OML REGULATORY COMPLIANCE RISK POLICY

Policy Number
P10

Risk Policy Owner
OML Chief Risk Officer

Contact
OML Group Chief Compliance Officer

Version/Date
Version 3/Approved 25 August 2020

Effective Date

This Policy was approved by the OML Board Risk Committee. It is effective from 01 September 2020.

Group Governance Requirements

This Policy must be read in conjunction with the requirements of the OML Group Governance Framework (GGF) and the OML Enterprise Risk Management Policy.

Policy Waiver Process

The prescribed waiver process must be followed where a subsidiary can demonstrate justification for specific alternative arrangements to meeting the Policy requirements.

OLDMUTUAL

1. What is the purpose of this policy?

This Policy forms part of the Old Mutual Limited (OML) Group Governance Framework (GGF) and its objective is to set the OML Group-wide principles for the management of Regulatory Compliance risk, defined as the risk of breaching laws, regulations or regulatory directives.

The OML Enterprise Risk Management (ERM) Policy sets out the overarching principles for the management and escalation of all risks and risk events identified in the ERM Risk Classification Model, including Regulatory Compliance risk.

This Policy must be read in conjunction with the OML ERM Policy and the requirements of the other applicable policies of the OML Risk Policy Suite, particularly the Market Conduct and Legal risk policies.

This Policy is supported by detailed subordinate Regulatory Compliance policies, each setting out their own specific Regulatory Compliance requirements as defined from time to time.

The OML Group Chief Compliance Officer (OML Group Compliance) is mandated by the OML Board Risk Committee (BRC) to oversee implementation of this Policy, determine whether subordinate Regulatory Compliance policies are required, designate a Policy Owner for these policies and prescribe minimum standards for related methodologies, processes and tools, including the proportional application of requirements and the approval of related waivers and risk exposure acceptances.

This policy must be managed and maintained as per the requirements set out in the OML ERM policy.

2. Who does the policy apply to?

This Policy is applicable to OML and all subsidiaries that form part of the OML Group where Old Mutual as shareholder has effective management control. In instances where Old Mutual as shareholder does not have effective management control, this Policy will apply insofar as it has been agreed with the other shareholders. No subsidiary is out of scope of this Policy unless it is expressly indicated.

Boards of subsidiaries must adopt this Policy and ensure all the applicable requirements are implemented and complied with unless it is expressly agreed otherwise. Boards must ensure local regulatory requirements that apply are included in policies adopted at subsidiary level. Local regulatory requirements prevail where such requirements are more rigorous or in conflict with this Policy. Where appropriate, subsidiaries must apply for waivers from the OML Risk Policy Owner.

The adoption and implementation of this risk policy must be aligned to the requirements of the GGF and the OML Board-approved proportional governance principles.

3. What risks are managed by this policy?

The ERM Risk Classification Model includes Regulatory Compliance risk in the Level 1 Legal & Regulatory risk definition, defined as the risk of not applying or conforming to the law, or breaching laws, regulations or directives, resulting in fines, sanctions, reputational damage and/or financial loss.

3.1 Regulatory Compliance risk (distinct from Legal risk and Tax risk which is dealt with separately) is classified as the risk of breaching laws, regulations or regulatory directives, resulting in possible fines, regulatory sanctions, reputational damage and/or financial loss.

3.2 Strategic Stakeholder Management risk may arise where there are ineffective relationships with regulatory authorities, impacting the ability to comply with current or future legislation, influence future legislation and/or correctly interpret applicable legislation.

3.3 Regulatory Compliance risk may arise in any of the jurisdictions where the OML Group conducts operations and could include breaches of any requirement included in the OML Regulatory Universe.

3.4 An important consideration is the potential impact on the operations and reputation of the OML Group of legislation with extra-territorial impact, particularly from trading blocs and countries with an important role in the operation of global banking, financial and trading systems. Examples include European Union (EU) privacy and data protection laws, the UK Anti-Bribery Act and the US Foreign Corrupt Practices Act (FCPA).

3.5 Potential impacts of Regulatory Compliance breaches include:

- Business not obtaining regulatory approval or authorisation and/or the imposition of prohibitive regulatory capital requirements.
- Breaches of laws, regulations or mandate agreements, resulting in regulatory intervention, fines, or restrictions on the ability to operate, including suspension or withdrawal of licenses.
- Failure to adapt to regulatory change ultimately resulting in an inability to continue trading and/or in missed market or business opportunities.
- Negative impacts on customers, litigation and/or reputational impacts arising from Regulatory Compliance failures in relation to Treating Customer Fairly (TCF) outcomes.

4. What risk appetite statements apply to this policy?

The OML Group's risk preferences and appetite limits are set out in the OML Risk Strategy document which describes specific risk preferences and metrics. This Risk Strategy is reviewed at least annually by the OML Board and subsidiary risk preferences and appetite limits may need to be adjusted accordingly.

We are committed to complying with regulatory requirements and have **zero tolerance** for deliberate non-compliance. However, we acknowledge that non-compliance may occur from time to time and where such risks arise appropriate steps will be taken to mitigate these. We also have **no tolerance** for being uninformed of regulatory changes that could have a material impact on our business operations, our licence to operate, strategic objectives or could cause reputational damage.

5. What are the minimum mandatory requirements of this policy?

5.1 Boards of subsidiaries must approve the Regulatory Compliance Strategy, consider aggregated levels of Regulatory Compliance risk, obtain assurance that Regulatory Compliance requirements are implemented in the business, approve the annual high level Regulatory Compliance operational plan setting out compliance activities to be conducted, understand how they will be resourced and be satisfied that those resources will be adequate.

5.2 Boards of subsidiaries must receive and review regular reports on the nature and extent of all material Regulatory Compliance risks and exposures, including the:

- extent to which the business is ready to comply with emerging laws and regulations, including changes to existing requirements,
- occurrence of any regulatory non-compliance events and/or findings raised in the business (including compliance-related control breaks, breaches and regulatory enforcement actions),
- overall status of Regulatory Training in the business,
- adequacy and effectiveness of related processes and controls and any Regulatory Exposures identitied in the business
- status of any mitigating actions agreed with management; and
- status of engagements with the Regulator.

5.3 Management has primary responsibility for ensuring business products, procedures, processes, systems, external reporting and disclosures to the regulator comply with applicable regulatory requirements, that employees and staff are adequately skilled and experienced, that they conduct themselves in a manner that complies with applicable regulatory requirements and for building a business culture that supports the objectives of this Policy.

5.4 Management is responsible for developing and implementing procedures and controls to manage and report on their Regulatory Compliance risk and exposures, including conducting periodic risk assessments on key business processes and controls and taking timely management and/or disciplinary action in response to any regulatory non-compliance related risk events (including compliance-related control breaks, breaches and regulatory enforcement actions).

5.5 Management must consider Regulatory Compliance risk as part of business planning, monitor the external environment and prepare the business strategically and operationally in a timely manner for emerging and new laws and regulations, particularly where these may adversely impact current business models, require significant investment of resources or require significant changes to business products, procedures, processes or systems.

5.6 Primary responsibility for the relationship with OML regulators resides with the OML Group Chief Compliance Officer. Having regard to the importance of a uniform and co-ordinated regulatory engagement model, subsidiaries must ensure that a regulatory engagement model, aligned to the approach established by the OML Group Chief Compliance Officer, is put in place to manage relationships and interaction with all key regulators overseeing their business, ensuring that regulatory risk is managed and trust is built and maintained with regulators.

5.7 Subsidiaries must establish and maintain an adequately resourced Compliance Control Function in accordance with the approved OML Group Compliance Mandate and ensure appropriate integration with the OML and subsidiary risk management and internal control systems, as well as the requirements of the OML Group Combined Assurance Framework. This Mandate is attached as **Annexure A**.

5.8 It is the task of the Compliance Control Function to formulate the Regulatory Compliance Strategy and annual operational plan, consider aggregated levels of compliance risk, perform independent monitoring of the extent of compliance in the business with applicable laws, regulations and directives using a risk-based approach and to provide assurance to subsidiary Boards and to OML Group Compliance that regulatory requirements are being adhered to, related controls are working as intended and any mitigating actions are effective.

5.9 Management may not abdicate or delegate their responsibility for ensuring the business operates in accordance with applicable regulatory requirements to their local Compliance Control Function or to an outsourced function and they retain overall accountability for monitoring any outsourced functions, including such a function's adherence to applicable regulatory requirements.

5.10 Where key business functions or operations, including compliance oversight or monitoring are outsourced, regular reviews must be performed by the Compliance Control Function to ensure both the frequency and quality of the oversight or monitoring activities being undertaken by management meet applicable regulatory requirements and that any exceptions or breaches are being addressed and satisfactorily resolved.

5.11 Management must immediately report instances of actual or potential regulatory non-compliance to their local Compliance Control Function, including providing details of the management actions being undertaken to address the non-compliance and to mitigate the impacts or potential impacts on the business. Management must inform their local Compliance Control Function of all proposed waivers in respect of the minimum requirements of this Policy and the proposed exposure related to a material Regulatory Compliance risks.

6. What needs to be pre-approved and escalated?

6.1 Prior Approval:

6.1.1 Subsidiaries must obtain prior approval for material deviations from the mandatory requirements of this Policy or the prescribed Regulatory Compliance-related processes, methodologies and tools, from the OML Chief Compliance Officer. Approval of deviations may only be granted for specified periods of time and must be reviewed annually.

6.1.2 Subsidiaries must obtain prior approval for the following from the OML Group Chief Compliance Officer, before undertaking these activities at subsidiary level:

- The proposed acquisition or disposal of a legal entity in the Group.
- The reporting of any material non-compliance or regulatory breach to a regulator.
- Any proposal requiring an application for a regulatory licence for a new business activity or an application for a waiver from a regulator.
- The proposed formal risk acceptance of any material Regulatory Compliance risks.
- The proposed appointment or removal of the local Head of Compliance or equivalent of any regulated legal entity.
- Any deviations from the prescribed OML Group Compliance Control Function Mandate.

6.2 Escalation:

6.2.1 Subsidiaries are responsible for immediately escalating identified material compliance breaches, exposures, new material compliance risks, risk events or material non-compliance with this Policy, using the prescribed processes, methodologies and systems, to the OML Group Chief Compliance Officer.

6.2.2 Subsidiaries are responsible for escalating the following to OML Chief Compliance Officer within 2 days of the event being identified:

- Any regulatory enforcement action or non-routine regulatory investigations being taken against a subsidiary.
- The imposition of any regulatory fines or restrictions on the ability to operate, including suspension or withdrawal of licenses to operate.
- The receipt of any report from a regulator expressing any significant concerns regarding compliance by the business.
- Any material breach of applicable laws, regulations or regulatory directives or any material disputes with a regulator.

ANNEXURE A

Revision History

Revision/approval date	Document version	Summary of changes	Approval
27 February 2018	V1	OML Risk policy developed	OMGH Board Risk Committee
12 November 2019	V2	Changes as part of the annual Risk Policy refresh for 2019	OML Board Risk Committee
25 August 2020	V3	Changes as part of the annual Risk Policy refresh for 2020	OML Board Risk Committee