

Three Lines Model – Best Practice

This Best Practice paper looks at the **Three Lines Model** which is an effective structure used within financial services firms to assist in the achievement of objectives and facilitate strong governance and risk management.

What are the three lines?

The Three Lines Model has been in existence for over 20 years. A series of economic events, including the 2008 financial crisis, highlighted systemic deficiencies in risk identification, ownership, oversight, and governance to effectively manage risks in financial services. One of the responses to this was creation of the Three Lines of Defence, now referred to as the Three Lines Model.

A Three Lines Model aims to address control deficiencies by clarifying risk management roles and responsibilities and is now a requirement for most regulated firms who employ three lines as part of their operational risk governance and risk management structure. A strong risk culture, good communication, understanding, and a strong sense of risk awareness, can provide comfort to a firm's governing body when used in conjunction with this approach.

The most common approach is for the three lines to be comprised of the following:

1. **First-line** generally comprises roles most directly aligned with the delivery of products and/or services to the customer of a firm, and managing risk within these areas.
2. **Second-line** assists with managing risk by monitoring and challenging risk-related matters and generally comprises operational risk management and compliance functions.
3. **Third-line** is the audit function and provides independent and objective assurance and advice on the adequacy and effectiveness of governance and risk management within both first and second-lines.

Relationship between lines 1 and 2

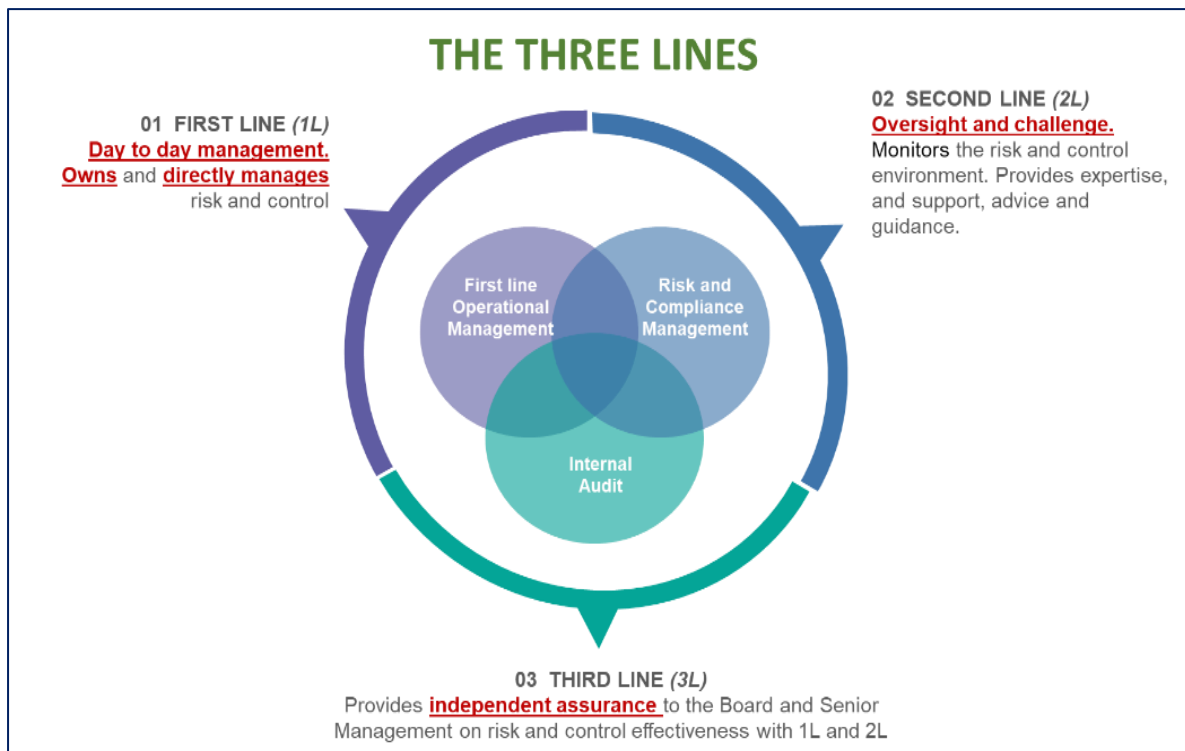
The first-line is primarily responsible for managing risks within a firm through the design and implementation of appropriate mitigating controls, which are then owned and managed, with the first-line accountable for ensuring effective day-to-day controls are in place to manage operational processes in compliance with regulations.

The second-line, comprising risk management and compliance functions, supports the first-line with advice, oversight, and challenge of the day-to-day management, control, and reporting of risks. Second-line functions promote operational compliance across a firm but should have no direct operational responsibility or authority over first-line activities.



THE TA FORUM

AML Working Group



Requirements to satisfy effective oversight

In the three lines model, the first-line is directly responsible for the acceptance and management of any operational risks and the day-to-day management of staff, business processes, and technology within the firm. The first-line will direct and make business decisions usually within an agreed overarching risk management and compliance framework.

To satisfy effective oversight the second-line is responsible for defining the overarching risk management and compliance framework, within which all business decisions are required to be made, with powers assigned by the firm's governing body.

Second-line oversees and challenges management on the design and implementation of first-line policies, as well as the evaluation, reporting, and effective control of exposures and risks.

This oversight and challenge drives second-line monitoring and assurance plans which include all potential activities or areas, including key regulatory themes and changes, that can be monitored. First-line can discuss concerns or highlight areas to be addressed within annual assurance plans, or more frequent as desired.

Potential activities or areas considered for review may include:

- Key business processes;
- Delivery of customer outcomes;
- Regulatory interest;
- Material changes (internal, regulatory, industry);
- Previous areas of concern;
- Financial crime concerns;
- Incidents (breaches, errors, near misses and complaints);
- Issues identified by the business;
- Material risks reported;
- Internal and external audit reports; and
- Formal requests from the firm's governing body.

Second-line monitoring aims to be flexible so that planned assurance focus can change as the risk landscape, or the risk profile of the firm, evolves and changes.

Second-line monitoring aims to provide oversight on design & operation of the firm's control environment and framework as it is expected to remain separate from those responsible for delivery in the first-line.

Demonstration of effective oversight

Effective oversight and assurance can be delivered by many methods within a firm. The Three Lines Model helps to identify and understand the different contributions that these various methods can provide. By defining the sources of assurance into three broad categories, it helps to understand how each contributes to the overall level of assurance provided and how best they can be integrated to be mutually supportive. For example, management assurances can be harnessed to provide coverage of routine operations, whilst third-line activity can be targeted at riskier or more complex areas.

First-line

Within the first-line and business operational areas, there are many arrangements and controls that can be used to determine how well a firm's objectives are being met, risks managed, and controls applied, for example, good policy and performance data, monitoring statistics, risk registers, reports on the routine system controls, and other management information.

Arrangements and controls are introduced by those directly responsible for delivering specific objectives or operation. Monitoring of these provides assurance that performance is managed, risks identified and addressed, and objectives are being achieved. The value of this type of assurance, despite the potential lack of independence and objectivity, comes from those who know the firm's culture, and day-to-day challenges.

Second-line

The activities associated with the second-line relate to oversight of risk management activity. The second-line remains separate from those responsible for delivery in the first-line, but is not fully independent of the firm's management chain. Second-line activities typically includes monitoring assessments or reviews carried out to determine that policy, systems and controls and quality arrangements are being met in line with expectations for specific areas of risk across the firm, for example, information assurance, security, and the delivery of key strategic objectives.

Second-line assurance provides valuable management insight into how well operational activities are being carried out, in line with set expectations and policy or regulatory considerations. It is distinct from and more objective than first-line assurance.

Third-line

This is independent and more objective assurance and generally places reliance upon assurance mechanisms in the first and second-lines, where possible, to enable it to direct its resources most effectively to areas of highest risk or where there are gaps or weaknesses in other assurance arrangements.

It also takes assurance from other independent assurance providers operating in the third-line, such as those provided by independent regulators.

Independent of the first and second-lines, the third-line operates to professional and ethical standards in carrying out its work, independent of the management line and associated responsibilities.

The third-line may include external auditors or regulators, and although they sit outside a firm can play an important role through their scrutiny of governance and control structures where this is relevant. Specific governance and risk management requirements are often set by regulators who may undertake their own independent control assessments, which can be a further useful source of assurance.

Management Information to evidence oversight

It is important that a firm's governing body or senior management receives sufficient and timely assurance information on the management of risk to enable them to exercise good and effective oversight.

Both first-line and second-line assurance should aim to provide valuable management information that informs assurance and stewardship reporting. When drawn together with third-line assurances, they provide the essential information needed to support reporting.



Management information should be produced on a regular basis, either monthly or bi-monthly throughout the year as this helps to validate the process and gives time to escalate and remedy any issues identified.

Second-line management information is likely to include the following high level reportable activities:

- **Advice and guidance:** This will include reporting on all first-line operational activities within the firm to satisfy compliance with regulations. This includes objective oversight and ongoing challenge of risk mitigation, management, and performance.
- **Oversight of business projects:** Second-line involvement in projects can help ensure that appropriate regulatory advice and challenge is given. Management information on project deliverables and timeframes ensures an independent view is presented on progress.
- **Monitoring and assurance reviews:** Second-line monitoring aims to assess whether controls to manage key regulations and risks are appropriately designed and operating effectively. Issues identified and progress on agreed management actions to address weaknesses should be reported so that senior management can understand areas of concern.
- **Regulatory change:** Firms are subject to a wide range of regulatory, legal and industry requirements. It is important for a firm to keep abreast of, understand and implement regulatory change where appropriate. Second-line activities should include monitoring and reporting of material regulatory change to ensure controls are implemented and are effective.
- **Financial crime:** A programme of anti-financial crime activities carried out by the second-line should aim to assess whether financial crime risks and controls are being managed appropriately to satisfy relevant regulations. Regular reporting on these activities will provide a robust and proportionate level of assurance as to whether the business is operating compliantly.

Important Information This document has been compiled for the use of TA Forum members only; it is for guidance purposes and has been written from the viewpoint of TA's and the administration activities that they perform for regulated firms. It is a regulated firm's responsibility to comply with the regulatory rules and ensure that they receive all required information in order that they can perform adequate oversight regularly.