TRANSCENDENT GROUP INSIGHT

NEW PERSPECTIVE ON THE THREE LINES OF DEFENSE

During the summer, an update was presented on one of the most central and well-established models in the area of GRC: the concept of governance and organization in accordance with the Three Lines of Defense (3LOD). An international working group composed of various experts spent a long time in consideration and decided ultimately that it was time to update and refresh the model. The concept itself does not of course cease to exist, but as a start we now have to get used to a new name: the "Three Lines Model".

We will briefly explain why a change was considered necessary and the differences the new model will bring to the GRC table.

Why did it need to be changed?

The defense line concept has actually been around for more than 20 years, although it was not formalized until 2013 following inclusion in the IIA's Position Paper "The Three Lines of Defense in Effective Risk Management and Control". A comprehensive review and update to meet more current changes and challenges was therefore due.

Although the old model was suitable for its time, it has been subject to criticism in several key areas for several years. For instance, the name itself. Many believe that "defense" triggers images of resistance and avoidance of risk, that risk management is about defending oneself and that the business is seen to be under continual attack. This in itself means that risk management is perceived as reactive rather than proactive, i.e. that it diverts focus from the real purpose of risk management: namely, well-founded risk-taking (accepting the right risks) and acting on the most critical risks for the business.

Other criticisms include that the model is too limiting and restrictive and that it tends to create organizational silos with overly rigid structures. The authors of the new model also point to a drop in trust due to a number of scandals and crises in recent years in spite of the organizations in question having had three clear lines of defense in place.

An update to the model was therefore considered necessary in order to identify potential shortcomings, to make it applicable to modern organizations and also to underline the value creation of risk management to a greater extent than before.

New in the 2020 model

According to the IIA itself, the model has now been "optimized" through having:

- A principles-based procedure (comprising six principles) where the model can be adapted to the individual organization's goals and conditions
- Increased focus on risk management, thereby contributing to goal fulfillment and generating value, rather than just protecting value.
- Clarified the model's roles and responsibilities and how they relate to each other

- Increased emphasis on how the goals of the business need to be coordinated with priority stakeholder requirements.

The directly visible changes in the model are that the terms "defense" and "first", "second" and "third line" have been removed. The line concepts, however, are still used and are found in the principles, with the explanation that they are so established and accepted that removing them would lead to unnecessary confusion.

In terms of the model, lines 1 and 2 have been visually merged to demonstrate the possibility of different organization-specific solutions, even if the different activities for the original roles naturally remain (e.g. perform, monitor, advise and test). The third principle states explicitly that roles within the first and second lines can both be merged and separated.

Line 3 (internal audit) has for the same reason been disconnected to show that this is exactly where independence is important.

Whilst the previous model concretizes external audit and legislator / supervision (regulatory authorities) on the side of the model (sometimes referred to as the 4th and 5th line, respectively), the 2020 model has chosen only to highlight "external assurance".

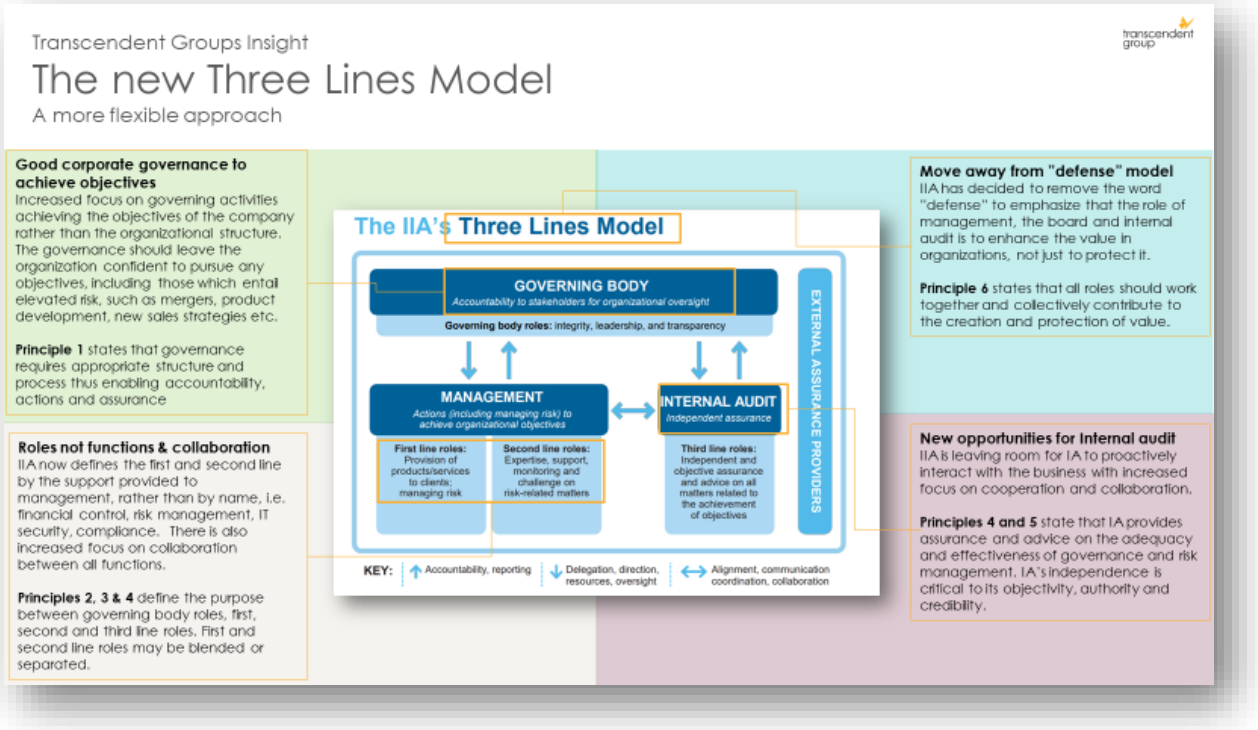

Figure 1. Highlight of changes to the new model

Reflections on the changes:

Governance to achieve objectives - focus on activity instead of organization:

The updated model does not really bring about a dramatic change in its approach to governance, i.e. how an organization should organize itself in order to have sound governance and internal control. It is very positive that the focus is on *activity* rather than *organization*. The 1st principle clarifies that **responsibility**, **activity** and **assurance** is required, rather than organizational functions.

The increased flexibility regarding an appropriate governance structure and the expectations that the Board of Directors ("BoD") should decide is very good from an efficiency and responsibility perspective. It is clear that the model aims to support businesses in making their own decisions on how to appoint, separate and also coordinate roles and functions, in comparison to the earlier more prescriptive model.

The increased flexibility will, in our view, support businesses better in their continual need to evolve out of necessity; responding to customers demanding real-time interactions, regulators applying increasing levels of scrutiny, and governance stakeholders requiring assurance in this complex and dynamic risk environment.

Roles not functions - Collaboration is key

The updated model has a much greater focus on coordination and collaboration. The 2013 model speaks, albeit very briefly, of coordination and information sharing between the lines, but it is stated that risk management "… is strongest when there are three separate and clearly identified lines of defense".

In the new model, the cooperation, collaboration and communication between lines and roles are now highlighted as key for effective governance. All too often, independence between different lines has been judged as being more important than collaboration, which has led to, in our opinion, both an ineffective governance structure with no coordination gains (e.g. increased efficiency, better coverage and clearer reporting) as well as frustration within the business. Focusing on roles instead of functions is an opportunity for the organisation; by placing risk thinkers in business processes, implement assurance activities into controls as they are designed will provide more real-time assurance and a better span of control across the organization.

Finally, by choosing to name the "4th line" as external assurance, thoughts are led to combined assurance. In our opinion, this is a clear signal of the value of coordinating assurance areas. We think, however, that it is slightly regretful that the model (at least not visually) does not advocate the importance of coordination and communication between external assurance and the business.

New opportunities - flexibility also in internal auditing

Good wording found in the text is that independence should not be interpreted as isolation. A well-functioning and efficient internal audit must, of course, maintain a good dialogue and functioning collaboration with the business and with the other assurance functions. It is interesting and welcomed that the model clearly opens up for internal audit to have other areas of responsibility and that it is not a problem if the internal auditor advises on different areas.

The focus is rather on the business's own assessment and whether it affects the ability to provide the credible assurance that the Board of Directors expects. Both "cooling off solutions" and the possibility for the BoD to turn to a "qualified third party" are mentioned if assurance is required in an area where internal audit is not considered to be sufficiently independent. Also note that principle 4 states explicitly that internal audit may also consider using assurances from other internal or external parties.

The interesting 2nd principle

The principles of the new model highlight a number of concrete points that are included in good governance, which make the model more adaptable. To be able to "prove" that the 2nd principle is followed, the BoD has to demonstrate that it has made active decisions on

reasonable and efficient processes and governance structures, and that the BoD has ensured that the business's goals are in line with stakeholders' requirements and expectations.

The same principle also clarifies that the responsibility for division of responsibilities and resource allocation lies with the board; both for goal fulfillment and compliance with rules, but interestingly enough also for "ethical expectations". In principle two, a requirement has also found its way in for the Board to appoint an independent and competent internal auditor.

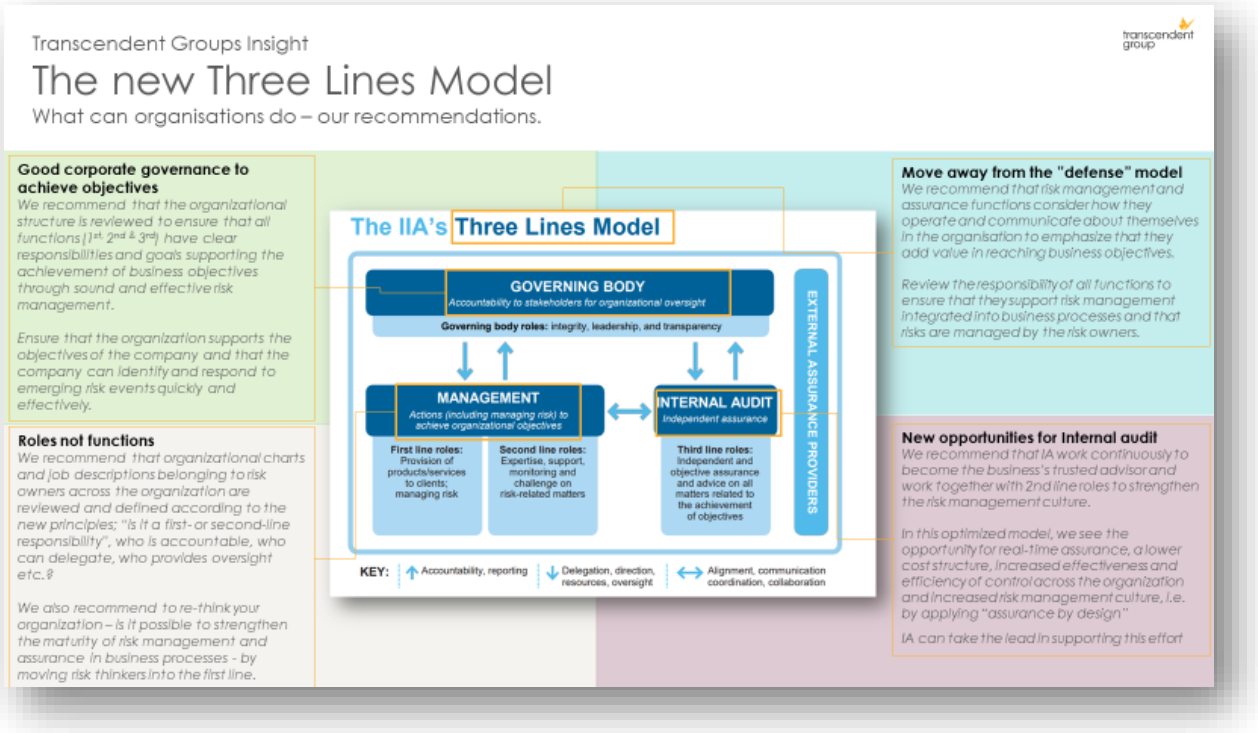

Figure 2: Recommendations updating current three lines model

Concluding reflections:

In summary, the most interesting conclusions in the updated Three-Line Model, i.e. how an organization should organize itself in order to achieve good governance and internal control, are:

- Focus on defined roles and responsibilities instead of organizational structures
- Room for increased flexibility requiring increased involvement and more "informed decisions" by the Board
- Clearly increased focus on the importance of collaboration between assurance functions
- Collaborate from top management to business management, ensuring that business goals are achieved through thorough risk informed decision-making

Let us know your thoughts and questions! How are You are going to use the new model?

Figure 3: Recommendations leveraging the new model

Please reach out

Hampus.Pihl@transcendentgroup.com

+46 72 329 59 79

Rasmus.Forssblad@transcendentgroup.com

+46 70 841 77 32

Heidi.Gliese.Hylleborg@transcendentgroup.com

+45 51 63 14 46

Gillean.Dean.Nordal@transcendentgroup.com

+47 48 01 40 71