



THREE LINES OF DEFENCE REVIEW

Issued 19 September 2019

ICAEW welcomes the opportunity to respond to the Three Lines of Defence Review published on 20 June 2019 by the Global Institute of Internal Auditors, a copy of which is available from this [link](#).

ICAEW is a world-leading professional body established under a Royal Charter to serve the public interest. In pursuit of its vision of a world of strong economies, ICAEW works with governments, regulators and businesses and it leads, connects, supports and regulates more than 152,000 chartered accountant members in over 160 countries.

ICAEW members work in all types of private and public organisations, including public practice firms, and are trained to provide clarity and rigour and to apply the highest professional, technical and ethical standards.

© ICAEW 2019

All rights reserved.

This document may be reproduced without specific permission, in whole or part, free of charge and in any format or medium, subject to the conditions that:

- it is appropriately attributed, replicated accurately and is not used in a misleading context;
- the source of the extract or document is acknowledged and the title and ICAEW reference number are quoted.

Where third-party copyright material has been identified application for permission must be made to the copyright holder.

For more information, please contact: representations@icaew.com

KEY POINTS

1. The exposure document on the *Three Lines of Defence* is an important and valuable initiative in helping to strengthen and improve corporate governance. Having considered the paper and the questions it poses, we are of the view that the model remains fit for purpose, subject to the following key revisions.
2. The paper should make it clear that the application of the model should be principles-based, and as such it needs to provide guidance that recognises that 'one size does not fit all'. This will help organisations of differing scale and complexity apply the model to their specific needs. This does not mean that it should compromise on the fundamental principles of the three lines of defence, rather it should aim to deliver a proportionate and cost effective approach to risk management. For example, the paper should provide detail on how the *Three Lines of Defence* model can be adapted to suit the needs of smaller, less mature organisations, and how it might need to change to include a maturity model as organisations become more complex.
3. It is critical that there is clarity about who performs the three lines of defence activities. In some organisations this clarity may be achieved by teams performing their respective line activities. However, in others it may be desirable for some 1st line activities to be performed by functions with a primary role in the 2nd line, and for some 2nd line activities to be performed by the independent 3rd line. However, within this model it should always be the case that the 3rd line must remain independent and objective, and there should be clear, documented organisational designs and safeguards to ensure the main roles of the functions are not compromised.
4. The model should also be activity based rather than focusing on functional roles. This will determine where each activity sits in the three lines of defence, rather than using a generic, high-level functional description, for example as is currently used for the 2nd line in the model.
5. The fundamental reporting line of internal audit should be to a non-executive director to ensure it can maintain the right level of independence and objectivity. Currently, internal audit reporting lines do not always promote sufficient independence and objectivity, particularly where audit committee oversight is weak and/or management has too much say in the scope and approach of the internal audit work and plans, the budget allocated to it, and the performance review and remuneration process. The objectivity of internal audit would be enhanced by avoiding any reporting line that does not have accountability to non-executive directors. If a second line of reporting is required, this should be to the CEO only.
6. We recommend that organisations review the design, operation and effectiveness of their three lines of defence model every three to five years, under the oversight of the audit committee. This review should be performed by a suitably skilled party – which could be internal audit, or a first/second line team, or by an external party.

RESPONSE TO SPECIFIC QUESTIONS

Section A1: The case for refreshing and updating the Three Lines of Defence

What is your opinion of the familiar graphic that has been used to illustrate the Three Lines of Defence since 2013?

Strongly disapprove

Mostly disapprove

Neither approve nor disapprove

Mostly approve

Strongly approve

What recommendations do you have for improving the Three Lines of Defence graphic?

7. The *Three Lines of Defence* model graphic is static and defines a target operating model, which may suit larger established organisations better than smaller organisations. However, governance is rarely delivered in the way set out in the model, but rather it evolves as an organisation grows or changes. Given this, the model could be enhanced to provide broader appeal to small or growing organisations by considering how it can be made flexible to deliver a proportionate and cost effective approach to risk governance.
8. The content in the boxes mixes the three line activities with rather vague descriptions of roles and functions, and it omits certain policy-setting functions such as legal and human resources from the 2nd line. The content would also benefit from using text that reflects the different roles and responsibilities from a risk perspective – risk ownership and management for the 1st line; risk review and oversight for the 2nd, and risk assurance for the 3rd line.
9. The current graphic constrains a more flexible application of the model as it suggests specific functions are neatly aligned to each line in the model. In addition, the examples given for the 2nd line may mean different things to different organisations. For example, in some organisations there can be a degree of independent quality assurance activity in the 1st line which, while valuable, cannot be viewed as a 2nd line activity. Importantly, we also view the role of financial control as primarily 1st line in nature, and not 2nd line as indicated in the model.
10. The exposure document should adopt a principles-based approach in defining the roles and responsibilities so that organisations have the flexibility they require when implementing or enhancing the model.
11. This approach would also help to address two key challenges - where the 2nd and 3rd lines are under-resourced, and where excessive monitoring and assurance by organisations can lead to an environment where the 1st line abdicates some of its ownership for managing its risks to the 2nd line.

Section A2: Assessment of the Three Lines of Defence model***What is your opinion of the assessment made of the Three Lines of Defence model described in this section?***

Strongly disapprove

Mostly disapprove

Neither approve nor disapprove

Mostly approve

Strongly approve

What further comments do you wish to add to the assessment of the Three Lines of Defence Model?

12. Despite the simplicity of the *Three Lines of Defence* model and the need for clear governance and organisation, there is sometimes considerable contention and confusion around the responsibilities for the key activities in each of the lines. Where this happens, responsibilities may become blurred and the careful balance between management, monitoring and assurance functions will become misaligned, which can lead to a breakdown in effective controls. It is only when these three lines are properly structured with no gaps in coverage that the organisation and its risks are more likely to be effectively managed.
13. The paper needs to provide guidance that recognises that 'one size does not fit all' to help organisations of differing scale and complexity apply the model to their specific needs. This does not mean that it should compromise on the fundamental principles of the three lines of defence.
14. Where there is no overlap, the 1st, 2nd and 3rd lines can become too detached from each other because they see their roles and boundaries as fixed. This can lead to an organisation being reluctant to modify the model to achieve a better overall result in risk assurance. Risk

assurance mapping can help to tackle where gaps occur, but it does not seem to be widely used.

15. The exposure document should be clear that the *Three Lines of Defence* model is the way in which the requirements for a sound system of risk management and internal controls are achieved. As such, it should be reassessed by the board/audit committee once every three to five years by a suitably skilled party - either by internal audit or by a first/second line team, or by an external party.
16. It is important that there is clarity about who performs the three lines of defence activities within an organisation. In some organisations this clarity may be achieved by the organisation's structure, with the 1st and 2nd lines respectively performing all their activities and 3rd line teams delivering objective assurance. However, in other organisations it may be a desirable for some 1st line activities to be performed by the 2nd line, or for some 2nd line activities to be performed by the 3rd line. Where there is overlap it is critical though for the 3rd line to retain its independence and objectivity. While this can be effective in managing risk, it does require clear, documented organisational designs and safeguards to ensure the main activities within each line are not compromised.

Section B1: Why organisations exist

The exposure document proposes to strengthen the Three Lines of Defence model by repositioning it in the context of governance, organisational success and value creation. To what extent do you approve of this approach?

Strongly disapprove

Mostly disapprove

Neither approve nor disapprove

Mostly approve

Strongly approve

What challenges do you see in applying the model to this broader governance context?

17. The *Three Lines of Defence* model as currently perceived lends itself to risk mitigation rather than being perceived to contribute to organisational success and value creation. The prevention of significant incidents or crises does underpin organisational success and value creation, but there is a lost opportunity to demonstrate greater value.
18. We welcome the intent to strengthen the model by repositioning it in the context of governance, organisational success and value creation. However, our view is that the model, if correctly positioned, should already be contributing to these three objectives.
19. The exposure document does not spell out how these objectives will be achieved. The *Three Lines of Defence* model needs to be clearer on how good governance and risk management links to and drives value creation by focusing on both risk mitigation and on opportunities, and creating clearer linkage to strategic objectives.
20. The effectiveness of implementing the model will depend significantly on the effectiveness of an organisation's audit and risk committees. These committees should have sufficient expertise in governance, risk management and internal control to discharge their roles and responsibilities, and should challenge the principles rigorously with the senior leaders in their 1st line of defence roles.
21. Internal audit reporting lines do not always promote sufficient independence, particularly where audit committee oversight is weak and/or management has too much say in the scope and approach of the internal audit work and plans, the budget allocated to it and the performance review and remuneration process. The objectivity of internal audit would be enhanced by avoiding any reporting line that does not have accountability to non-executive directors. If a second line of reporting is required, this should be to the CEO only. This will ensure that heads of internal audit are not competing for bonus or incentive payments with

those they are auditing, which occurs at present. We would like to see this made clear in the *Three Lines of Defence* model as part of its links to governance.

Section B2: How governance fosters organisational success and value creation

The exposure document identifies four main complementary and overlapping groups of roles and activities that typically support governance, organisational success, and value creation namely: leadership and oversight; strategy execution; support, guidance and control; and objective assurance and advice.

These four groups form the basis of the main functions that comprise the Three Lines of Defence model. To what extent do you agree that this analysis is helpful in advancing the understanding of the model and improving its application?

Strongly disagree

Mostly disagree

Neither agree nor disagree

Mostly agree

Strongly agree

What further comments do you wish to make on this approach?

22. This should be more upfront and the focus of the exposure document as it goes to the heart of how the *Three Lines of Defence* contributes to effective governance, organisational success and value creation.
23. Culture is integral to effective governance, organisational success and value creation. Boards under the UK Corporate Governance Code have a duty to address and monitor the culture of their organisations. The Committee of Sponsoring Organisations (COSO) recent update to its **enterprise risk management framework** (ERM) recognises the role that culture plays in ERM. The update suggests that boards should embed culture into discussions about strategy and risk. Implementing the *Three Lines of Defence* is not enough if it is not supported by a culture that enables effective risk management. The paper should highlight the important role that culture plays in delivering an effective three lines of defence.
24. Organisations are also more likely to adopt the model effectively if they can see the contribution to value creation that each line brings. For example, the paper should articulate how the management of risk by the 1st line leads to commercial success; how the 2nd line is focused on overseeing the board's appetite for risk and helping the board feel informed and reassured about the new risks being taken; and how the 3rd line provides assurance to the board that risk management is operating as intended.
25. There are significant differences in the depth and breadth of 2nd line activities both within, and between, industries. In some cases the 2nd line can be quite thin on the ground or may not exist at all. In this case the 3rd line can play a more direct monitoring role. The result is there is no one-size-fits-all activity to make the *Three Lines of Defence* fit every organisation. One option would be to adopt a principles-based approach in defining the roles and responsibilities, as organisations will have flexibility when implementing or enhancing the model.

Section C1: Building on the model

This section describes the typical roles and responsibilities of each of the main functions that comprise the model as well as key external bodies that contribute to governance, organisational success, and value creation. What is your assessment of this section of the exposure document?

Strongly disapprove

Mostly disapprove

Neither approve nor disapprove

Mostly approve

Strongly approve

What further comments do you wish to add on this section?

26. The 1st line needs to be more involved in establishing a robust *Three Lines of Defence* model, in particular by playing a stronger role in its implementation and successful operation. A key weakness of the model is that its principles are not well understood or embedded within the 1st line or sometimes certain functions that perform 2nd line activities.
27. There is insufficient emphasis on the role, responsibility, accountability and culture for managing risk in these two lines. This is a critical success factor otherwise 1st line management can be seen as deferring its responsibility to other lines. What is important is driving ownership and accountability within the 1st line. The root cause of all major corporate failures and scandals arise within the 1st line, inadvertently aided by insufficient review and challenge from the 2nd and 3rd lines.
28. The exposure document should emphasise how the roles and responsibilities of each of the three lines contribute to governance, organisational success and value creation. Without this understanding it is difficult to judge whether and how the roles and responsibilities may need to be revised to meet these objectives. The risk is that the paper will be seen as an exercise in promoting governance for governance's sake. The paper must articulate how governance safeguards existing value but also helps to drive value creation.
29. The key roles of the governing body in the exposure document could be made more active to reflect the responsibility of boards to monitor the performance of organisations and hold senior management to account.

Section C2: A coordinated approach

The exposure describes the importance of coordination, integration and alignment across roles as well as the opportunity for internal audit to play a leading role in facilitating this. Do you agree that this is an appropriate role for internal audit?

Strongly disagree

Mostly disagree

Neither agree nor disagree

Mostly agree

Strongly agree

What further comments do you wish to add on this section?

30. The exposure document makes a really important point about how internal audit can play an important role in leading efforts toward a more integrated approach to the strategic priorities and operational needs of an organisation. Organisations also need to receive objective assurance on the adequacy and effectiveness of their governance if they are to avoid bloated governance which can be as damaging as too little governance.
31. The paper references how greater integration can be fostered by leveraging data and technology, but it fails to explore in any detail what the impact of technology might be on the model. Organisations are expanding their use of technology. The rapid evolution we are seeing is leading organisations to automate more of their 1st and 2nd lines, and using the results, including any discrepancies, into the work respectively of the 2nd and 3rd lines. The amount of data that is being collected is reshaping the risk-management environment, for example in monitoring critical risks. The assurance that is required over these new technologies is also not recognised in the paper.
32. As noted earlier, it may be appropriate for new or emerging companies to choose not to establish a three lines of defence model in their early growth phase, particularly where the organisation can leverage its technology capabilities to support more automated/ agile risk management. Critics that suggest this is inappropriate ignore the innovations that are taking

place. The exposure document should focus on the value that third line assurance can provide to boards/ audit committees, particularly as organisations grow.

33. As technology is disrupting business models, we are seeing organisations recruit people with the necessary skill sets to use these developments to manage risks in the 1st line. Second and 3rd lines must similarly incorporate the right capabilities to remain abreast of changes and ensure they are able to provide respectively effective oversight and objective assurance. Talent management strategies will need to be in place to recruit the right people with the right skills to deliver an effective three lines of defence. The paper would benefit by highlighting the need for organisations to understand their skills requirements, training and succession planning.

Section D1: Scalability

The exposure document describes ways in which the model can be adapted to suit the needs of an organisation, including a maturity model. To what extent do you approve of this more flexible approach?

Strongly disapprove

Mostly disapprove

Neither approve nor disapprove

Mostly approve

Strongly approve

What further comments do you wish to add on this section?

34. This section does not provide detail on how the *Three Lines of Defence* model can be adapted to suit the needs of smaller, less mature and less highly regulated organisations, and how it might need to change to include a maturity model as organisations become more complex and subject to greater regulation.
35. In certain sectors there are mandatory regulatory requirements that drive the separation of functions between the lines of defence, particularly financial services organisations, as opposed to focusing on the separation of activities within the model chosen by the organisation.
36. In smaller and less complex organisations, there is a risk that the 2nd and 3rd lines operate on a 'best efforts' basis rather than meeting the organisation's full risk management and assurance needs. The 2nd and 3rd lines can also end up compensating for a lack of knowledge/capability in the 1st line to 'get the job done'. Guidance is required on how the model should be applied in a way that recognises proportionality, and how to mitigate the inherent risks to operating effectiveness when these circumstances occur.

Section D2: 'Blurring of the lines'

The exposure document provides a way of explaining and allowing for "blurring of the lines", recognising that the internal audit function can provide value in non-assurance roles, as long as there is a clear assessment of the potential impact on the effectiveness of governance and safeguards are considered.

Ultimate responsibility rests with the governing body to determine the structure and roles most appropriate for the organisation. To what extent do you approve of this approach?

Strongly disapprove

Mostly disapprove

Neither approve nor disapprove

Mostly approve

Strongly approve

What further comments do you wish to add on this section?

37. It is critical that ultimate responsibility rests with the board, with delegation for oversight of the organisation's system of risk management and internal control (through the three lines of defence) to the risk and audit committees. Reinforcing this requirement in the paper would be beneficial. In particular, the board must set out clearly the scope and purpose of their internal audit function. This should be documented to avoid the erosion of their independence and objectivity, or the scope of their activities without board and relevant committee approval.
38. The board/ audit committee should understand where the lines are drawn in relation to the activities required for each line of defence and how these map to the design of the organisation's functions. It is important that safeguards are put in place to ensure the objectivity of the 2nd and 3rd lines is maintained. In this regard, the Institute of Internal Auditors (IIA) **position paper** on the role of internal audit in enterprise risk management sets out safeguards to achieve this.
39. Where separate internal audit and risk management teams are managed by a joint head of audit and risk, there should be a mechanism in place to ensure that the audit committee and senior management can differentiate between the opinions of internal audit and the descriptions of risk provided and collated through the risk management function, and maintain the objectivity of internal audit. It must be clear that risks are managed by the 1st line and that the risk management function is maintaining the overall system of risk management and internal control and collating the views of the 1st and 2nd lines.

OVERALL**Please add any further comments you may have about the exposure document and the overall direction it proposes for refreshing the Three Lines of Defence in effective risk management and control**

40. The exposure document on the *Three Lines of Defence* is an important and valuable initiative in helping to strengthen and improve corporate governance. Having considered the paper and the questions it poses, we are of the view that the model remains fit for purpose. But the model would benefit from being centred more clearly on key risks to reflect a proportionate approach by organisations to avoid over-governance. It also needs to address the misperception that either the 2nd line or internal audit as the 3rd line are responsible for all control or regulatory matters, when the 1st line also has a key role to play.
41. The paper should make it clear that the application of the model should be principles-based, and as such it needs to provide guidance that recognises that 'one size does not fit all'. This will help organisations of differing scale and complexity apply the model to their specific needs. This does not mean that it should compromise on the fundamental principles of the three lines of defence, rather it should aim to deliver a proportionate and cost effective approach to risk management. For example, the paper should provide detail on how the *Three Lines of Defence* model can be adapted to suit the needs of smaller, less mature and less regulated organisations, and how it might need to change to include a maturity model as organisations become more complex and subject to greater regulation.
42. It is critical that there is clarity about who performs the three lines of defence activities. In some organisations this clarity may be achieved by teams performing their respective line activities. However, in others it may be desirable for some 1st line activities to be performed by functions with a primary role in the 2nd line, and for some 2nd line activities to be performed by the independent 3rd line. For example, it may be more efficient for the 3rd line to step in and take on a monitoring role because of the rigour and robustness it will bring to the activity. However, within this model it should always be the case that the 3rd line must remain independent, and there should be clear, documented organisational designs and safeguards to ensure the main roles of the functions are not compromised.