

TO: IIA Three Lines of Defense Working Group

Jenitha John, IIA working group chair; vice chairman of The IIA Global Board of Directors; Chief Audit Executive, FirstRand Ltd

Mark Carawan, Chief Compliance Officer, Citigroup

Greg Grocholski, Chief Audit Executive, SABIC

Trygve Sørli, Independent Service Provider, Trygve Sørli Services EPF

Shannon Urban, Managing Director, EY

Beili Wong, VP, Audit and Risk, CAE, Liquor Control Board of Ontario

Charlie Wright, Chief Risk Officer, Jack Henry and Associates

c.c.:

Richard Chambers, CEO and President IIA

Paul Sobels, Chair of COSO

Re: June 2019 IIA Three Lines of Defense Exposure Draft

Thanks for the opportunity to provide feedback on the June 2019 exposure draft. This is an important IIA initiative and one that I have been actively encouraging my readers/followers globally to provide feedback on before the September 19th deadline.

I have been providing input directly to Jenitha John since the exposure draft was issued in June describing my top concerns with the 3LoD framework. For those interested in a more detailed commentary on 3LoD you can access a paper I co-authored with my daughter, Lauren Hanlon, then CAE of a listed Canadian company, published in THE HANDBOOK OF BOARD GOVERNANCE.

<https://riskoversightsolutions.com/wp-content/uploads/2011/03/3LoDvs5LoA-Elevating-the-Role-of-the-Board-and-CEO-Final-TLeech-LHanlon.pdf>

A short summary of my top concerns follows.

Use of the word “DEFENSE”: While I like the notion of “lines” in the name of the framework, I am strongly against retaining the word “DEFENSE”. It implies that the primary purpose of all the “lines”, particularly risk specialists and internal audit, is “DEFENSE”. This marginalizes the role of all the “lines” and implies the framework has no role in value creation or strategic planning. This is not consistent with the direction of COSO ERM 2017 for risk management or what Richard Chambers, IIA CEO/President sees for the IA profession. A Linked In post this week where I comment on this issue is available at <http://bit.ly/2ITwMHM>. The June ED

mentions the issues raised by the word “defense” but does not address the huge damaging impact of the word “DEFENSE”.

Recommendation: Replace the word “DEFENSE” with “ACCOUNTABILITY” or “ASSURANCE”

Role of management - the 1st line: Page 8 of the ED describes the role envisioned for management. It does not indicate that management is/should be responsible for learning how to self-assess the acceptability of the current state of risk linked to top value creation and preservation objectives. It also does not state that the 1st line should be responsible for regularly reporting on the state of risk linked top objectives upwards to the CEO and board. This **suggests to me that the working group has accepted/endorsed a WEAK 1st LINE governance model** and described the roles of all other lines assuming a WEAK 1st LINE that is not responsible for assessing and reporting on the state of risk linked to top objectives. This is very akin to endorsing manufacturing operations decades back that relied on the inspection department to identify and correct flaws from production. The framework should distinguish between WEAK 1st LINE models and STRONG 1st LINE models and provide an overview of what the roles of all the lines are in a WEAK 1st LINE model, and the quite different role of all the lines in a STRONG 1st LINE model. More comments on the weakness are available on my Linked In post available at <http://bit.ly/2IBKz5t>.

Recommendation: Provide readers with an overview of the roles of all the lines assuming a STRONG 1st LINE model where management is the primary risk assessor/reporter linked to top value creation and value preservation objectives. The current draft provides the role descriptions of the lines for a WEAK 1st LINE model. The guidance could describe the differing roles of the lines to illustrate the differences between a STRONG 1st LINE model and a WEAK 1st LINE model.

Assurance method(s) being used: There are 5 primary assurance methods organizations use to get assurance. These assurance methods are broadly defined as objective centric, risk centric, process centric, control centric, and compliance centric. These methods can be done by the 2nd and 3rd lines directly, or performed by management and quality assured by the 2nd and 3rd lines. These different assurance methods are described in an overview available at <https://riskoversightsolutions.com/wp-content/uploads/2011/03/Risk-Oversight-Solutions-Inc-10-Main-Assurance-Approaches-2019.pdf>. There are significant differences between the different methods.

When a company uses an objective centric assurance method applied to top value creation and value preservation methods it significantly elevates the role and stature of the 2nd and 3rd lines and helps “GOVERNING BODIES” meet escalating expectations that boards oversee the

company's strategic planning process. The ED makes no reference to the technical assurance method(s) being used by an organization, in spite of the fact that roles of all the "LINES" is significantly impacted. For example, in most organizations that use a risk centric/risk register based ERM framework few internal audit departments today provide much formal assurance to the board that the information they are receiving from the 2nd line/risk group is reliable.

Recommendation: Provide an overview of this issue in the guidance that describes the impact on the lines when different combinations of assurance methods are used.

Number of "lines": the ED is about THREE LINES OF DEFENSE but introduces a fourth line – GOVERNING BODY. It isn't clear if the current 3 lines in the IIA THREE LINES OF DEFENSE model is going to become 4 lines in the final guidance document. The ED does not envision the CEO and C-Suite as a "line" in spite of the fact that, in my experience, the role of the CEO is absolutely key to the long term success of an assurance framework.

Recommendation: Endorse the five line approach many have advocated since the IIA THREE LINES OF DEFENSE was introduced that elevates the roles of the CEO and C-Suite and the board of directors.

Thank you again for the opportunity to comment. I hope you find my summary observations useful. I would be happy to provide my support/details for all of the points made above. Best wishes for success with the final guidance.

Sincerely,



Tim Leech CIA CRMA CCSA
Managing Director