The Three Lines reimagined: Critical success factors for an effective implementation of the Three Lines of Accountability

A DISCUSSION AND POSITION PAPER
Prepared by the GRC Institute

Lead Director and Author: Annette Donselaar

With thanks to the GRCI CCP/CCRP and Fellow Alumni for their contributions in our workshops.

October 2021

Executive Summary

Since 1996 the GRC Institute ("GRCI") has been the preeminent member organisation for Compliance and Risk professionals in Asia Pacific.

One of the important matters that has been the subject of discussion and debate from our members has been issues arising from their experience with implementing the 'Three Lines' model ("The Model"). To better understand these issues, the GRCI held workshops with our senior accredited members during 2021.[1]

Based on that feedback and additional research, the GRCI recommends the following:

1. The Model is built on the existing three lines, which is illustrated at Appendix 1.

2. Although the name has been recently changed to just the "Three Lines" model, we believe the deletion of the words "of defence" should be replaced by "of accountability." The "Three Lines of Accountability" title clearly states the key element of ownership at all three lines to deliver an effective business risk model.

3. Implementation of the Three Lines of Accountability by Compliance and Risk professionals should be through designing, developing and delivering critical success factors. Critical success factors are the activities that need to be undertaken in order to achieve a strategic goal. They are essential for success.

4. Five critical success factors should be used to embed the Three Lines of Accountability model into an organization:
    a. **Clarify** compliance and risk management responsibilities within an organisation and at all levels;
    b. ensure appropriate **accountability** for risk and compliance management and culture throughout the organisation;
    c. maintain structural and operational **independence** of the second line compliance and risk functions;
    d. facilitate compliance and risk **assurance** and verification; and
    e. deploy appropriate compliance and risk management **resources**.

5. Each critical success factor has supporting actions which help the Compliance and Risk professional deliver the Three Lines of Accountability model. These are discussed in detail in the paper and summarised at Appendix 2.

6. The critical success factors are supported through regular and effective engagement and communication across the three lines.

A glossary of terms used in this paper is at Appendix 3.

[1] Senior Accredited Members refers to GRCI members who have successfully completed qualifications to be accredited as a Compliance Certified Professional ("CCP") or CCP Fellow. For further details on minimum eligibility criteria, please refer to the GRCI website.

Three Lines: Purpose and structure

Since its launch in the early 2000s, the 'Three Lines' has been an important part of the risk and compliance framework, both in Australia and across the world. It has been recognized by the Basel Committee for Banking Supervision, the Institute of Internal Auditors ("IIA"), Institute of Chartered Accountants, and a number of regulators as an important model in structuring and managing risk.

The IIA was one of the first to fully document the theory of The Model and describe what is the role and responsibility of each line. The IIA states that the purpose of The Model is to help a business to achieve strong governance and risk management.[2] While the IIA updated their paper in 2020 ("IIA Paper") to become more principles based, the fundamental purpose remains; The Model is, first and foremost, a business risk model.

The IIA Paper removed the word 'defence' from the original title.[3] While no stated reason is given by the IIA for doing so, commentary suggests that removal of the word 'defence' addressed 'one of the principal criticisms of the old model, which was primarily too focused on defending against risk, rather than focusing on value creation and prospectively managing risk.'[4] The GRCI supports the removal of the word 'defence.' We consider that the use of the word 'defence' limited understanding on the potential breadth and depth of The Model by implying that the focus is for each line to 'defend' against control failures and breaches. The inclusion of the word 'defence' created confusion about the purpose of The Model.

The name of The Model is important. It should clearly convey the purpose and why The Model should be part of a business framework. To that end, the GRCI proposes renaming The Model as the 'Three Lines of Accountability.' This title clearly demonstrates the core of what The Model is trying to achieve and is consistent with the increased focus by regulators on how accountability is integral to an organisation's performance.

Delivering the Three Lines of Accountability through Critical Success Factors

One of the redeeming features of The Three Lines of Accountability model is its simplicity of design, being three separate 'lines' that have distinct but interrelated accountabilities. An illustration of The Model is at Appendix 1.

However, the generic nature of The Model has also caused debate as to how it should work in practice. Deloitte (2020) notes the overlapping of the first and second line roles and/or second and third line has limited the effectiveness of The Model.[5] Oliver Wyman (2015) argues many of the problems that stem from The Model is due to it being adopted in a 'half-hearted way'.[6] Armstrong Wolfe (2021) found, in a survey of first-line practitioners, that implementation issues stemmed from difficulties in defining the details of how The Model works in practice.[7]

For Compliance professionals the broadly defined and over-simplified concepts within The Model pose real challenges. The business (i.e., staff and management who are directly engaged in revenue

[2] International Institute of Auditors, 2020, 'The IIA's Three Lines Model, An Update of the Three Lines of Defence', July 2020.
[3] Ibid.
[4] Jeager J, 2020, 'Practitioners weigh in on the IIA's new Three Lines', Compliance Week ebook.
[5] Deliotte, 2020 'Modernising the three lines of defence model: An Internal Audit perspective'.
[6] Daisley, M., et al, 2015 'Whose line is it anyway? Defending the three lines of defence', Oliver Wyman.
[7] Armstrong Wolfe, 2021, 'The 3 Lines of Defense ('3LoD') 2021 Report: A view from the first line', June 2021.

generation for the entity), their governing body (such as a board) and/or even the regulator, look to the Compliance function to provide guidance and structure to implementing The Model. Typically, the Compliance function is regarded as the architect of The Model and is held accountable for the successful implementation within an organisation.

This places the Compliance professional with a significant strategic challenge. While The Model provides flexibility to be tailored to the nature of the industry and maturity of the entity, successful implementation can be both difficult to achieve and measure without any supporting tools or measures for success.

To help deliver the successful implementation of the Three Lines of Accountability, the GRCI recommends that Compliance and Risk professionals focus on structuring their implementation strategy with critical success factors. Critical success factors are defined as 'the few key areas of activity in which favourable results are absolutely necessary for a manager to reach their goals.'[8] They focus on the cause of success implementation; unlike key performance indicators which measure the level of success. Through using critical success factors the Compliance professional is able to achieve the goal of implementing the Three Lines of Accountability into their organisation.

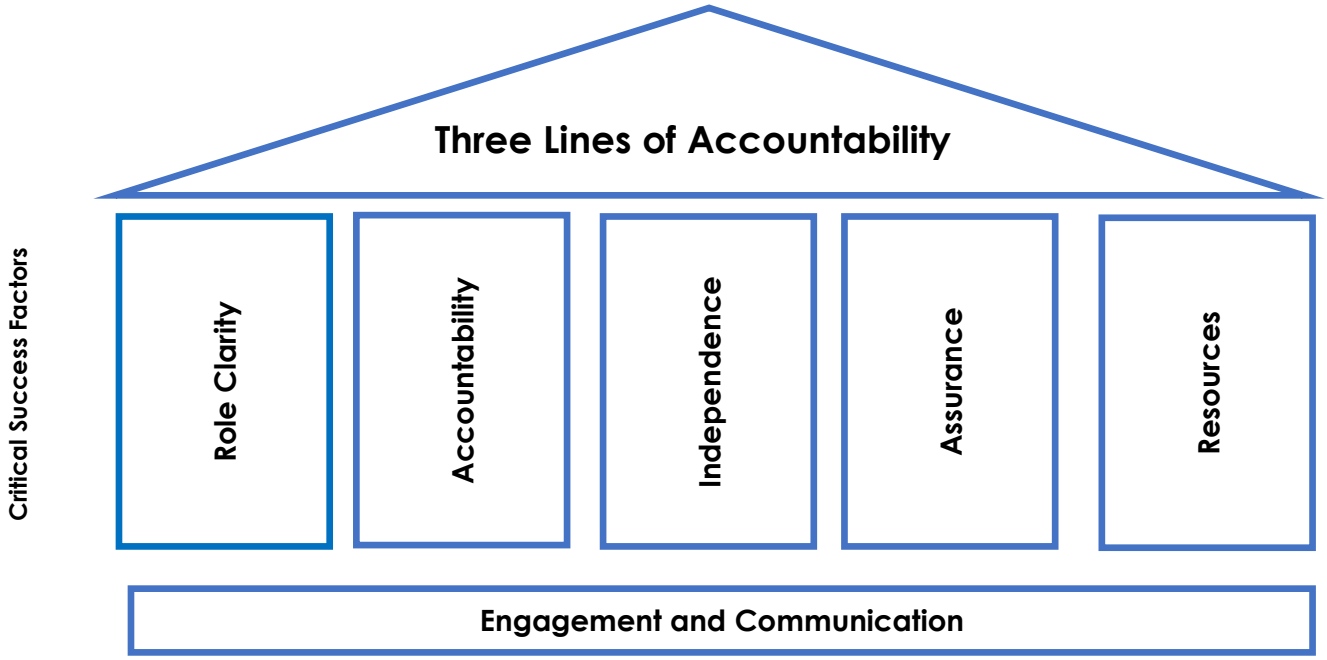
By its very definition, the factors must be 'critical' to success. The GRCI recommends five critical success factors that should be incorporated in the implementation of the Three Lines of Accountability:

1. **clarify** compliance and risk management responsibilities within an organisation and at all levels;
2. ensure appropriate **accountability** for risk and compliance management and culture throughout the organisation;
3. maintain structural **independence** of the second line Compliance and Risk functions;
4. facilitate compliance and risk **assurance** and verification; and
5. deploy appropriate compliance and risk management **resources**.

The GRCI Three Lines of Accountability Critical Success Factors approach is illustrated at Figure 1 below. Each of the five critical success factors are explained in detail in the next sections of this paper and summarised at Appendix 2.

[8] Rockart J and Bullen C, 1981, 'A Primer on Critical Success Factors', Center for Information Systems Research, Sloan School of Management, Massachusetts Institute of Technology, June 1981.

Figure 1 — Critical Success Factors for Implementation of the Three Lines of Accountability



1. Role Clarity

Since the earliest articles on The Model in 2004[9], the fundamental structural element is that it includes 'three lines.' There has been much debate as to who should be each line, what they should do, and whether there should be more than three lines. Some commentators, such as the Financial Stability Institute (2015), believe there should be recognition of a 'fourth line' (being external auditors and regulators) for financial services.[10] Even the IIA Paper states that "logically, governing body roles also constitute a "line", but this convention has not been adopted to avoid confusion."[11]

The GRCI supports the retention of only three lines for the Three Lines of Accountability for the following reasons:

- The lines should be limited to personnel who, through their actions, achieve the delivery of Three Lines of Accountability. Accordingly, the governing body, regulators and external auditors should not be considered as a separate line, but rather parties who rely upon the delivery of the documented compliance and risks standards in assessing their performance. Regulators govern stakeholders; they are not participants.
- The Chief Executive Officer and senior ('top') management are part of the first line. They are ultimately the stewards and owners of business risk. As a result, they should not be segregated into any other 'line'.

Prior to The Model being developed, there was a tendency to rely on regulators, boards and/or in-house Compliance professionals to drive the agenda in identifying and addressing risks. This led to a disjointed approach where senior management focused on revenue-generating activities, the

[9] Caprasse, D., et al., 2004, 'Three Lines of Defence: How to take the burden out of compliance', PWC Digest, Belgium
[10] Andorfer and Minto, 2015 'Occasional Paper No. 11, The "four lines of defence model" for financial institutions', Bank for International Settlements, December 2015.
[11] IIA, above n 2.

Compliance function was tasked with managing problems and breaches, and Internal Audit detected systemic issues.

The critical differentiator of the Three Lines of Accountability – and why it is supported by the GCRI – is its focus on the role of management to understand and manage its risks. As the business has direct contact with the customer, revenue and business structures, it is the first line that sees the issues first-hand. It is the front line of any organisation and is responsible to staff, stakeholders, and customers for sound ethical, economic performance. When we refer to 'the business', we are referring not only to customer-facing staff, but all other functions that support the strategy, development, sale and management of the product or service. It incorporates all of the day to day activities of the organisation, and those that perform them.

The second line, by comparison, is typically comprised of a small team, and sometimes only one person. As the Compliance professional within the firm, their role is primarily to be a subject matter expert on the structures and processes aligned with the Three Lines of Accountability and to deliver on its purpose. This is practically achieved through advice, support, governance structures and assurance. The third line (Internal Audit) is accepted as an independent team that conducts risk-based audits to ensure the adequacy and effectiveness of the Three Lines of Accountability.[12]

Designing the roles across the three lines should be adapted for the size and complexity of the business. While small organisations may not be able to employ a dedicated Compliance function, senior management should consider options that reinforces role clarity across the three lines. One option may be to engage a third-party vendor that provides specialised compliance and risk services[13]. Another could be for a first line employee to complete tasks across lines one and two. Where this approach is used, the job description should clearly split out the functions into each line to clearly demonstrate how and when they operate in practice. This is important when considering performance, managing conflicts of interest and segregation of duties. Under no circumstances should one person both complete a task and then test it.

While the term 'three lines' is used to distinguish the respective roles in The Three Lines of Accountability model, it is important to think of those roles as comprising one team, which seeks the same goal: an efficient, transparent and ethical business. The success of the Three Lines of Accountability is fully dependent upon the performance of each line. It does not work where lines attempt to shift responsibility out of one line into another. If staff in each line are aware of their role and responsibilities, the interdependencies of their actions, and supported by structured engagement, the Three Lines of Accountability model is far more effective.

The GRCI recommends the following actions be taken to deliver the role clarity critical success factor:

1. **Clear Job Descriptions.** For the Three Lines of Accountability model to be effective, setting out and documenting clear roles and responsibilities is key. Control tasks that form part of a role in the first line should be integrated into their job description. It should be treated as part of the responsibilities of the job, not a 'compliance activity' that is tacked onto a role. The job description should also clearly set out the interdependencies related to that activity and impact if not completed correctly.

2. **Avoid blurring the lines.** In larger organisations, there is a tendency to have specialised control staff in line one who may consider themselves to be part of the Compliance team. Often referred to as 'line 1.5' or 'line 1B', these roles typically provide specialised advice or conduct monitoring for the business for early detection of potential issues. Creation of a line 1.5 team is not encouraged and, if required, should be done with caution. It must be clear that such

[12] Ibid.
[13] As noted at page 29 of ISO 37301:2021 (see note 17), if the compliance function is outsourced it should be limited to the tasks and activities of the Compliance role; organisations should maintain authority and oversight of the Compliance function.

resources are utilised to provide specialist advise to the business, not remove the controls oversight and monitoring responsibilities that should sit across first line roles. To do so would defeat the purpose of line one responsibilities, which requires that all staff understand and manage the compliance and risk management programme within the organisation. The Compliance function would engage with line 1.5 staff just as they do with any other member of the first-line. Line 1.5 staff do not form part of the Line 2 Compliance function.

3. **Controls clearly appoint individual functional responsibility**. Each task in a compliance or risk control should document who is the owner, which is consistent with the tasks set out in their job description. Apart from providing clarity to the staff member involved on what they are expected to deliver, it also provides clarity for documenting the control risk owners in the compliance risk register and information to Internal Audit on who to discuss matters with when conducting their third line audits.

4. **Compliance information management and escalation**. Communication and engagement between the lines is significantly enhanced where there is a documented compliance information management and escalation policy. This outlines which matters should be reported to Compliance by the first line on a regular basis, and which matters should be escalated immediately. This can be enhanced through compliance software and other tools that facilitate transfer of information without delay.

5. **Standing working committees**. Developing and building on role clarity can only be achieved through ongoing communication. Standing working committees for all three lines to discuss issues and promote functional collaboration is strongly encouraged.

6. **Performance Metrics**. To evaluate whether roles and responsibilities in each line is fully understood, performance metrics should be in place to track compliance risk, management issues, and improvements. In creating the metrics, we recommend the following considerations:
    a. Focus on the outcomes or results, not the inputs (such as money or resources).
    b. Identify what are the important issues to measure, not the easiest.
    c. Examine results that link risk and reward. Are certain activities driving the wrong behaviours?
    d. Keep the number of metrics to a small list to assist management decision-making and judgement.

2. Accountability

Coupled with role clarity is accountability. Where a task is documented to be completed by an individual, they should be held to account for doing so. Simply put, accountability is being held responsible for one's actions.[14] This is not confined to documented controls ownership, but related actions such as culture, transparency and ethical decision making.

Regulators have held accountability as a foundation for effective compliance and risk management. The Australian Banking Executive Accountability Regime ("BEAR") and, more recently, the draft Financial Accountability Reform Bill ("FAR") were developed to 'improve the operating culture [in Financial services] to increase transparency and accountability across these sectors – both in prudential matters and conduct related matters.'[15]

What is clear to the regulators, and the GRCI, is that the most robust compliance or risk programme structure under The Three Lines of Accountability model will be ineffective if staff, and especially

[14] Muller, J., 2018, 'The Tyranny of Metrics,' Princeton, USA, p. 4.
[15] Financial Accountability Regime Bill (2021) Exposure Draft Explanatory Memorandum, p. 7.

senior line one management, are not held accountable for their actions. Structures are undermined by cultures, which is why we understand the BEAR and FAR regimes have placed additional responsibilities on 'accountable persons' as they drive and set the culture across the organisation. This not only extends to the behaviour of sales and support staff, but also the resources that senior executives are prepared to spend on compliance and risk.

Accountability then, is not just about doing your role but doing it properly, even when no-one is watching.

For first line management, the focus is increasingly acting with honesty and integrity, due skill, care and diligence, and working with regulators in an open, constructive, and cooperative way.[16] It is also about senior management leadership and 'tone from the top.' As stated in the International Standard for Compliance Management Systems: Requirements with guidance for use ("ISO 37301:2021"), it is vital for top management to clearly and visibly demonstrate their commitment to compliance in order for the business to be successful in the long term.[17]
The second-line functions (Compliance, Risk and Legal), as subject matter experts, are accountable for developing and delivering management systems which address their specific risks in the organisation. ISO 37301:2021 states that for the Compliance function this includes the delivering, overseeing and providing advice on the operation of the compliance management system.[18]

As stated by the IIA, the third line function (Internal Audit) "communicates independent and objective assurance and advice to management and the governing body on the adequacy and effectiveness of governance and risk management (including internal control) to support the achievement of organizational objectives and to promote and facilitate continuous improvement."[19]

The GRCI recommends the following actions be taken to deliver the accountability critical success factor:

1. **Training and support.** Line one staff should receive consistent messaging and on-going training on the importance of successfully completing their control-related tasks. To ensure this is built into the overall culture messaging, awareness and training programmes should be built in conjunction with the Human Resources function, and delivered regularly as part of a structured awareness, communication, and training programme.

2. **Performance assessment on impact to the entity.** Individual performance metrics should be both qualitative and quantitative. Line one staff, especially senior managers, should be measured and rewarded for their contribution to an ethical, transparent, and compliant culture.

3. **Appropriate consequence management.** Culture is shaped by example. If a line one staff witnesses poor behaviour being ignored, or worse, rewarded, it will be increasingly difficult for a Compliance professional to work with management to reinforce accountability for the actions of all involved. An effective consequence management programme, which reinforces a culture of compliance and holds all staff accountable, demonstrates first line ownership of their actions. An ineffective consequence management programme can result in the Compliance function taking actions against poor behaviours, thereby removing the accountability from line one management.

[16] Ibid, p. 14.
[17] International Organization for Standardization, 2021, 'Compliance management systems – Requirements with guidance for use, International Standard ISO 37301,' pp. vi and 25.
[18] Ibid, p. 9.
[19] Ibid, p. 6.

3. Independence

The word 'independence' is often used to discuss the roles and responsibilities of line two and three functions in The Three Lines of Accountability. The independence of line three (Internal Audit) is clear in the IIA Paper as it functionally reports to the governing body (typically the board) and is structured so that it can work "with the freedom from bias or interference in the planning and delivery of audit services."[20] Internal Audit does not report into line one (other than possibly for administrative purposes) and is directed by the governing body.

The Compliance function is in line two, and therefore separated from line one (the business) in The Three Lines of Accountability. However, unlike Internal Audit, it is part of the business model typically reporting through to the Chief Executive Officer or a member of their executive. ISO 37301:2021 states that "while maintaining its independence, it is preferable that compliance management is integrated with the organisation's other management process and its operational requirements and procedures."[21]

The Compliance function is required to challenge, advise, verify and monitor line one. This means that Compliance professionals must act independently within an organisation. Compliance is carved out as a separate line for an important reason – to ensure that there is an expert, unbiased, trained professional who can support and assist the first line in managing compliance risk.

'Independence' can be confusing for all concerned if the rules of engagement are not clear. If the Compliance function focuses too strongly on being independent, it can become disengaged from the business and be considered more as a branch of Internal Audit. If the Compliance function becomes too close to the business, it may impact its impartiality to challenge issues. ISO 37301:2021 states that independence means that the Compliance function is, as far as possible, not personally involved in activities that are exposed to compliance risks.[22]

For the Compliance function to be an integrated part of an organisation but remain independent requires the Compliance professional to be 'operationally independent.' This requires the Compliance professional to engage with the first-line and be integrated with their business objectives, but at the same time be empowered and supported to challenge decisions that do not meet the values or ethics of the organisation. This includes escalation to the governing body and regulators, where necessary. Operational independence is an integral part of the role of a Compliance professional.

To show how compliance is operationally independent the GRCI recommends that Compliance professionals develop a clearly documented value proposition for their Compliance function to deliver the independence critical success factor. That value proposition should set out the Compliance function operating model, especially how the Compliance function interacts and supports the business, and the ongoing engagement process. It should also align with the structural elements of ISO 37301:2021 to ensure that there is a consistent framework which is able to be independently evaluated.

At its core, the value proposition should show how the business and compliance goals should be aligned: to grow a sustainable business in an ethical way. This requires the Compliance professional to also be conversant with the business plan and developments, which we discuss further under Section 5, 'Resources', below.

[20] Ibid.
[21] Ibid, p. vi.
[22] Ibid, p. 29.

4. Assurance

One of the criticisms of The Three Lines of Accountability is that there can be duplication of work by the three lines. The area that attracts the most attention in this regard is assurance, which is conducted by all three lines. While Armstrong Wolfe (2020) believe this could be due to a lack of trust between the lines,[23] we consider that part of the issue can be addressed through a clear set of definitions, coordinated planning and a focus on analysis and response.

The terms 'assurance', 'testing', 'monitoring', 'review' and even 'audit' are often used interchangeably. The GRCI recommends that the word 'assurance' describes the overall process across all three lines. The purpose of assurance is to ensure that the governing body and senior management are fully apprised of the effectiveness of the compliance controls.

The remaining terms are used to describe actions at each line in Table 1, below.

Table 1
Assurance Definitions across the three lines

Term	Definition	Potential Frequency[24]	Line Owner
Non independent Management Monitoring	• Repeatable checking by the business of routine issues that may cause loss, reputational damage or a breach. • Often automated e.g. monitoring of training completion by management or monitoring trends as part of a dashboard review.	High (daily, weekly, monthly)	Line One
Independent Compliance Testing, Review and Monitoring	• **Testing:** The testing of compliance controls in accordance with a defined sample methodology. The specific controls in scope are documented and operationalized by Line 1. The testing includes design effectiveness testing and operational effectiveness testing. • **Review:** Structured or thematic reviews at a specific point in time of a Compliance process risk or control by Compliance based on risk assessment. This method provides a better understanding of how well the controls are designed to mitigate the compliance risk based on the annual plan. • **Monitoring:** Consistent with the monitoring definition at Line One but is conducted independently from the business. This form of assurance does not focus on assessing design or operating effectiveness and therefore is not considered either a review or testing.	• High • Medium (Quarterly, Bi-annually or annually)	Line Two
Audit	• Performs auditing process in accordance with an annual plan and provides an independent assessment of the risk management and internal control systems.	Low: contingent on risk assessment. Range from 1-3 years.	Line Three

[23] Armstrong Wolfe, above n. 7, p. 8.
[24] 'Potential frequency' stated in Table 1 is a guide only and should be adjusted to suit the type and size of the business.

The focus by each line in assurance is different:

- Line one monitors business activity to detect any actual or potential weaknesses, breaches or issues as part of their regular business activities.
- Line two undertakes independent actions to evaluate if the controls operate to ensure compliance with the obligation.
- Line three tests operational effectiveness for the purpose of assessing the internal control of the organisation.

Once the scope and frequency of the work undertaken has been clarified across all lines, it is important that the three lines coordinate when and how the work will be undertaken. Apart from reducing the perceived duplication of work, it also provides a useful opportunity to leverage the work undertaken and focus only on outstanding risks. This is especially the case between lines two and three, where the Internal Audit function can leverage the assurance work completed by the Compliance function and both can form an overall coordinated plan.

The GRCI recommends the following actions be taken to deliver the testing critical success factor:

1. **Clearly define the monitoring programmes across lines one and two.** To avoid duplication of work, lines one and two should clearly define the scope in the separate monitoring processes. Where possible, line two should leverage the monitoring work to assist with line two reviews. Lines one and two should continually discuss and train staff on the differences of the assurance across all three lines and how it supports the business with risk mitigation.

2. **Coordinated planning, analysis, and response across all three lines.** The GRCI recommends that all three lines discuss the timing and focus of assurance, at least on an annual basis. This will minimize overlap of timing and potentially repeated questions being asked of the same area by different lines. The outputs of the assurance – analysis and response – should also be actively shared across all three lines to ensure that the results are understood and all views on the management response are heard. Structured meetings to discuss the analysis and response is encouraged.

5. Resources

For The Three Lines of Accountability to work effectively, all three lines must be properly resourced to undertake the required tasks. As mentioned above, one of the key changes in moving to The Three Lines of Accountability is that line one must manage and own business risks. This requires continual reinforcement by the Compliance function on the need to support integration of line one control tasks into line one roles, together with reinforcing the role of compliance.

The GRCI recommends the following actions be taken to help deliver the resources critical success factor:

1. **Skills training.** The Compliance function should support line one control owners by providing training on how to manage issues arising when addressing controls matters. Preferably a 'train the trainer' approach should be used, where a line one manager is able to address both the knowledge and cultural issues concerning controls management. Training is usually more effective when presented by a line manager, because participants see the training as being part of the line one objectives, not that of the Compliance function.

2. **Compliance knowledge and alignment of business outcomes.** For a Compliance professional to be effective they must know and understand the business drivers and outcomes. Not only does this improve knowledge on potential risks and opportunities for the business, but it also enables the Compliance function to understand the potential impact of any regulatory or control change. Being seen as a curious, informed business partner greatly

assists in stronger collaboration with the business, without compromising the line two independence.

3. **Compliance resource planning.** As with all functions, Compliance needs to carefully plan and budget on how to best deploy resources. To ensure that the Compliance function has the right skillset mix and number of resources, the Compliance Head should develop an annual compliance plan to discuss with their management. Annual plans should draw on the statements in their compliance value proposition as to the critical issues they will deliver to support the business and The Three Lines of Accountability. An annual plan documents the deliverables to which the Compliance function will hold itself accountable, underpinning effective delivery of The Three Lines of Accountability's aims.

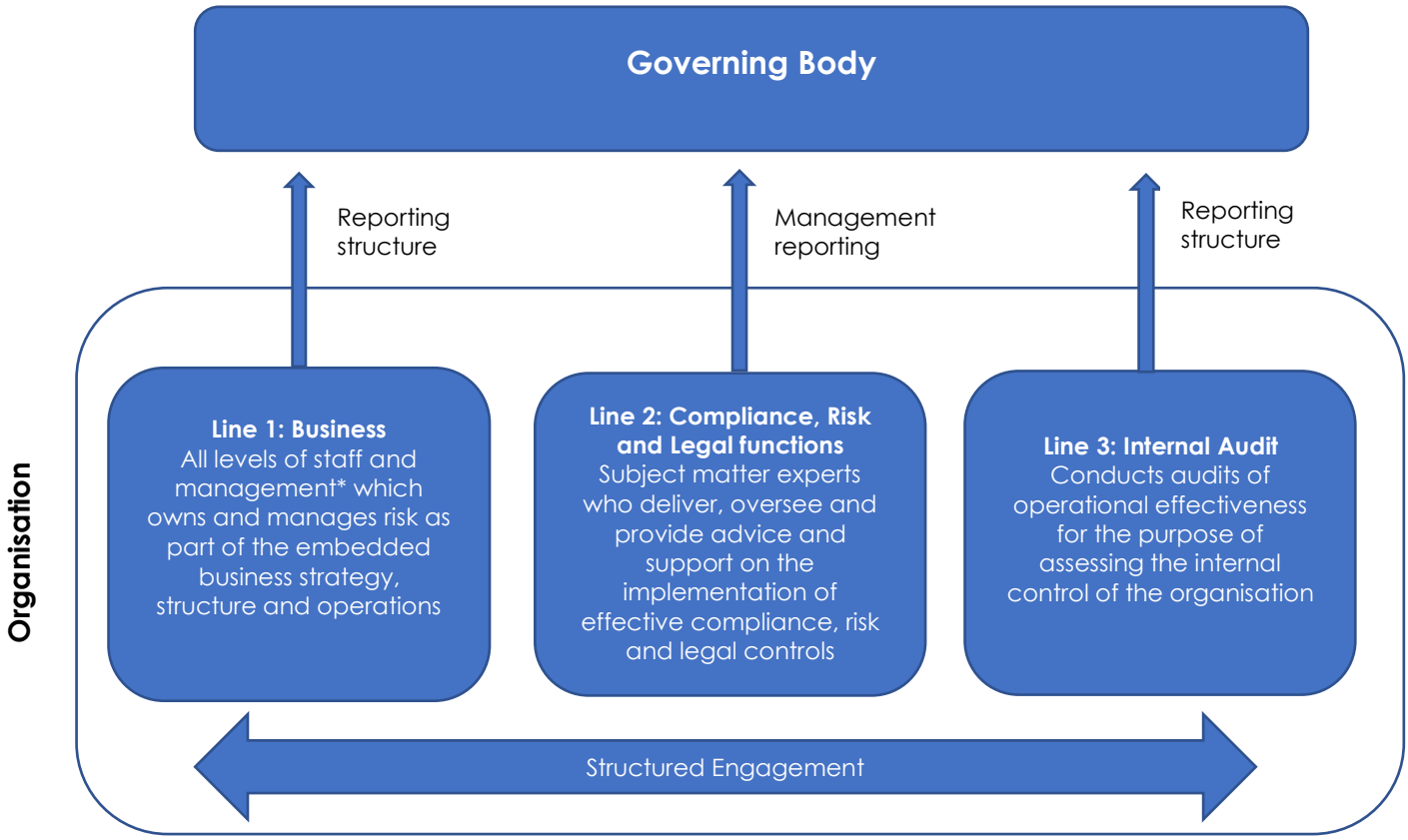
Engagement and Communication

Underpinning the critical success factors of the Three Lines of Accountability model is engagement and communication.

The importance of regular and effective engagement and communication between each of the lines cannot be underestimated.

Regular discussions between the lines should outline each line's annual plan and areas of focus. Progress to the plans and additional areas of focus that arise as a result of legislative and/or regulatory review, external industry focus and/or items identified internally play an important part of ensuring the plan remains dynamic and current in its deliverables.

Appendix 1
Three Lines of Accountability Model



*including Chief Executive Officer and senior management

Appendix 2
Three Lines of Accountability Critical Success Factors Summary

Critical Success Factor	Actions
Role Clarity	• First line job descriptions clearly define which controls they must manage. • Internal controls/procedures clearly documenting who is responsible in the first and second line to conduct or manage the task. • Escalation triggers (i.e., from the first to the second line) clearly documented. • Standing working group/committee to discuss risks and matters management by lines one and two. • Performance metrics developed to identify areas of improvement in ownership, delivery, and engagement.
Accountability	• Ongoing awareness and training programme on the importance of culture and ownership. • Balanced scorecards on performance reviews that rewards contribution to a culture of compliance. • Appropriate consequence management.
Independence	• Develop, demonstrate, and deliver the line two Compliance Value Proposition.
Assurance	• Clearly define the monitoring programmes across lines one and two. • Coordinated planning, analysis, and response.
Resources	• Skills training to line one on controls issues. • Compliance function understanding of the business and alignment with business outcomes. • Annual compliance plan to evaluate quality and quantity of line two resources.

Appendix 3
Glossary of terms

Accountability
Being held responsible for one's actions

Assurance
The overall controls monitoring, testing, review and audit process across all three lines to provide evidence to the governing body and senior management on the effectiveness of compliance controls

Audit*
Systemic and independent process for obtaining evidence and evaluating it objectively to determine the extent to which the audit criteria is fulfilled

Compliance Value Proposition
Documented statements and examples on why and how the Compliance function supports an organisation achieving its objectives

Critical success factors
Activities that need to be undertaken in order to achieve a strategic goal

Governing body*
Person or group of persons that has the ultimate responsibility and authority for an organisation's activities, governance and policies and which senior (top) management reports and by which senior (top) management are held accountable

Operational independence
Organisational structures which empower and support Compliance professionals to challenge first line decisions that do not meet the organisational obligations, values and/or ethics

Resources
Capital within an organisation which is required to design, deliver, assess and verify the Three Lines of Accountability

Role Clarity
Documented job descriptions/role purpose statements which clearly describes the roles and responsibilities of staff and/or vendors in delivering the Three Lines of Accountability

Senior Management
Senior executives within the organisation who are responsible for achieving business objectives.

Note: Senior Management is referred to as 'Top Management' in ISO 37301:2021

Three Lines of Accountability
Business risk model which reinforces accountability at all levels of an organisation for governance, compliance and risk management

Three Lines of Accountability critical success factors
Five critical success factors that will assist a Compliance professional to achieve the goal of implementing the Three Lines of Accountability into their organisation.

*These definitions are consistent with ISO 37301:2021

The GRC Institute

Since 1996 the GRC Institute (GRCI) has been the preeminent member association for Asia Pacific Compliance and Risk management professionals. Based in Sydney, Australia, the GRCI represents and provides professional support and recognition to over 2,000 practitioners across Asia Pacific and more than 100 organisations from a diverse range of industry sectors.

As a Registered Training Organisation, we provide leading-edge training and educational qualifications on core skills for our profession, including Compliance and Risk Management and Anti-Money Laundering. Our members are supported by our continuous professional development programmes, accreditation, networking events, access to supporting tools and online resources, together with advocacy to Government and Regulators on critical issues to the profession and the community.

Disclaimer

The GRCI publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The GRCI recommends seeking independent expert advice relating directly to any specific situation. The GRCI accepts no responsibility for anyone placing sole reliance on this material.

Contact us

Naomi Burley, CEO
naomi.burley@thegrcinstitute.org

Find us on LinkedIn: GRC Institute or go to our website http://www.thegrcinstitute.org

Version: 1.0
Publication Date: October 2021
Version Review Date: October 2023

Copyright © 2021 The GRC Institute. All rights reserved.