

Three Lines of Defence

A governance model that separates risk work into three distinct roles: management that owns and controls risk, risk and compliance functions that oversee it, and internal audit that gives the board independent assurance that the first two are working.

PREPARED BY _____ DATE _____

1 FIRST LINE: MANAGEMENT OWNS AND CONTROLS RISK

Operational management and the teams delivering products and services. They own the risks their activities create, design and operate the day-to-day controls, and are accountable for fixing what breaks.

2 SECOND LINE: RISK AND COMPLIANCE FUNCTIONS OVERSEE

Specialist functions such as risk management, compliance, financial control and quality. They set frameworks and policy, challenge and support the first line, and monitor and report on risk across the organisation, without owning the controls themselves.

3 THIRD LINE: INTERNAL AUDIT ASSURES INDEPENDENTLY

Internal audit, reporting functionally to the governing body. It provides independent, objective assurance on the adequacy and effectiveness of governance, risk management and control, including the work of the first and second lines.