



Legal Compliance Reporting – Pilot Report

Outcome requested	Audit and Risk Committee is asked: [a] to consider the LCR pilot report from a review conducted with the Finance business area; and [b] to note that a full LCR report will be submitted to the Committee in March 2025, and any significant changes to the risk profile will be highlighted at the September 2024 meeting.
Executive Summary	[a] The Legal Counsel undertook a pilot LCR report with Finance, employing the new LCR framework considered by the Committee in March 2024. [b] Finance reported only one material change to legal compliance risk in the coming 12 months, being OECD Pillar 2 regulations. Finance is identifying required steps to ensure compliance within risk tolerance. Finance otherwise maintains a register of ongoing operational, compliance and external risks. [c] Finance otherwise noted the importance of communication and accessibility of compliance obligations across the University to ensure broad awareness and 'buy-in' from internal stakeholders. [d] Legal Counsel identified no material concerns in relation to legal compliance risk in the Finance business area.
QMUL Strategy:	Good governance supports all aspects of the strategy
Strategic Risks:	Compliance; operational legal risk
Subject to prior and onward consideration by:	For the Committee only.
Confidential paper under FOIA/DPA:	No
Equality Impact Assessment:	Not required.
Timing:	This paper reports on the pilot of a new approach to legal compliance reported that was considered by the Committee in March 2024.
Author(s):	Thomas Shaw, Legal Counsel
Date:	12 June 2024
Senior Management Sponsor	Jonathan Morgan, Chief Governance Officer and University Secretary

Introduction

1. At the March 2024 meeting, the Committee noted the new Legal Compliance Reporting (**LCR**) framework submitted by Legal Counsel (paper ARC23/28). As noted in that meeting, a pilot report was to be undertaken and reported to the Committee in its June meeting.
2. Based on the information below, the University's Legal Counsel identified no material concerns in relation to legal compliance risk in the Finance business area, and considers that Finance is engaging meaningfully with compliance risks. Discussions also emphasised the broader importance of staff-level 'buy in' to internal compliance processes, and the application of risk tolerance in balancing compliance certainty against efficiency and practical limitations

Basis for assurance

3. The Chief Governance Officer and University Secretary maintains a register of compliance areas that are relevant to the University's current and planned operations, with Senior Executive Team and functional leads for each area (**Annex A**).
4. The pilot was undertaken in collaboration with the Finance business area, involving the CFO, and senior staff within the Finance Department (**Finance Staff**).
5. Finance Staff were asked to self-report on any anticipated material risks arising from regulatory or legal changes over the coming twelve months. Responses were discussed during a subsequent meeting, as well as broader approaches to managing legal compliance risk. The outcome of that engagement is summarised below. No areas of systemic non-compliance with identified legal requirements within Finance's remit had been identified in the last three years.
6. This report also benefits from two recent audits provided to the Audit and Risk Committee in November 2023 which support management of the legal compliance risk in the Finance business area:
 - 6.1. external audit report 2022-23: this report did not identify any areas of concern in relation to legal compliance that had been encountered in the course of the external audit; and
 - 6.2. internal audit report 2022-23: this report included a 'significant assurance with minor improvement opportunities' rating for the internal audit on Core financial controls.
7. All staff are required to complete the following mandatory training in Anti-Bribery Essentials and the Criminal Finances Act. The University has recently implemented a new Learning Management System which will make compliance with this training more easy to monitor.

Anticipated legislative or regulatory risks

8. Finance reported one anticipated legal compliance risk arising from changes to the regulatory or legal environment over the coming twelve-month period – the OECD Base Erosion Profit Shifting (**BEPS**) and Country by Country Reporting (**CBCR**) regulations.
9. The University recently became subject to the CBCR regulations due to its global operations and meeting the turnover threshold (€750M turnover in the last financial year).

As a result, the University will need to review its operating procedures and agreements to ensure compliance consistent with Queen Mary's risk tolerance.

10. The BEPS regulations are intended to reduce tax base erosion resulting from multinational corporations exploiting differences in tax regimes between OECD member countries. The BEPS regulations aim to ensure large multinational companies pay a minimum level of tax in each jurisdiction in which they operate. Queen Mary is, then, not the intended target of the BEPS regulations, but must nonetheless ensure compliance.
11. The Finance department intends to review the applicable regulations, whether through internal work, engaging its external networks (e.g. the British Universities Finance Directors Group), or retaining external advice, as required to ensure compliance within the required timeframes.
12. The Finance otherwise maintains a risk register that includes legal compliance risks (relevant risks extracted at **Annex B**). The register monitors a range of ongoing risks, including Brexit impacts, CMA and OfS compliance, incident management, health and safety, GDPR compliance, financial controls risks, and tax risks. In many instances, these risks are also monitored by other teams within the University (for instance, CMA and OfS regulations, GDPR compliance, and health and safety are also monitored by Governance and Legal Services, amongst others). Additional risks monitored by Finance and included elsewhere in the risk register include compliance with degree apprenticeship regulations, and the any potential application of the Public Contracts Regulations. Finance's response to the newly applicable regulations will fall under their existing identified risk categories.

Broader compliance culture

13. Legal Counsel and Finance Staff discussed broader topics on how best to identify, mitigate, and communicate legal compliance risks. The discussion was productive, collaborative, and demonstrated awareness of the relative merits, and limitations, of various approaches to legal compliance risk.
14. Numerous topics were covered, including: identification of external risks through external adviser updates and membership with external bodies; the challenges in communicating processes internally and maintaining visibility over university operations; and the value in communication channels between different University teams. In particular, the discussion noted the importance of: compliance processes being accessible, digestible, and actionable for internal stakeholders (i.e. making them 'user friendly'); and working with Faculty and School staff to ensure knowledge and engagement is embedded across the University rather than concentrated centrally.
15. The discussion recognised the importance of staff-level 'buy in' to internal compliance processes, and the application of risk tolerance in balancing compliance certainty against efficiency and practical limitations.

Ongoing LCR Reporting

16. The new LCR reporting framework has demonstrated value and effectiveness in fostering mutual engagement, discussion, and visibility of legal compliance risk – both centrally within Governance and Legal Services, and with the department engaged.

17. Going forward, Governance and Legal Services will ensure the LCR reporting framework continues to remain flexible and adaptive to ensure it remains an effective and meaningful means of engaging with legal compliance risk.
18. The next report will be brought to the Audit and Risk Committee's March 2025 meeting, and will cover both the Finance and Governance and Legal Services legal areas. Legal areas overseen by the Chief Operations Officer (see Annex A), as the widest ranging areas, will be dealt with in the June 2025 report.
19. To ensure broad visibility of compliance risks across the University, the LCR process will also pro-actively engage with other operational compliance centres on an ongoing basis, drawn from Part 2 of the Risk Register. Priority will be given to those risks that are out of tolerance, or which have seen significant improvements to bring the risk within tolerance.

Annex A – Legal compliance register

Business Area	Legal Area	Owner	To be completed by
Governance	Office for Students	CGO (non-financial) CFO (financial)	Director of Governance and Legal Services Director of Finance
	Charity Law (as it applies to QMUL and QMSU)	CGO	Director of Governance and Legal Services
	Fundraising	CGO	Director of External Relations
	Education Act, including: Freedom of Speech Council responsibilities under 1994 Education Act for the Students' Union Public Interest Disclosure	CGO	Director of Governance and Legal Services
Finance	Finance, tax, procurement, and company law	CFO	Director of Finance
	Standards of business conduct: Fraud & Bribery Modern slavery	CFO	Director of Finance
Equality and Diversity	Equality and diversity legislation	COO	Director of Human Resources
Staff and student matters	Employment legislation	COO	Director of Human Resources
	Occupational health	COO	Director of Human Resources
	Immigration and asylum	COO (staff) CGO (students)	Director of Human Resources Director of Student Experience
	Safeguarding	CGO	Director of Student Experience
	Competition Law and Consumer Protection	CGO	Director of Governance and Legal Services
	Counter-terrorism	CGO	Director of Student Experience
Estates	Property law, buildings and maintenance	COO	Director of Estates and Facilities
	Environmental law	COO	Director of Estates and Facilities
Academic and research	Research governance, including: Clinical research Research integrity International research security and compliance	COO	Director of Research and Innovation
	Intellectual property and copyright	COO (IP) CGO (copyright)	Director of Technology Transfer and QMI Director of Student Experience
	Interjurisdictional matters (e.g. in relation to partnerships)	CGO	Director of Governance and Legal Services
	Animal welfare	COO	Director of Biological Services
Health and Safety	<i>Treated separately</i>	COO (operations) CGO (monitoring)	Director of Estates and Facilities Director of Health and Safety
Information Governance	Freedom of Information Data Protection Computer misuse	CGO (information) COO (security)	Director of Governance and Legal Services Chief Information Officer

Annex B – Finance risk register excerpt

Operational, Compliance and External Risk

15.01	16. Incident Management and Business Continuity Relevant KPI: --- ---	Failure to respond effectively to exceptional events. Caused by inadequate planning and training for staff across the University. Leading to significant disruption to University operations causing damage to the student and staff experience.	The University has focused previously on improving the resilience of its digital infrastructure and business continuity arrangements for some high-impact operations. Gaps in governance, training and business continuity planning across individual areas need to be addressed and greater account needs to be taken of the growth in off-campus and overseas activities. The University has a low appetite for risk in this area and intends to minimise its exposure to exceptional events as far as possible. Risk Tolerance = 4	Current Controls: <ul style="list-style-type: none"> Whatsapp & Teams group in place for FLT. [Director of Finance] [A, Q3 2025, ongoing] Individual team whatsapp and Teams group in place to ensure communication channel. (Team Manager) [A, Q3 2025, ongoing] Business continuity plans are in place and need to be further communicated (Finance Leadership Team) [5, Q4 2025] Further Controls: <ul style="list-style-type: none"> Review and understand ITS business continuity plan for all core finance systems [Finance Leadership Team] [D, Q3 2024] Notes:	Impact: 4.0 Likelihood: 3.0 Score: 12.0	Impact: 4.0 Likelihood: 2.0 Score: 8.0 Dir: ←→ OUTSIDE OF TOLERANCE	Impact: 3.0 Likelihood: 2.0 Score: 6.0 Target Date: _____ _____
16.02	17. Compliance - i. Health and Safety Relevant KPI: --- ---	Failure to safeguard sensitive and confidential information Caused by inadequate policies, failure to follow policy, lack of training and inadequate systems to ensure information security. Leading to litigation, financial penalties and reputational damage for QMUL. Loss of competitive advantage, research continuity and national security implications. Loss of business opportunity due to lack of accreditation.	The University has no appetite for risking the health and safety of students, staff and visitors and will fully obey the Health and Safety at Work Act 1974 and the Management of Health and Safety Regulations 1999. A stronger compliance culture is being established through more effective leadership, training and escalation pathways. Risk Tolerance = 5	Current Controls: <ul style="list-style-type: none"> Wellbeing check in during team meetings and 121s ensuring colleagues know how to escalate any concerns, managers are alert to and spotting any signs of potential wellbeing deterioration (Finance Leadership Team) [A, Q3 2025, ongoing] Mental health first aiders within Finance, who circulate and share information (Finance Leadership Team) [A, Q3 2025] Communicate and encourage access to Queen Mary support (Finance Leadership Team) [A, Q3 2025] Further Controls:	Impact: 2.0 Likelihood: 3.0 Score: 6.0	Impact: 2.0 Likelihood: 2.0 Score: 4.0 Dir: ←→	Impact: 2.0 Likelihood: 2.0 Score: 4.0 Target Date: _____ _____
17.01	17. Compliance - ii. Data Protection (GDPR) Compliance Relevant KPI: --- ---	Failure to show a duty of care towards students, staff and visitors regarding their health and safety. Caused by an ineffective compliance culture and health and safety controls. Leading to harm to one or more individuals, potentially resulting in litigation, fines and reputational damage.	Given data protection legislation and the current cyber environment the University must accept some appetite for risk in this area, subject to safeguarding our staff and students. Risk Tolerance = 12	Current Controls: <ul style="list-style-type: none"> Information is stored within systems and share drive areas, with restriction to each area of Finance. (Finance Leadership Team) [A, Q3 2025] Information is available only to staff if relevant to carry out their role. (Finance Leadership Team) [A, Q3 2025] Segregation of duties in place to ensure compliance and minimise risks. (Finance Leadership Team) [A, Q3 2025] regular review information storage and compliance - Documentation retention (Finance Leadership Team) [5, Q3 2025] Further Controls:	Impact: 4.0 Likelihood: 3.0 Score: 12.0	Impact: 3.0 Likelihood: 2.0 Score: 6.0 Dir: ←→	Impact: 3.0 Likelihood: 1.0 Score: 3.0 Target Date: _____ _____
20.01	17. Compliance - v. CMA Compliance Relevant KPI: --- ---	tbc Failure to: comply with legal or regulatory requirements Caused by: lack of planning or human error Leading to: fines or reputational damage	The University has a low level of appetite for CMA compliance risk Risk Tolerance = 9	Current Controls: <ul style="list-style-type: none"> Procurement policies and process have embedded methods of transparency, fairness and upholding competition. This complies with the CMA requirements. (Deputy Director of Procurement) [A, Q3 2025] Ensuring fee regulation is updated and published annually (Deputy Director of Finance, Financial Control) [A, Q3 2025] Review CMA requirements (Finance Leadership Team) [A, Q3 2025] Further Controls: <ul style="list-style-type: none"> Ensure ongoing communication to raise the importance of compliance (Finance Leadership Team) [A, Q3 2023, ongoing] Notes:	Impact: 4.0 Likelihood: 3.0 Score: 12.0	Impact: 4.0 Likelihood: 2.0 Score: 8.0 Dir: ←→	Impact: 3.0 Likelihood: 1.0 Score: 3.0 Target Date: _____ _____
22.01	17. Compliance - vii. OFS compliance Relevant KPI: --- ---	Failure to: comply with legal or regulatory requirements Caused by: lack of planning or human error Leading to: fines or reputational damage	The University has a low level of appetite for OFS compliance risk. Risk Tolerance = 8	Current Controls: <ul style="list-style-type: none"> Maintain an annual timetable for required returns to be submitted (Finance Leadership Team) [A, Q3 2025, ongoing] Further Controls:	Impact: 4.0 Likelihood: 3.0 Score: 12.0	Impact: 4.0 Likelihood: 2.0 Score: 8.0 Dir: ←→	Impact: 4.0 Likelihood: 1.0 Score: 4.0 Target Date: _____ _____
25.01	17. External Environment - iii. BREXIT Relevant KPI: --- ---	Failure to: comply with legal or regulatory requirements Caused by: lack of planning or human error Leading to: fines or reputational damage	[No Title]	Current Controls: <ul style="list-style-type: none"> Guidance for import/ export has been compiled and communicated to colleagues via e-bulletin and emails. (Deputy Director of Procurement) [A, Q3 2025] Supply chain analysis carried out to ensure mitigations can be implemented for risks around labor, supply chain, commercial and legal. (Deputy Director of Procurement) [A, Q3 2025] Brexit & covid impacts on Supply chain for IT and construction. to continuously review and understand market conditions. UK Market analysis shared with stakeholders. [A, Q3 2025] Ongoing review of legislation and guidance updated and shared. (Deputy Director of Procurement) [A, Q3 2025] Further Controls:	Impact: 4.0 Likelihood: 4.0 Score: 16.0	Impact: 3.0 Likelihood: 2.0 Score: 6.0 Dir: ←→	Impact: 2.0 Likelihood: 2.0 Score: 4.0 Target Date: _____ _____