent in the business, including our enterprise risks and emerging risks; and the company's process for monitoring compliance with laws, regulations, and ethical codes of practice. The ARC certifies to the effectiveness of our risk management and internal controls in our Annual Report.

The Corporate Responsibility Committee (CRC) has oversight of Enterprise Risks determined by the Board to be most relevant to the Committee's areas of expertise and responsibility. The Science committee undertakes more in-depth risk oversight of R&D related activities.

Roles and responsibilities

Roles	Key responsibilities
Employees	Comply with policy requirements, identify and escalate risks, demonstrate GSK culture.
Leaders	Ensure appropriate risk management and ICF in place to manage risks, regardless of where they occur or are managed within the organisation.
RMCBs	Ensure appropriate risk management forum gathers, manages business risks and reports on risks within hierarchy
ERO	Oversee assigned Enterprise Risk
ROCC	Assist the Board, ARC, CRC, Science Committee and GSK Leadership team (GLT) to oversee effective risk management and ICF.
GLT	Executive management of GSK. Oversees and manages risks agreed and ensures adequate reporting to the Board and committees.
Board	At the top of GSK's corporate governance framework accountable for risk management which includes: monitoring of information on major risks and exposures and decisions regarding those exposures; review and approval of internal controls and risk management policies and processes.

Roles	Key responsibilities
Board Committees	ARC, CRC, and Science Committee support the Board with its responsibilities. Defined remit includes oversight of Enterprise Risks determined by Board to be most relevant to the Committee's areas of expertise and responsibility.

What monitoring is required for this policy?

Leaders are accountable to ensure risk management activities are aligned with this policy. Questions on risk management and monitoring can be raised to Compliance.

Glossary

Definitions of terms in this document can be found online GSK Written Standards Glossary.

Term	Definition
Risk	Potential events that create uncertainty or could affect achieving business objectives
Enterprise Risk	The most relevant risks to GSK's business, financial conditions and operations that may affect our performance and ability to achieve objectives. Enterprise risks include, but are not limited to, risks we believe could cause actual results to differ materially from expected and historical results, those that could result in events or circumstances that might threaten company's business model, future performance, solvency or liquidity and reputation. GSK refers to Enterprise Risks as Principal Risks externally. Under GSK's risk management framework, enterprise risks are determined annually by the ROCC and agreed at the ARC. Enterprise Risks warrant active oversight at the ROCC (or GLT as agreed) with an Enterprise Risk Owner responsible for risk oversight.
Significant risk	A risk, or combination of risks, to which the Business, Function or Group is exposed to that is significant in terms of severity of impact and likelihood of occurrence.
Internal Control Framework (ICF)	A set of components that provide foundations for designing, implementing, monitoring, reviewing and continually improving risk management. The ICF supports the implementation of requirements within this Policy.
Emerging Risk	Risks on the three-year horizon, in line with GSK's viability statement, or risks where GSK needs to know more about how likely they are to materialise, or what impact they would have if they did, and where additional evaluation is needed.
Enterprise Risk Plan (ERP)	Strategic plans that define and describe risk, its context and how it may occur, the risk assessment, risk appetite, risk treatment approach, and actions Businesses and Functions need to take in line with GSK's ICF. ERPs also enable our Board committees to assess the effectiveness of our risk management strategies.

Where to raise questions, concerns or exceptions

If you are unsure about how to apply this policy, or feel you need to raise an exception to it please bring this to the attention of your manager, supervisor or Compliance Business Partner.

If you see any violations of this company policy, please report it through the appropriate Speak Up channels. To find your local Speak Up integrity line number or to report online, please visit: **www.gsk.com/speakup**

References – related documents and information

Doc number and name	Doc relationship
VQD-POL-001179: The Code (Translations available)	Expectations for employees, complementary workers; unites culture and responsible conduct
VQD-GUI-011335: GSK Risk Rating Guidance (English)	Guidance to perform risk assessments required under policy.
VQD-GUI-011334: Internal Control Framework Overview	Additional guidance on ICF to support policy.
VQD-GUI-011333: RMCB Guidelines	Additional guidance on responsibilities of RMCB
VQD-GUI-011332: Risk Oversight and Compliance Council Terms of Reference	Additional guidance on responsibilities of ROCC

Information	Where to find it
Web Communities	ERM Resource Hub intranet site

Administration – document governance

Governance Board approval	Risk Oversight and Compliance Council (ROCC)
Owner	Chief Compliance Officer
Author	Enterprise Risk Management Director
Current version:	VQD-POL-000847 (7.0) See header and/or signature page for effective date. Changes since last revision: – Aligns to new template, The Code and culture; broader inclusion of internal control framework and leadership requirements. – Clarification of responsibilities, including GLT, ROCC, CRC and Science Committees and alignment with Corporate Governance Booklet. – Text simplification, elimination of references to adopt/adapt. – Author, owner and governance approval updated.
Previous versions:	25-APR-2019: VQD-POL-000847 (6.0); 12-MAR-2019: VQD-POL-000847 (5.0) 23-JAN-2015: VQD-POL-000847 (4.0)
Document alias:	POL-GSK-500
Records retention:	Retain versions in accordance with GSK Records Retention Schedule code GRS058 unless over ridden by an active Legal Preservation Notices.