Chapter 12

The Three Lines Model

¶12-010 Introduction

As noted in earlier chapters, new developments in the task of monitoring had been pioneered and it is known as the 'Three Lines Model'. This shall be the focus of this chapter, starting with the history followed by an in-depth discussions. This model is expected to offer a more holistic or at least a more robust approach to monitoring, as well as organizing compliance.

¶12-020 Principles

- In order to be entrenched in an organization, ccompliance needs to be organised along with solid structure and processes. Both dimensions are relevant to making a chosen setup effective and efficient as the tasks are increasingly challenging.
- One time-honored and proven concept from ancient military as well as sports is represented by the so-called three lines of defense. It was taken up by the management to look at risk management first, but has increasingly been developed towards the use for governance issues.
- Compliance falls into that remit, whilst it has to play its role together with all other governance roles. Therefore, using the concept is a simple yet effective method to set up and maintain a compliance function. This is even more true as the three lines have gained acceptance with regulators as well as within the law.
- As a basic principle, the concept posits three lines of defense as a structural organizational norm: besides the governing body and outside assurance providers, three separate, increasingly independent but related functional roles have to be established:
- As the first line, the management ensures the daily operations including operational controls – owning and managing the risks, including compliance risk that affect legal, regulatory and ethical aspects. It is supported by the special knowledge of the second line – notably including the compliance function, but also risk management and some financial control functions etc. – which helps set up and monitor, quasi as oversight functions with some limited independence. As the most independent function, the third line provides additional assurance and advisory in the form of an internal audit role.
- All the three lines are to be set up in order to have a fully functional governance system. With any element missing, none of the stakeholders can provide its deliverables fully. Regulators regularly

look at the completeness of all three lines, even when they allow for specific organizational solutions.

- Besides the purely structural elements, there have to be processes to coordinate and communicate. This is in line with the often misunderstood approach to view the three lines not as consecutive activities, but rather as complementary and permanently necessary tasks that can mutually strengthen each other.
- The most cited model in this realm is the Three Lines of Defense, which was published in 2013 and has developed into something like the gold-standard for this field. It is referred to not only by regulators, but also by legislators increasingly. It includes very noteworthy recommended practices which can help strengthen the overall model and make it more robust.
- As a further development, the so-called Three Lines Model (actually a renewed version by the same author) provides new perspectives such as the introduction of some key principles. It also provides clarifications on the previous version and takes care of issues like reporting and coordination. Possibly due to its marginal changes, its adoption so far has been relatively muted – also reflecting the success of the previous version – but still, it can offer positive ideas for practitioners.
- We therefore recommend a hybrid use of the two models, with strong adherence to the three lines setup of the initial model plus its practices, complemented by some guiding principles and approaches for coordination as provided by the latest version. The role of the governing body is key here, and whilst not common in practice yet, the latest trends suggest additional reporting lines of compliance to the governing body and not just to the first line it supports.
- Finally, when it comes to coordination tasks, it will be key to look for the latest best practices in one's own and other industries, as regulations are only the minimum standards one needs to be compliant with – a fact not lost on the stakeholders.

¶12-030 Issues

To anchor compliance in any organization, its respective elements must be implemented in an effective and efficient manner. This implementations does not only entail the existence of all the necessary elements, but also affects the overall design of the system, including the links to management or to neighboring functions such as risk management. It is thus concerned with the important question of how to set up structures as well as processes to achieve good compliance outcomes – i.e. how to actually organize for compliance.

This design task is in itself challenging enough: (a) compliance requirements are not static, they change with time and in response to the expectations

of regulators and other relevant stakeholders. In practice, respective expectations tend to also be a reflection of evolving best practices, thus permanently stepping up the game. The organization must reflect this necessary flexibility; (b) at the same time, compliance must involve a number of external and external stakeholders across and beyond the organization, resulting in complex communication and coordination tasks. The design must facilitate or even necessitate such coordination, without permanent intervention; (c) finally, from an overall perspective, the governing bodies of the respective organization need to ensure that the chosen setup is 'fit for purpose', adequate resources are available and the system is functioning. This is part of their duties, making sure that compliance is embedded in an overall system of governance.

As would be expected, there have been ongoing debates on how to best structure the related functions.[1] Nonetheless, as noted by Eulerich, the "*design of an efficient and effective internal corporate governance and monitoring structure remains a central challenge for modern corporate management. Theory and practice have not yet been able to present a generalizable framework*".[2] Instead, research and practice are resorted to pragmatic models that can support them in the task of organizing for compliance. A time-tested approach here is the concept of 'three lines', often also described as 'lines of defense'. This model has its roots in old military terms[3] as well as in some team sports.[4] The basic idea is one of multiple lines of defence, supporting and complementing each other in case of impending risk.

Despite its long history, management practice has only recently rediscovered the multiple-line approach, mostly for risk management purposes.[5] First applications for business were traced back to the 1990s, which were concept-based in practice,[6] and were subsequently picked up by academic literature,

1 See for example, Jose Tabuena (2015) 'Effective governance and the three lines of defense'. *Compliance Week*, 12(132), 34.

2 Marc Eulerich (2021) 'The new three lines model for structuring corporate governance – A critical discussion of similarities and differences'. *Corporate Ownership and Control,* vol. 18, no. 2, 180-187, at p. 180.

3 Andrew Chambers (2013) 'Maginot Line, Potemkin Village, Goodhart's law? The third line of defense: second thoughts (part 1)', *internal auditing (Boston, Mass.)*, vol. 28, no. 6, p. 15.

4 Dentons (2020) 'Re-assessing the Three Lines of Defense (3LoD) model during a time of continued crisis and remote working', May 6, 2020 (online), https://www.dentons.com/en/insights/articles/2020/may/6/re-assessing-the-three-lines-of-defense-3lod-model-during-crisis-and-remote-working

5 Tim Leech & Lauren C Hanlon (2016) 'Three Lines of Defense versus Five Lines of Assurance : Elevating the Role of the Board and CEO in Risk Governance', in The Handbook of Board Governance, John Wiley & Sons, Inc, Hoboken, NJ, USA, pp. 335–355.

6 Andrew Chambers (2013) 'Maginot Line, Potemkin Village, Goodhart's law? The third line of defense: second thoughts (part 1)', *internal auditing (Boston, Mass.)*, vol. 28, no. 6, p. 15.

which at the start, mostly with a focus on banking as it got on track after the global financial crisis. Especially the consultations regarding Basel II created the platform for the development of this concept, which is now fully established in governance literature and practice.

Early business adopters of the three lines of defense can be identified in risk management applications of the 1990s, giving the concept a foundation in management practice. Academic literature subsequently picked up on it with a clear focus on the field of banking, with discussions after the global financial crisis and the various consultations regarding Basel II providing a platform for the development and quick adoption of the model. This initial emphasis on risk management and the financial service industry,[7] can still be observed in how the concept is adopted and where it is most accepted today.

Its best-known version, the Three Lines of Defense (TLOD), as popularized by the Institute of Internal Auditors (IIA) in the early 2010s,[8] provides both structural and process-related guidance for management, support and governance functions including compliance, for the governing bodies and even regulators. Now being a well-known term for most executive and non-executive directors,[9] it has practically become a reference for how to organise governance compliance, which is also helpful for the dialogue with related parties in governance. Its history is interesting, as it shows the necessary interactions of functions in an organisation:

One of the first documents was issued by the two European organizations representing both the Internal Audit and the Risk Management professions, namely the European Confederation of Institutes of Internal Auditing (ECIIA) and the *Federation of European Risk Management Associations (FERMA)*, in 2010. These two organizations jointly issued a Guidance on Article 41-2b of the 8th European Company Law Directive,[10] given that this Directive had left a void in understanding how to fulfill the related directors duties. The two associations proposed the audit committee to 'monitor the effectiveness

7 Andrew Chambers (2013) 'Maginot Line, Potemkin Village, Goodhart's law? The third line of defense: second thoughts (part 1)', *internal auditing (Boston, Mass.)*, vol. 28, no. 6, p. 15 and B. Daugherty & U. Anderson, (2012). The third line of defense: internal audit's role in the governance process. *Internal Auditing (Boston, Mass.)*, 27(4), 38.

8 Institute of Internal Auditors (2013) 'The Three Lines of Defense in Effective Risk Management and Control', Institute of Internal Auditors, Altamonte Springs.

9 Dietmar Glage (2020) 'Das neue Three Lines Model des Institute of Internal Auditors (IIA)', *Der Aufsichtsrat*, vol. 2020, no. 10, p. 137, (online) https://research.owlit.de/document/d35412c4-72e2-3f8e-a405-f7812e079161

10 ECIIA and FERMA (2010) 'Guidance on the 8th EU Company Law Directive, Article 41: Monitoring the effectiveness of internal control, internal audit and risk management systems, Guidance for boards and audit committees, 8th European Company Law Directive on Statutory Audit DIRECTIVE 2006/43/EC – Art. 41-2b'. September 21, 2010. https://www.ferma.eu/publication/guidance-on-the-8th-eu-company-law-directive/

of the company's internal control, internal audit where applicable, and risk management systems',[11] – in effect suggesting a three-line approach, and also including a graphic representation of the three lines that has been referred to by most of the subsequent authors.

With this, these two European associations can be seen as the grandparents of the TLOD.[12] Remarkably, they had responded to a European Company Law Directive initiated to address the global financial crisis in a different way than the heavy-handed US approach of Sarbanes-Oxley.[13] In the subsequent years, however, their approach has found its ways into the practice and regulations of much wider geographies and organisations than originally intended, thanks mostly to the clarity of thought and ease of communication intrinsic in the model – and thanks to a short, seven pages position paper by the US-based global auditors' organisation IIA that is today referred to as the classic TLOD.[14]

This paper was not a joint exercise anymore, ending a rare example of cooperation between two governance-related professions, namely, audit/assurance and risk. It can rather be seen as a pragmatic acceptance of the strong response to the concept,[15] and the IIA later agreed that it did not originate the model by itself, but rather embrace it. Accordingly, the descriptive graphic in the IIA paper refers to its immediate source, stating "'Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*.[16]

Over time, the 'three lines' as a concept and the TLOD itself have been widely adopted and become a quasi-reference not only for the affected firms, but also for legislators and sector regulators, and for the legal plus

11 Ibid.

12 See detailed explanation by Flemming Ruud (2019) 'Reflections on the Three Lines of Defense, European Commission, Audit Services, November 27, 2019, Brussels (online). https://ec.europa.eu/info/sites/default/files/business_economy_euro/accounting_and_taxes/presentations/presentation_flemming_ruud_2019_en.pdf

13 Linda Sama & Victoria Shoaf (2005) 'Reconciling Rules and Principles: An Ethics-Based Approach to Corporate Governance', *Journal of Business Ethics*, vol. 58, no. 1/3, pp. 177–185.

14 Institute of Internal Auditors (2013) 'The Three Lines of Defense in Effective Risk Management and Control', Institute of Internal Auditors, Altamonte Springs.

15 Howard Davies & Maria Zhivitskaya (2018) 'Three Lines of Defence: A Robust Organizing Framework, or Just Lines in the Sand?', *Global Policy*, vol. 9, no. S1, pp. 34–42.

16 Institute of Internal Auditors (2013) 'The Three Lines of Defense in Effective Risk Management and Control', Institute of Internal Auditors, Altamonte Springs, p. 2.

compliance professions.[17] Specifically, the adoption by regulators gives the concept a strong backing and thus helped the model dissemination – as the Basel Committee on Banking Supervision recognized the three lines in its governance principles for banks (Bank for International Settlements, 2015), a wide visibility was ensured. Many other such regulatory events have followed, where reference is made to it.[18]

Also, initially more remote areas have started to make use of the concept, such as the field of cyber security.[19] As the TLOD undertakes to see risk management and control in a cross-functional and cross-departmental way, it can be of help to such areas as IT security – bringing it back to the root of the concept, the management of risk. A 2019 review of the TLOD, executed with a wide group of involved professionals and scholars, came to the following conclusion:

> "*Over that 20-year period, and with increasing pace in the last five, the Three Lines of Defense has become widely known and routinely applied, especially in financial services, where regulators commonly expect organizations to adopt it quite explicitly. Laws, regulations, codes, policies, and other frameworks (such as the COSO 2017 Enterprise Risk Management) that express reference to the model*."[20]

It is therefore worth diving into the basic elements of this model, its major recommendations and some of the (relatively limited) caveats identified over the years. The next subchapter sets out to accomplish this task, making reference mostly to the original model rather than secondary literature. Not only do the authors find the TLOD itself very solid, but also does this allow to build an extra layer of defence. It is also a reference intrinsically cited by regulators. As a compliance professional, this should be the approach, rather than short-sightedly following the latest approach propagated by consultants or trade journals.

17 Marc Eulerich (2021) 'The new three lines model for structuring corporate governance – A critical discussion of similarities and differences', *Corporate Ownership and Control*, vol. 18, no. 2, pp 180-187.

18 See for example Bradford Hu & Aslihan Denizkurdu (2020) 'Risk governance framework and the three lines of defense construct: A challenged self-assessment process through an activity-based approach', *Journal of Risk Management in Financial Institutions*, vol. 13, no. 3, pp. 212–223.

19 Christophe Veltsos (2017) 'Take a Load Off: Delegate Cyber Risk Management Using the Three Lines of Defense Model', *Security Intelligence*, November 20, 2017 (online), https://securityintelligence.com/take-a-load-off-delegate-cyber-risk-management-using-the-three-lines-of-defense-model/

20 Francis Nicholson (2019) 'Three lines of defense: Report on the public exposure findings June – September 2019', IIA October 2019, p. 3 (online), https://na.theiia.org/about-us/about-ia/Documents/Public-Exposure-Report-General-Release.pdf

[A] The Three Lines of Defense Model

The seminal January 2013 paper 'IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control' the IIA,[21] sets the theme already in its title. It looks at how the different teams of diverse risk and control professions – including specialists in internal audit, risk management, compliance, internal control, quality, etc. – are cooperating to help their organisations manage risk. This affects both structures, i.e. assigned roles, and processes, i.e. coordination among these groups – areas that are usually not covered by classic risk management frameworks or other literature. The intent is to avoid gaps in coverage as well as duplications in effort.

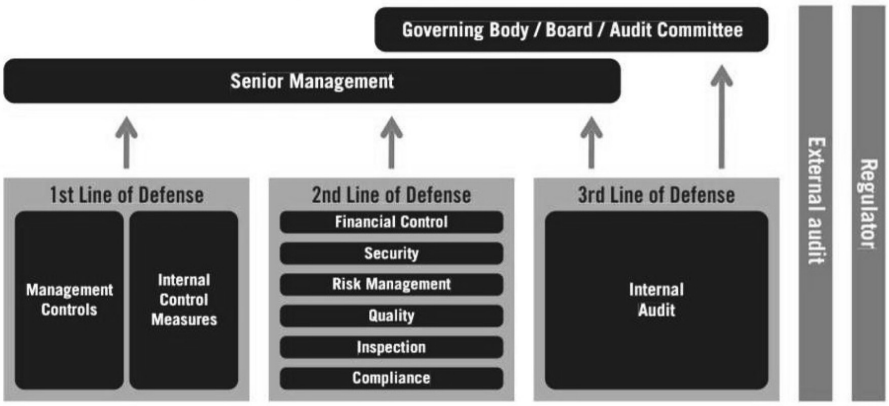
Such efforts to systematically organise for effective and efficient execution of all the relevant areas, including but not limited to compliance, have high relevance. The increase in related crises or even breakdowns of governance systems in very different organisations are testament to this necessity. Some simple and effective model, as targeted by IIA, is most helpful here: As noted by Eulerich, rather than lacking on some specific details, perfect implementation or highly sophisticated tools, most corporate scandals are related to a poor or quasi-non-existing governance setup as such.[22] As a consequence, those players with undefined roles and duties tend not to recognize warning signals from inside or outside the organization. In short, an adequate organization will help avoid such risks.

In its effort to describe a generic model for any type of organization, irrespective of its complexity or size, the TLOD refers to very broad, yet logical categories. First of all, it defines three roles to be filled in the overall governance framework: with management control being the first line of defense, the second line is defined as risk control compliance oversight support functions, complemented by an independent internal audit as the third line. Neither senior management nor the governing bodies are part of these lines, just as external audits and regulators are positioned outside. Furthermore, though much less cited than the three lines, but all the more important, it provides guidance on how to coordinate between the lines. These are given in the overall text explaining the model. Finally, it suggests some recommended practices worth considering.

21 Institute of Internal Auditors (2013) 'The Three Lines of Defense in Effective Risk Management and Control', Institute of Internal Auditors, Altamonte Springs.

22 Marc Eulerich (2021) 'The new three lines model for structuring corporate governance – A critical discussion of similarities and differences', *Corporate Ownership and Control,* vol. 18, no. 2, pp 180-187.

Figure 7: The Three Lines of Defense Model (TLOD Model)



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*

Source: Institute of Internal Auditors, 2013

As a basic principle, each of these lines needs to be given its own level of independence, ensuring a sufficient level of objectivity. This allows one to employ different perspectives on a certain risk, thus allowing for a systematic evaluation. It is therefore important not to misunderstand the three lines as subsequent stage in a process, but rather as parallel perspectives. They all have their specific roles and duties:

- Before (or outside) the three lines, the senior management and the governing bodies shall first of all set objectives for their organization, then define relevant strategies to achieve them, and finally establish governance structures and processes to manage risks in realizing the objectives.[23]

  It is interesting to see that IIA defines senior management not as the first line of defense, but rather in a role of oversight and strategy-setting, similar to the governing bodies. Not all practical reality will reflect such a task allocation to senior management, but it is worth reminding the specific roles of C-level executives also in the governance context.

- The operating management owns and manages risks, which represents the first line of defense. This includes the task of setting up adequate management controls, potentially embedded into systems, and the daily management of risk and control procedures, including

23 Institute of Internal Auditors (2013) 'The Three Lines of Defense in Effective Risk Management and Control', Institute of Internal Auditors, Altamonte Springs, p. 3.

mitigating measures. In terms of the risk management process, this group covers the operating management as a risk owner.[24]

- The second line then assists risk owners in their tasks – via a risk management function, a compliance function, and some financial control functions. These disciplines are actually established by the management to help set up and monitor front-line controls. As risk oversight functions, they have a somewhat limited independence and typically report to the management as risk owners.[25] The model provides a list of typical responsibilities allocated here, as visible in the above figure.

  As to the topic of compliance, TLOD gives a detailed description – much more so than for risk management and financial controllership. In its core, it requires

  > "*(The) compliance function to monitor various specific risks such as non-compliance with applicable laws and regulations. In this capacity, the separate function reports directly to senior management, and in some business sectors, directly to the governing body. Multiple compliance functions often exist in a single organization, with responsibility for specific types of compliance monitoring, such as health and safety, supply chain, or quality monitoring*".[26]

  One major element here is that it is management (and not compliance itself) that sets up these functions to ensure that the first line is organized correctly, i.e. not only well designed and in function, but also operating as intended. This is often described as the core topics of testing (a) design, (b) implementation and (c) effectiveness of compliance measures, a distinction to which we will come back in the next chapter. As the second line functions are having (only) some amount of independence from the first line, they remain in effect management functions themselves – but still they are separate. This is a key characteristic of compliance, often underestimated by outsiders. Professional duty and care are to balance these limitations.

- Assurance is allocated the highest level of independence. Located as the third line of defense, this field is normally defined as an internal audit function of some nature, depending on the size and complexity of the organization. The scope of this assurance includes the whole organization, all its risk management and internal control aspects, including the two previously mentioned lines, plus a specific set of internal audit objectives. The achievement of such wide responsibilities requires a certain level of professionalism and an effective reporting line (also) to the governing body.[27]

24 Ibid., 6.

25 Ibid.

26 Ibid., 4.

27 Ibid., 6.

It is interesting to note that internal audit would not only have the freedom to test the "neighboring" compliance function, but in fact even should do so to ensure the compliance activities are fit for purpose. In practice, there is detailed guidance for the audit functions to check on the overall compliance systems, either issued by the professional bodies for internal auditors,[28] or by the professional bodies for external auditors.[29] Practitioners are well advised to look at these standards when organizing their compliance function.

- External assurance providers, both external auditors and regulators, mostly reside outside the organization's boundaries. They are not part of the three lines, but may play an important role at times. For regulated industries, notably financial services and insurance as mentioned specifically in the TLOD, they 'can be considered as additional lines of defense providing assurance to the organization's (stakeholders)'.[30] The introduction of a fourth or even fifth line of defense, as promoted by some authors,[31] is therefore not at all new, nor is it really helpful, given that as outsiders, these "lines" would end up with less extensive information than the internal setup.

The basic principle of the TLOD is very clear: 'all three lines should exist in some form at any organization, regardless of size or complexity. Risk management is normally strongest when there are three separate and clearly identified lines of defense. However, in exceptional situations... especially in small organizations, certain lines of defence may be combined'.[32] This also means that the compliance function cannot be organized independent of

28 See example, Institute of Internal Auditors – Australia (2016) 'Whitepaper – Auditing your entity's Compliance Framework', Institute of Internal Auditors - Australia, Sydney, October 2016. (online) https://iia.org.au/sf_docs/default-source/quality/white-papers/auditing-a-compliance-and-ethics-program.pdf?sfvrsn=2&submission=267946591

29 See example the "IDW Assurance Standard: Principles for the Proper Performance of Reasonable Assurance Engagements Relating to Compliance Management Systems" by Institut der Deutschen Wirtschaftspruefer, 2021

30 See example, Institute of Internal Auditors – Australia (2016) 'Whitepaper – Auditing your entity's Compliance Framework', Institute of Internal Auditors - Australia, Sydney, October 2016, p. 6 (online) https://iia.org.au/sf_docs/default-source/quality/white-papers/auditing-a-compliance-and-ethics-program.pdf?sfvrsn=2&submission=267946591

31 Isabella Arndorfer & Andrea Minto (2015) 'Financial Stability Institute Occasional Paper No. 11, The four lines of defence model for financial institutions' (online). http://www.bis.org/fsi/fsipapers11.pdf and Christophe Veltsos (2017) 'Take a Load Off: Delegate Cyber Risk Management Using the Three Lines of Defense Model', *Security Intelligence*, November 20, 2017 (online), https://securityintelligence.com/take-a-load-off-delegate-cyber-risk-management-using-the-three-lines-of-defense-model/

32 Institute of Internal Auditors (2013) 'The Three Lines of Defense in Effective Risk Management and Control', Institute of Internal Auditors, Altamonte Springs, p. 7.

the overall setup of governance functions, but must take into account its environment.

While recognizing that organizations are different and the actual circumstances are also varying, the TLOD therefore stresses the importance of information sharing plus the coordination of activities across the three lines or even with external assurance providers, thus attempting to avoid gaps in coverage without duplication of work. This covers the procedural dimension of organization, beyond the pure allocation of roles to certain teams. The TLOD model then ends with specific recommendations:

> "*Recommended Practices:*
>
> - *'Risk and control processes should be structured in accordance with the Three Lines of Defense model.*
> - *Each line of defense should be supported by appropriate policies and role definitions.*
> - *There should be proper coordination among the separate lines of defense to foster efficiency and effectiveness.*
> - *Risk and control functions operating at the different lines should appropriately share knowledge and information to assist all functions in better accomplishing their roles in an efficient manner.*
> - *Lines of defense should not be combined or coordinated in a manner that compromises their effectiveness.*
> - *In situations where functions at different lines are combined, the governing body should be advised of the structure and its impact. For organizations that have not established an internal audit activity, management and/or the governing body should be required to explain and disclose to their stakeholders that they have considered how adequate assurance on the effectiveness of the organization's governance, risk management, and control structure will be obtained*"[33]

For the specific role in the compliance profession, the TLOD model and its recommended practices offer good guidance when looking at setting up an adequate organization. At the same time, given its positive reception and wide acceptance, it can serve as a good reference point to have the necessary discussions with all parties involved. Lastly, its simplicity and clarity make it easy to remember and refer to, thus increasing the chance of making good arguments and good choices.

[B] An Update: The Three Lines Model

Despite its excellent reception, the TLOD has of course had its fair share of criticism. This does not surprise, since any model must simplify reality, as Ruud noted with respect to the TLOD – a model can only be fit for a certain

33 Ibid.

purpose.[34] One may also argue that the higher the number of stakeholders and related interconnections, the more criticism to be expected for a model targeting general applicability. Both theory and practice had their own remarks, with the first one mostly concerned with the unusual model background and a lack of empirical testing,[35] and the latter one anxious about more practical issues with experts like Nicholson conceding that:

> *"[T]he model also has many critics. By focusing narrowly on risk management and control, it separates defensive measures without telling the whole story. It has a tendency to create silos that may appear static and inflexible. The graphic illustrates clearly separated components that are (or need to be) much more closely interrelated with areas of overlap and "blurring." Unrealistic expectations of the second and third lines can give false comfort to the first line and the governing body. It can seem more relevant to the private for-profit sector and larger organizations. Despite its best intentions, the model may create confusion and the impression of duplication of resources and overlap of effort with respect to risk management... There is even debate over the appropriate naming of the model and how many "lines" there are. A number of alternate models have been created, but without the high adoption rates of the Three Lines of Defense*."[36]

These critical voices from practice have been well organized in an overview by Deloitte,[37] which intends to align these along different stages of maturity. In that approach, early stage adoption turns out to be mostly characterized by complaints of inefficiencies and duplicated efforts. Then, the more established lines of defense seem to be habitually plagued by lack of coordination, with silo mentality reducing the effectiveness due to gaps and misalignments plus a retroactive view. Finally, the most mature lines of defense are described as making efforts to be more proactive, but now facing the danger of over psychological reactions in each line – audit fatigue by the first line due to perceived double testing, over-reliance by management on the second line, and potential overburdening of the second and third lines by ever-added new tasks.

34 Flemming Ruud (2019) 'Reflections on the Three Lines of Defense', European Commission, Audit Services, November 27, 2019, Brussels (online). https://ec.europa.eu/info/sites/default/files/business_economy_euro/accounting_and_taxes/presentations/presentation_flemming_ruud_2019_en.pdf

35 See Howard Davies & Maria Zhivitskaya (2018) 'Three Lines of Defence: A Robust Organizing Framework, or Just Lines in the Sand?', *Global Policy*, vol. 9, no. S1, pp. 34–42.

36 Francis Nicholson (2019) 'Three lines of defense: Report on the public exposure findings June – September 2019', IIA October 2019, pp. 3-4 (online), https://na.theiia.org/about-us/about-ia/Documents/Public-Exposure-Report-General-Release.pdf

37 Deloitte (2020) 'Modernizing the three lines of defense model: An internal audit perspective' (online), https://www2.deloitte.com/us/en/pages/advisory/articles/modernizing-the-three-lines-of-defense-model.html

This led IIA to consider the introduction of a (partially) new model, the so-called three-line model (TLM) – interestingly promoted by the same organization that had popularized the original version with its long history in risk management. Its July 2020 paper,[38] again has a programmatic title 'The IIA's Three Lines Model – An update of the Three Lines of Defense' and makes clear the direction. However, the contents are much more far-reaching than the title would suggest, introducing a focus that is much broader than just organising the relevant functions.

In order to develop the model further and to ensure sufficient consensus, IIA had actually gone through a process of nearly one year of public exposure, also including questions regarding the TLOD acceptance and areas for improvement.[39] On the positive side, the responses were very encouraging for the existing model, with 80.9% strongly approving or mostly approving of the well-known graphics, and even 81.5% doing so for the overall TLOD model. Such good acceptance should in fact caution model developers as well as users not to deviate too far from the existing model. Nevertheless, the document also outlines major areas for improvement:

- *"The naming of the model to reflect something more than "defense."*
- *Encouragement for communication, coordination, and collaboration across the lines to avoid silos.*
- *The first line remains responsible for risk management and must be held to account for this.*
- *Emphasis that internal audit must review the effectiveness of the first and second lines.*
- *Allowance for maturity and scalability.*
- *Relevance for the not-for-profit sectors*."[40]

To answers such critical comments, the new TLM has set out to optimize the initial model along four avenues.[41] Firstly, it embraces a principles-based approach so as to suit all types of organizations (in an even better way). Secondly, it intends to move the focus from TLOD's value protection and "defense" to value creation and the realization of the organisation's objectives. Thirdly, it intends to provide a clear understanding of the roles and responsibilities provided in the model. Finally, the updated model shall

38 Institute of Internal Auditors (IIA) 2020 'The IIA's Three Lines Model – An Update of the Three Lines of Defense'. Institute of Internal Auditors, Altamonte Springs.

39 Francis Nicholson (2019) 'Three lines of defense: Report on the public exposure findings June – September 2019', IIA October 2019, (online), https://na.theiia.org/about-us/about-ia/Documents/Public-Exposure-Report-General-Release.pdf

40 Institute of Internal Auditors (IIA) 2020 'The IIA's Three Lines Model – An Update of the Three Lines of Defense'. Institute of Internal Auditors, Altamonte Springs. p. 13.

41 Ibid.

put a special focus on aligning all activities with the interests of stakeholders. These optimizations are presented in three major blocks, to be described and evaluated in the following paragraphs.

[B] [1] Six Principles of the Three Lines Model

In a very important step versus the previous model structure, the new TLM starts out with introducing six well-described new principles and was supplemented by a reworked graphic description of the model.[42] These basic principles tie in with the well-established discussion about the merits of rule-based versus principle-based regulatory approaches. This discussion, initially started with accounting and law, has come to a point of not viewing these two approaches as antagonistic, but rather as fulfilling specific tasks. Sama & Shoaf argue that both rules and also principles have their roles to fulfill, with principles giving direction more from a global perspective, and rules establishing something like minimum standards (which then may or may not be localized).[43] One may therefore argue that principles have their role to play, and therefore we see the development presented in the TLM as a logical extension to the prescriptions given in TLOD.

The TLM six principles are as follows:[44]

Principle 1: Governance

In line with its wider scope, this principle sets out to define governance of an organization. It posits that both appropriate structures and processes are needed to attain three major necessities: firstly, it must enable accountability by the defined governing body towards the stakeholders, allowing for integrity, leadership and transparency to be applied by this body. Secondly, governance must be based on actions (notably including the management of risk) by management to accomplish certain objectives through both risk-based decision-making and the related assignment of resources. Finally, it requires assurance and advice through an independent function such as internal audit function, complementing the two other functions, for confirmation and confidence. It should be noted that this in fact describes the role of three lines as per TLOD.

Principle 2: Governing body roles

In the next principle, the roles of the governing body are explained as ensuring the existence of appropriate structures and processes for effective implementation of Principle 1, plus as making certain that objectives and activities of the organization are aligned 'with the prioritized interests of

42 Ibid., 2-4.

43 Linda M. Sama & Victoria Shoaf (2005) 'Reconciling Rules and Principles: An Ethics-Based Approach to Corporate Governance', *Journal of Business Ethics*, vol. 58, no. 1/3, pp. 177–185.

44 Institute of Internal Auditors (IIA) 2020 'The IIA's Three Lines Model – An Update of the Three Lines of Defense'. Institute of Internal Auditors, Altamonte Springs

stakeholders'.[45] In assigning responsibilities and resources to management, the governing body shall assure that the given objectives are achieved whilst fulfilling the legal, regulatory, plus ethical requirements. In its oversight function, the governing body is also to set up and supervise an independent role and that shall provide visibility on progress – defining this as internal audit. This naming is of course logical, also in light of the authors of the TLM being from this profession, but it might deter smaller organizations or less complex setups to ensure that the role is fulfilled, be it internally or externally. We hold the view that the criteria of competence, objectivity and independence for such function are most important, definitely more so than the name given to such role.

Principle 3: Management and first and second line roles

Despite its recourse to the six basic principles, the TLM again takes up the language of first, second and third roles. As in the initial model, the first line is represented by the management, charged with the task of delivering products and service as per the objectives of the organization. Also allocated to the first line are support tasks such as HR and administration, as they are part of this delivery process. This makes them different from the second line roles which exist purely to assist with managing risk. In any case, the responsibility for managing risk stays allocated with the management and is therefore a first-line task.

This principle of ultimate management responsibility logically allows for an important clarification in TLM, namely that; "*[f]irst and second line roles may be blended or separated*."[46] No preconditions are given for such role combinations, rather pointing at the possibility of assigning second line roles to specialists with complementary expertise, including in the fields of risk; internal control; security of information and technology; sustainability issues plus quality assurance – and of course, "*[c]ompliance with laws, regulations, and acceptable ethical behavior*".[47] We had noted the possibility of combining roles already for the initial model, although in a much more muted tone, calling out that, "*[i]n exceptional situations that develop, especially in small organizations, certain lines of defense may be combined*."[48]

For a practitioner, it will be regularly difficult to decide on the adequacy of such exemptions, thus inviting special scrutiny by regulators or other institutions checking on governance. It is therefore recommended to stick with the three lines as much as possible, or otherwise to document the reasons as well as measures taken to mitigate the disadvantages, such as occasional external reviews or similar. In some way, our practical recommendation seems to

45 Ibid., 2.

46 Ibid., 3.

47 Ibid.

48 Institute of Internal Auditors (2013) 'The Three Lines of Defense in Effective Risk Management and Control', Institute of Internal Auditors, Altamonte Springs, p.7.

go against the authors' intention of more flexibility when organizing for compliance.

An important footnote to that principle reveals that in the minds of the TLM authors, the denominations as first, second and third line are, "*[r]etained from the original model only in the interests of familiarity. However, the 'lines' are not intended to denote structural elements but a useful differentiation in roles. Logically, governing body roles also constitute a "line", but this convention has not been adopted to avoid confusion. The numbering (first, second, and third) should not be taken to imply sequential operations. Instead, all roles operate concurrently*."[49] This is relevant, and it also applies to the third line which will be covered by the next two principles. For compliance, just as for any other function that is part of the governance structure, it is essential to understand that there is a real need to perform one's function concurrently to that of all other actors.

Principle 4: Third line roles

In this principle, the task of the third line is described as both assurance and advisory roles regarding adequate and effective governance and risk management, with a focus on independence and objectiveness for the role. This is in line with the current status for an internal audit function, which over the last decades has added the advisory part to the portfolio. As is evident, the balance between the important assurance functions and the newly added advisory role is subject to permanent review.

The principle also highlights the necessary capabilities of such internal audit providers, including the need of continuous improvement, and it points to the possibility of using assurance from other internal and external providers. Finally it posits that findings are reported to the management and the governing body, in effect requesting dual reporting lines.

Principle 5: Third line independence

In this principle, the state-of-the-art literature on internal audits and the IIA's own international standards for the professional practice of internal auditing (IPFF) published recently[50] are referred to when describing requirements as independence from the responsibilities of management, "[*t]hrough: accountability to the governing body; unfettered access to people, resources, and data needed to complete its work; and freedom from bias or interference in the planning and delivery of audit services*".[51] This strengthens their perception of being objective, authoritative, and credible.

49 Institute of Internal Auditors (IIA) 2020 'The IIA's Three Lines Model – An Update of the Three Lines of Defense'. Institute of Internal Auditors, Altamonte Springs, p. 3, footnote 1.

50 See Institute of Internal Auditors (IIA) 2017, 'International standards for the professional practice of internal auditing' (online), https://na.theiia.org/standardsguidance/Public%20Documents/IPPF-Standards-2017.pdf.

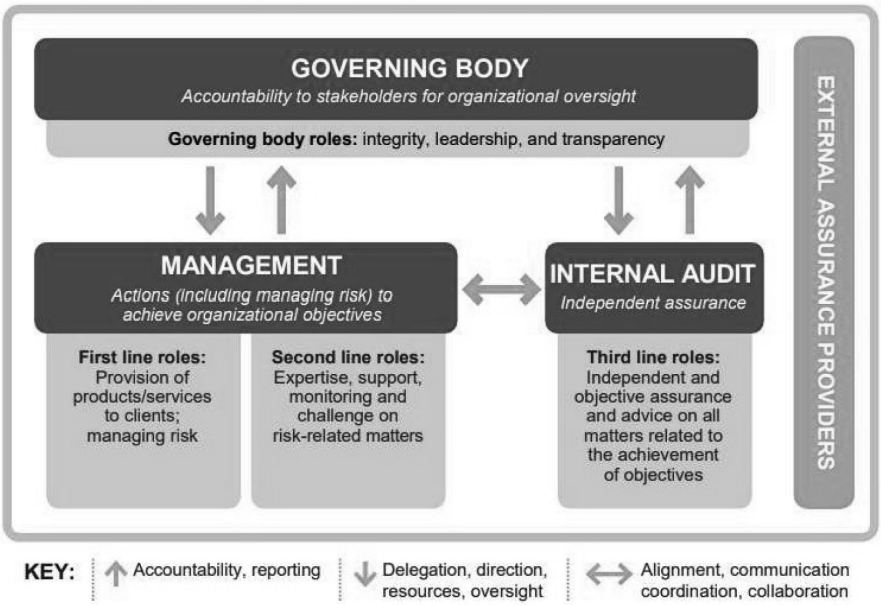
51 Institute of Internal Auditors (IIA) 2020 'The IIA's Three Lines Model – An Update of the Three Lines of Defense'. Institute of Internal Auditors, Altamonte Springs, p. 3.

Principle 6: Creating and protecting value

In the last principle, the model clarifies (already in its headline) that all roles are to work towards not only protecting value, but also towards creating it – a point often voiced, despite this being part of the previous model version already, given that it is part of the risk management that also look at opportunities. In that principle, alignment of all roles among each other and with the stakeholders' interests is called for – via communication, cooperation and collaboration so that adequate information for risk-based decisions can be provided. This last principle with its focus on coordination is in that sense similar to what the TLOD ends on, although without the recommended practices given by the earlier model.

Obviously, all the six principles relate to the key actors in corporate governance, although they do not take care of the relations among them yet. This is addressed in a new graphic illustration as per figure 8, and in the subsequent discussions.

Figure 8: The IIA's Three Lines Model (TLM Model)



Source: Institute of Internal Auditors, 2020

[B] [2] Key Roles in the Three Lines Model

Accepting the considerable differences in how responsibilities are organised in different organizations, the model TLM makes an effort to describe the key roles in a way that supports the principles set out for the TLM. It addresses this on a relatively high level for (1) the governing body, (2) management in both its first line and second line roles, (3) internal audit, and (4) added external assurance providers. In that effort, it turns out to be in line with most of the related governance literature: [52]

1. For the governing body, its responsibility towards stakeholders is key – in determining their prioritized interests and ensuring the achievement of related objectives, including cultivating an ethical culture, setting up structures and processes for governance, delegating responsibility and providing resources to management, setting up the desired level of risk appetite and ensuring the second and third roles are performed. Specifically for the topic at hand, it '"*[m]aintains oversight of compliance with legal, regulatory, and ethical expectations*."[53]
2. For management in its first line roles, it acts according to this guidance (including risk management) and uses the resources entrusted towards the set objectives, keeps in ongoing dialogue with the governing body through adequate reporting, implements and executes the necessary procedures and – again – "[*e]nsures compliance with legal, regulatory, and ethical expectations"*.[54] In the second line roles, the functions shall be responsible for, *"[c]omplementary expertise, support, monitoring, and challenge related to the management of risk*,"[55] towards the same targets, including compliance. It is noteworthy to see the task of challenging management form second towards first line as a task intrinsic to the compliance function. The provision of analysis or reports form the second line shall help achieving this in a balanced form.
3. As to internal audit, irrespective of any other reporting lines, it shall remain first for all accountable to the governing body, ensuring its independence. This is a key clarification that needs to be reflected in respective organizational designs. Administrative lines to management can be tolerable, should however, be kept at a minimum level. This allows the third line to provide independent and objective assurance and advice to the management and the governing body on the adequacy and effectiveness of governance and risk management (including internal control)'.[56] It shall also report any problems with its own independence and objectivity to the governing body as well as set up safeguards as needed. We would add that it is also the task

52 Ibid.

53 Ibid., 5.

54 Ibid.

55 Ibid., 6.

56 Ibid.

of the governing body to regularly ensure with the third line that it is sufficiently independent and has adequate resources to perform its task.

4. The external assurance providers, such as external auditors and other consultants, are tasked with providing additional assurance regarding legal and regulatory requirements 'that serve to protect the interests of stakeholders'.[57] Such external assignments can be initiated by both the management and the governing body. Whilst not laid out in the TLM, also the third line normally has the right to make requests for independent external assurance. Principle 4 also supports that view, as it makes external work a generic part of these efforts. The same is true for the compliance function, which as part of the second line is seen as the management and is thus also able to draw on such additional resources.

[B] [3] Relationships among core roles

Upon describing the roles in much detail, one challenge remains – the coordination between the respective roles. This brings back to mind the newly introduced flexibility of the new model, a flexibility necessary that *"[t]he model applies to all organizations*",[58] irrespective of their size and regulatory environment (just as claimed by the previous model already). The TLM maps out the following relationships:

Governing Body and Management

The relationship between the governing body and the management (explicitly including first-and second-line roles) acknowledges the role of the former in setting vision and mission, but also values and – outstandingly critical – risk appetite of the organization. The management is entrusted with the necessary resources and responsibilities to achieve its objectives.

The model allows for these roles to be partially overlapping again, surprisingly both for strategic issues and somewhat for operational topics: the lead in developing the strategic plan may (logically) be taken by either role, but also other hands-on interventions are not excluded. In any case, strong communication is required between the management, including where applicable, its chief executive officer, and the governing body.

This flexibility in terms of overlaps or separation between these two actors is not only due to the different models of governance in specific jurisdictions, with their single-tier, dual-tier, or hybrid board structures,[59] but may also arise from regulatory pressures or distinct governance choices, such as the

57 Ibid.

58 Ibid., 1.

59 Mohan Datwani, Junko Dochi, Say H Goo and Kai-Uwe Seidenfuss (2018), 'One-Tier, Two-Tier and Hybrid Board Structures in Hong Kong, Germany and Japan: A Governance Perspective' *Company Lawyer*, vol. 39, no. 10, pp. 345-348.

implementation of a chief risk officer or a chief compliance officer with reporting lines also to the governing body – both expressly acceptable and consistent with the new TLM. The graphic reflects this accordingly.

Management and Internal Audit

For this second set of relationships, the management again includes both first- and second-line roles. Alignment is required between internal audits and the management to ensure the achievement of organizational objectives. Whilst independent in its role, internal audit is not isolated and can pursue its core role of assurance most effectively when engaging in collaboration and communication with the other line(s).

Avoidance of double work, overlaps, or even gaps requires such exchange when limited to providing the core task of assurance, but even more so when targeting an advisory role for internal audit – as typical in the recent literature. Given the IIA authorship,[60] it is not surprising that the model follows the same path toward a wider role for internal audits in the TLM.

Internal Audit and Governing Body

Given the accountability of internal audits to the governing body, direct access to the Chief Audit Executive is key, as is a direct reporting line, although administrative secondary reporting line(s) can be established. This solution reflects the US and other countries' situations much more than the actual practice in several European or Asian setups, but it is nevertheless a desirable solution to establish such a line to the audit committee, although not necessarily the only one as posited in the TLM.[61] In addition, private sessions without the management are typical of many companies.

Among all roles

Lastly, for all actors to coherently contribute to the objectives of the organization, efficient alignment via regular coordination, collaboration, and communication is required in the TLM. This reminds of the last chapter in TLOD and thus closes the circle between the two model versions.

¶12-040 Implications

What does it mean for the task of organizing for compliance then? A comparison of model contents plus the difference in reception of the two model versions provide good guidance for this ongoing task: first of all, TLOD is surely the most established and well-received model so far, especially when

60 See also Nicole Di Schino (2020) 'Does the New Three Lines Model Give Short Thrift to Compliance?', Corporate Compliance Insights, August 12, 2020, https://www.corporatecomplianceinsights.com/three-lines-model-short-shrift-compliance/

61 For experimental evidence see Carolyn Strand Norman, Anna M Rose, & Jacob M Rose (2010) 'Internal audit reporting lines, fraud risk decomposition, and assessments of fraud risk', *Accounting, Organizations and Society*, vol. 35, no. 5, pp. 546–557.

it comes to being taken up by regulators. However, as stated by Wyman, the TLOD has always been a, *"[p]ervasive but unloved model (especially in the financial sector), but we believe that reluctance to commit to the framework is the primary driver of the ineffectiveness perceived in its implementation*".[62] The overall task remains a challenging one, whichever model is chosen, it requires considerable amounts of resources and discipline. A renewed model does not change this situation by making it more flexible. It may rather shift the balance to some degree. By the same logic, Arjoon already notes corporate governance as the task, *"[t]o strike an optimal balance between rule-based and principle-based approaches*."[63]

It thus remains to be seen whether members of the governance bodies in less-regulated industries will take the flexibility of the new model, or rather, for their own peace of mind, stick to the more predictable rules laid out in the TLOD. It is shown that while the new TLM provides some commendable elements, positive additions are the long-due (but rarely requested) inclusion of the governing body as a responsible actor, not least when setting up correct governance including compliance functions. The TLM also provides some helpful clarifications in terms of necessary communication and coordination, while it makes an effort to shift the balance towards a more integrative governance model. In addition, several criticisms of the previous model have been addressed, especially by clarifying the proactive stance of risk management and the need to consider the three lines not as consecutive, but as complimentary.

Of course, IIA has a valid point when it states that its TLM (or any other organization form, for that matter), "[*i]s most effective when it is adapted to align with the objectives and circumstances of the organization. How an organization is structured and how roles are assigned are matters for management and the governing body to determine."* [64] At the same time, the explicit allowance for organizational flexibility in terms of the three lines does not help practice, nor has it so far been taken up by regulators or practice, plus it comes at the cost of clarity and robustness.

We would rather argue to keep the structural proposals of the TLOD, especially to stick to the three separate lines wherever possible, and to keep in mind the recommended practices of the TLOD. We also remain strong proponents of the initial graphic description, which in fact did go back a much longer way, despite some of improvements included in the new one. In

62 Oliver Wyman (2016) 'Whose line is it anyway? Defending the three lines of defense, Asia Pacific Finance and Risk Series', p. 20 (online), https://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/nov/Three_Lines_of_Defence.pdf

63 Ibid., 53.

64 Institute of Internal Auditors (IIA) 2020 'The IIA's Three Lines Model – An Update of the Three Lines of Defense'. Institute of Internal Auditors, Altamonte Springs, p. 9.

our view, issues like reporting lines and coordination tasks are important,[65] but could very well be described in a simple, solid set of principles.

¶12-050 Recommendations

- We would therefore argue for a hybrid application of the TLOD and TLM – with a strong focus on the clear structural and procedural recommendations taken from the first, combined with the added flexibility of structure plus pragmatic principles and clarified roles taken from the updated second model.
- To be clear, when in doubt, it is recommended for practitioners to refer to the TLOD as the first recourse since the new TLM seems to increase complexity and reduce simplicity, which is of course typical for a more principle-based approach.
- Still, it may be a good idea to set up principles for the compliance function itself, for example in the form of a Compliance Charter or similar, which is embraced by the senior management, as is good practice for example in internal audit.
- As the permitted TLM departures from existing TLOD rules are not without risk, a guidance would be helpful.
- Finally, it is necessary to look at best practice around compliance organisations. Not only would this help to be at par with one's peers, thus avoiding criticism in case of unexpected compliance violations, it is also in line with the observation of Jennings that best practice should exceed legal standards – in our case, rules or principles – as such, standards are regularly designed to define a baseline or a minimum ethical level.[66] Compliance managers, as well as their senior management and the governing body should keep this in mind.

¶12-060 Conclusions and Commentaries

Apparent to all by now is that aims and goals of the three Lines Model was set out to be as comprehensive and thorough as possible with each of the lines monitoring and organizing compliance. Whilst the underlying idea behind this model is to minimize compliance gaps or even failures, it would appear to be somewhat cumbersome, overlapping or even complicated to implement with lots of redundancies built in. Nevertheless, it is a system that is more robust when it comes to monitoring as well as organizing compliance.

65 Ulrich Bantleon, Anne d'Arcy, Marc Eulerich, Anja Hucke, Burkhard Pedell, & Nicole V.S Ratzinger-Sakel (2021) 'Coordination challenges in implementing the three lines of defense model', *International Journal of Auditing*, vol. 25, no. 1, pp. 59–74.

66 Marianne M. Jennings (2000) 'Professional responsibilities, ethics, and the law', *AIMR Conference Proceedings: Ethical Issues for Today's Firm*, vol. 2, pp. 4-11.

However, more needs to be done in compliance audit, in particular creating an independent external audit like in financial reports. Critics might argue that it would increase the costs and burden of compliance, yet this should reduce chances of compliance failures in the overall scheme of things.