Revitalize 3 lines of defense if you stop …

*By **Kelvin To**, Founder and President of Data Boiler Technologies*

Have you and/or your risk and compliance teams been fidgeted lately, because:

(a) Overwhelmed by the regulatory burdens and/or the growing complexity of the market;

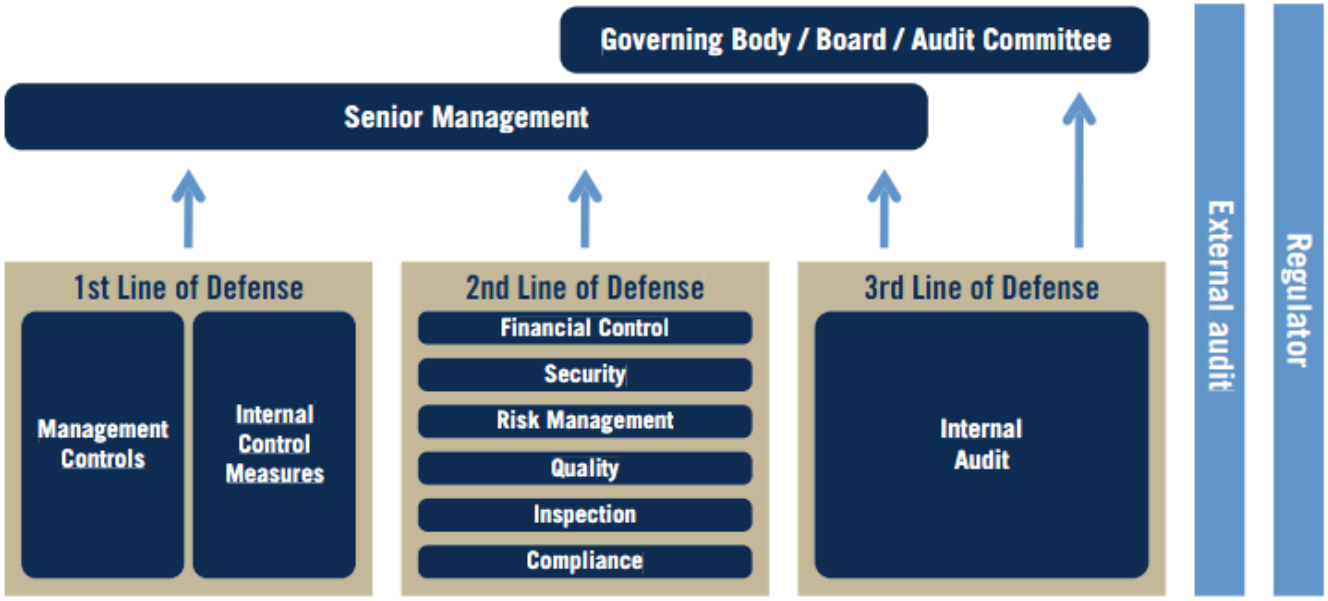
(b) There aren't enough people to do all the works, or overbearing of responsibilities for others' wrongdoing;

(c) Lack data and/or tools to perform risk aggregation, timely analysis, and/or implement preventive measures;

(d) All of the above; (e) No comment because I'll be gone (IBG) and/or you'll be gone (YBG).

Stop fidgeting regardless of what reason(s) you have chosen above. Revitalizing 3 lines (3LOD) of defense isn't about adding pressures on top of anxious teams.

The characteristics of the 3 lines of defense are summarized graphically below as per the ECIIA/FERMA guideline:



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

A large extent of the pressure may come from outside, especially for those who chose (a). The industry has been pushed to the corner. For the first time ever we have heard a major global bank cried out, "Deutsche Bank has no intent to settle these potential civil claims anywhere near the number cited", that's bold! The reality is: $14 billion in settlement could strain the bank's capital, making it the riskiest among its peers if not worst. You can perceive the situation as one

fighting back for survival, or speak up on a dispute, or simply fed up with the regulator directive to tell them what to do, etc. **The fact is, the industry has passed tests, deleveraged, and raised significant amount of capital time after time as per the regulators' instructions** (see related article)**.** Anyone would be frustrated if they see no end in this tunnel, or a further heightening of capital may introduce policy risks to the market. Instead of being in grief, let's honestly and positively work with the regulators. Share with them how you intend to strengthen the 3LOD, and hope there'll be appropriate reliefs.

According to Paper #11 by the BIS Financial Stability Institute (FSI), they outlined weakness and past failures of 3LOD as:

- "Misaligned incentives for risk-takers in first line of defense (1st LOD)
- Lack of skills and expertise in second line functions (2nd LOD)
- Lack of organizational independence of functions in second line of defense (2nd LOD)
- Inadequate and subjective risk assessment performed by internal audit (3rd LOD)"

These are pretty strong accusations. Allow me to rebuke them and decipher if anything the 3LOD can do better.

Stop accusing 1st LOD, respect their field experience and knowledge about nuances

First and foremost, I despise teaching the boss how to run a business! Business will do everything they can to protect the bottom-line if they are already held accountable for their own loss. One thing a Chief Risk/ Compliance Officer (CRO/ CCO) should pay close attention though, is short-sighted strategy that compromises controls and/or risks may only be exposed after IBG/ YBG. Other than that, let the 1st LOD do their jobs.

1st LOD are people in the field well versed with operational management. They should be respected and given the necessary discretions because they **know more of the nuances and possible glitches than anyone seating at the 2nd LOD**. Somehow, certain risk treatments are better to handle with immediacy than over analyze for a perfect solution. No doubt that 2nd LOD should set boundaries, policies and risk appetite to curb "misaligned incentive" in 1st LOD. You do need to tell 1st LOD exactly when to inform, consult, and escalate. If these weren't well defined and 1st LOD aren't supported by implementable procedures, then don't judge the ability and integrity of 1st LOD.

Given said that, 2nd LOD should leverage the field insights from 1st LOD in gathering essential early warning signals. By collaborating with 1st LOD, they should **jointly determine what data and/or tools they'll need to perform the necessary aggregation, accurate, complete, and timely risk analysis**. In other words, address the issues as stated earlier in point (c) via process automations.

Stop diminishing 2nd LOD for they are experts in design of controls and remediation

Next, I am perturbed by the FSI author whom undermines the independence, skills, and expertise of the 2nd LOD. I think it is wrong to stir conflicts between the 3LOD. Using the same example as in paper #11, 2nd LOD should ensure appropriate controls are embedded in the design prior to deployment of any complex models by the front-office. 2nd LOD should clearly set out conditions where the 1st LOD will do their daily monitoring via a robust control system. The 1st LOD is responsible for managing the queue of these warning signals, escalate as appropriate, and allow the system to retain proper audit trail for the 3rd LOD to review. As illustrated, 2nd LOD **should be encouraged to communicate with other stakeholders on regular basis, if not daily**.

They should have no worry about being swayed because professionals in 2nd LOD earn their authorities and creditability through extensive trainings, experience, and upheld absolute integrity**.** Risk management functions are in large, if not all, report formally to the board. If one can understand and appreciate the **segregation of duties** between 1st and 2nd LOD, then they'll know that it is not about how well the 2nd LOD can challenge the 1st LOD to demonstrate their supremacy. **2nd LOD expertise resides on their abilities to analyze the convergence of risks** and **skills to remediate**. They are supposed to be designers of systems to prevent possible gaming of controls.

Stop asking 2nd LOD to be judges when 3LOD are out of balance

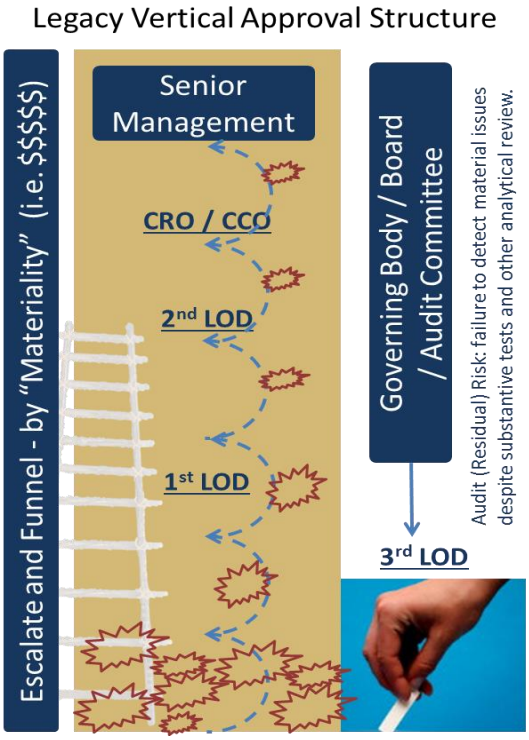
The balance of power and relationship between 3LOD should be **like the Executive, Legislative, and Judicial branches**.

When you got this big picture right, it'll be easy to figure out how to address the problem mentioned in (b). The reason why 2nd LOD feels there are not enough people to do the works is because they are **misguided to become the checker of everything the 1st LOD have done.** 1st LOD is like the Executive Branch, which meant to have the most headcounts in carrying out their responsibilities. 2nd LOD are indeed policies makers. They conduct in-depth researches, and debates on how to balance the right controls with fulfillment of business objectives. They may take up the market risk function and other macro issues. However, **don't pretend to be judges when they aren't**.

Detecting if there may be possible failure/ breach of control(s) in the front-office is indeed the responsibilities of the 3rd LOD. In reviewing the recent Wells Fargo's scandal, the matter could simply be unveiled by sending confirms to validate

accounts. I believe the audit team had done so, but they lack (or hesitated to use) authority to impose consequences when corrective actions are missing. As a result, the entire bank is punished by public criticisms. If CRO/CCO smells something fishy going on in the 1st LOD, they should refer to the 3rd LOD to perform independent assessment. **Evaluate the effectiveness of controls has always been, and should continue be, the professional duties of audit.**

Stop picking on the 3rd LOD's natural limitations while organization's hierarchy needs to be transformed



Most CROs/ CCOs rise to their ranks through a vertical hierarchy where they got higher and higher approval limits as they proven their abilities to manage bigger exposure items. However, this **legacy approval structure failed to cope with today's risk and compliance challenges**.

The old centralized process tends to funnel only the biggest dollar exposures for the upmost seniors to review. Risk measurements, such as Value-at-Risk, often over emphasized on dollar exposures and **neglected the timeliness of the matter**. As a lesson learnt from the Credit Suisse case where senior management were blindsided about risky positions, one should realize that breach of controls only take less than a split-second and losses can mount up to billion at lightning speed.

Besides, compliance checking and/or regulatory reportable items do not necessarily include every possible reputational risk for the organization.

Yet, the current political headwind will pinch down any seniors for every little wrongdoing within their organizations. Reference again to the Wells Fargo accounts scandal, **how to ensure warning signals won't be discounted along the hierarchy chain, and what constitute as "material"**? These are serious questions that every organization should revisit. In summing up the reasons for risk management failure, we can boil down to these two:

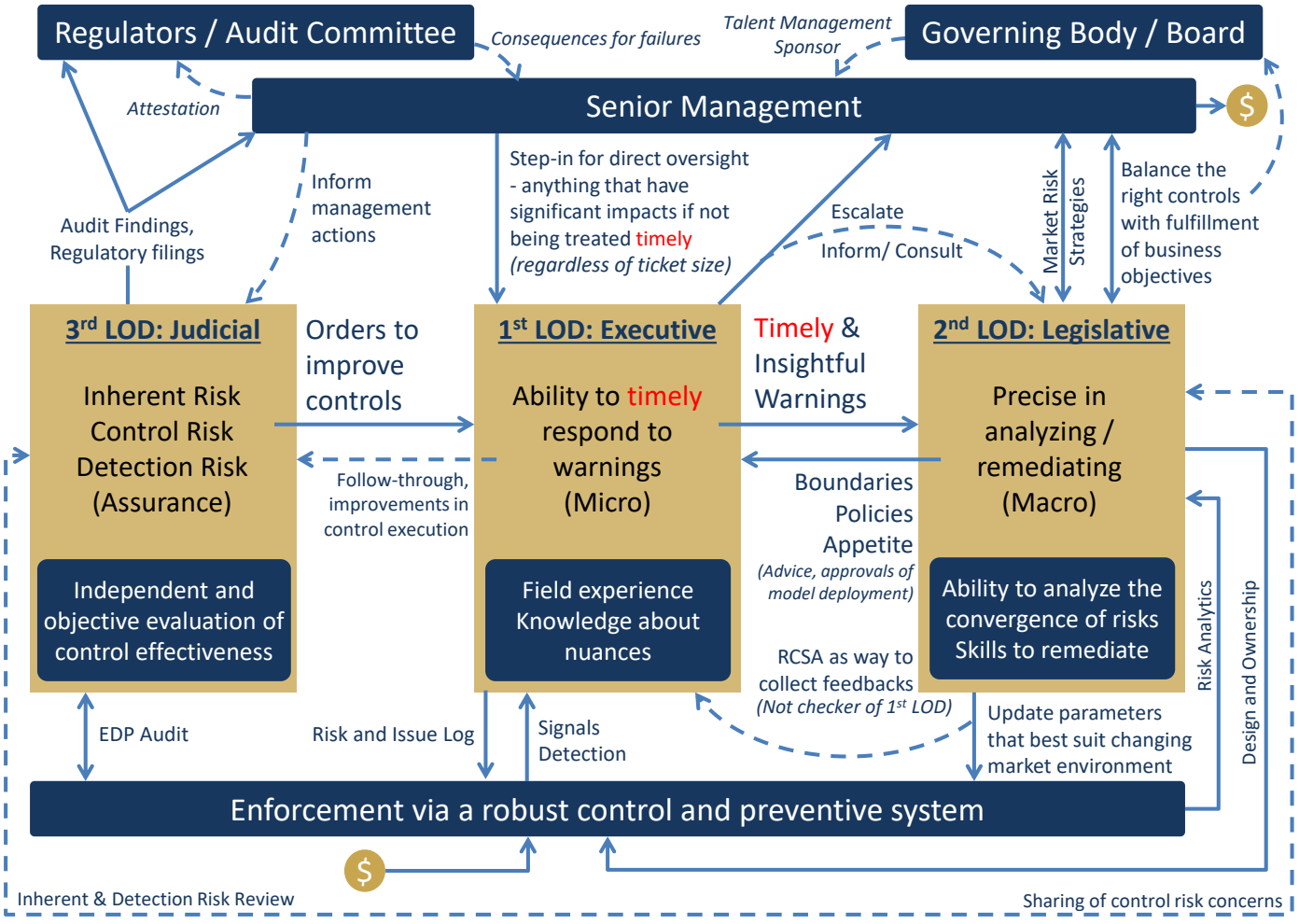
1. **Lack timely and insightful warning;**
2. **Inability to timely response to warning.**

A robust preventive risk management system should be able to help in here. In fact, management and the public should recognize that there bounce to be unknown risks that are not anticipatable. **The 3rd LOD has a natural limitation called residual risk**. It is the risk that an auditor may fail to detect material issue despite substantive testing and using analytical

reviews. There is no point in complaining about inadequate risk assessment when everybody is already stressed out. Besides, risk assessment will always have some degrees of subjectivity, such as possible misgauge of magnitude despite accurately predicting the risks. There could also be inexplicable events even things being reviewed after-the-fact. So, instead of keep beating the dead horse (and/or having a high staff turnover), senior management should look into realigning the 3LOD to booster efficiency and synergies.

Opportunity to synergize across 3LOD via a robust control and preventive system

The objective of realigning the 3LOD is to enable each LOD to excel at what they do best and encourage collaboration. Silos behaviors and/or mentality of racing for whose team is bigger should be abolished. We envisage significant savings from workflow automation, and there'll be no compromise of controls because the model is designed to have appropriate checks and balances. Without further ado, let see how we can **synergize across 3LOD by shifting the 1st LOD into the center focus**. Following diagram showcases a reshuffled 3LOD and their work relationship:



☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

1st LOD makes hard and fast decisions like an ER doctor

The shift of 1st LOD to the center focus is a strategic move to position them for a proper matchup against the rogues in a dynamic market. **1st LOD needs to be superfast in order to deal with countless non-conformance issues in real-time**. The only way they can handle the task in the briefest possible moment is through control automation. A robust preventive system should be capable of detecting possible abuses and discerning violations. 1st LOD's job is to **monitor a queue of early warning signals detected by the system**. They'll be utilizing their field experience and standard protocol (boundaries for 1st LOD's discretion as set by the risk committee, chaired by CRO of 2nd LOD) to make hard and fast decisions. Like an emergency room doctor in a crowded hospital, they are authorized to terminate treatment (certify death of a transaction), approve to continue processing under conditions, or seek referrals.

Who to inform, who to consult, when to escalate, and how soon an issue should be resolved are customizable parameters of the workflow system. We indeed **recommend a direct line from 1st LOD to the senior management for escalation**, and then a dotted line to inform and/or consult the 2nd LOD for anything a policy may need appropriate interpretation. This is different from a stream of pending cases waiting for the 2nd LOD to approve in a legacy hierarchy. **The 'timely and insightful warning signals' shared with the 2nd LOD are meant to be lessons learnt**, so that 2nd LOD may fine tune the risk appetite and/or update the control programs that best suit the changing market environment. Unless a referral is related to a remediation case that the 2nd LOD is actively pursuing, otherwise 2nd LOD should minimize their direct involvement in day-to-day matters because their skills are better fit for analytic/ remediation works.

2nd LOD designs the overall control system and runs a rehab center

Using the hospital again as an analogy, **2nd LOD** focuses on the patient's health recovery when they are in a rehab or remediation role. They also consider how to salvage the most and/or recover the quickest when bad things did happen. They are allowed more time to care for the patient than the 1st LOD, but they **are expected to be precise with their diagnosis/ risk analysis**. To optimize between efficiency and effectiveness, 1st LOD may suggest program changes based on their field experience as **substantiated** by factual cases accumulated in the integrated system. The communication can also be initiated from the 2nd LOD, to request 1st LOD to submit a risk control self-assessment (**RCSA**). It is a **discovery process to identify better risk warning signals, and prepare for a better standard protocol**. 2nd LOD aren't checkers of 1st LOD, they'll be sharing any control risk concerns with the 3rd LOD if the situation warrants.

2nd LOD also carry the market risk analytic function because they tend to be more well-verse with the macro issues. They'll be exchanging thoughts with senior management regularly on strategies, so that there'll be appropriate balance

between risk controls and the fulfillment of business objectives. They'll be diligently **monitoring the divergence of risks** and dynamic interactions of the market. They'll be constantly thinking about how a control may be by-pass and come up with **effective ways to close any loopholes**. In order to ensure controls are embedded into the design of any algorithmic trade model used by the front office, they'll be advising on circuit-breaker and approving the deployment as appropriate. They are the overall designer and owner of the risk control and preventive system.

From time to time, 2nd LOD may go back to the drawing board to independently decide how to update their programs and policies that **best suit the changing market environment**. Tightening risk controls or relaxing risk appetite, demanding additional scrutiny or granting further empowerments, these are all driven by an **autonomous 2nd LOD**. To help 2nd LOD to best perform in their jobs, **give them the tools** so they may easily aggregate data and conduct insightful risk analytics.

3rd LOD corrects failures and assures efficiency and effectiveness of controls

A robust system would retain complete audit trails, enabling the 3rd LOD to use **EDP audit** to efficiently and adequately review the compliance. It'll also minimize the subjectivity of the 3rd LOD for they can **objectively evaluate** controls' effectiveness by comparing warning signals generated by the control systems versus the amount of the **false positives/ negatives**. 3rd LOD can base on their findings to order the 1st LOD to follow-through, properly executing particular controls, and/or calling the 2nd LOD to tweak the control parameters. The 1st and 2nd LOD should work accordingly on their **corrective/ continuous improvement actions**, or else **face consequences**.

Senior management should inform the 3rd LOD of their strategic actions from time to time. Then 3rd LOD should consider, again the two possible cause of risk management failure: (1) if the organization may lack timely and insightful warning; (2) inability to timely response to warning. **Discuss any inherent and detection risk with the 2nd LOD**. If they are hesitated for not able to grasp hold of the bigger picture about risk, they shouldn't be shy to use their authority to halt business until proper **control assurance**. It's better for the 3rd LOD to trouble the senior management to fix any problems before things getting out of hand to become a reputational risk for the organization.

Senior Management invests in system to address the IBG/ YBG problem

Every organization would have different degrees of 'all of the above' problems – i.e. type (d). That's why senior management should engage an outsider to objectively look into the process and **be considerate of the human aspects**, so there'll be appropriate customization for the 3LOD revitalization project. In turn, they can expect better efficiency and

☏ 617.237.6111 ✉ info@databoiler.com databoiler.com

generate enough savings to invest in tools that will significantly help the 3LOD to strengthen their controls.

The benefits of system automation go beyond the objectivity of decisions and workflow efficiency; it addresses any IBG / YNG concerns – i.e. type (e). **Senior management should acknowledge the existence of IBG / YBG** persons in their organization. There is no way to terminate them all, but instead, management reliefs tedious jobs from people by way of using machines so human resources can concentrate on what they do best. It'll transform a fair amount of IBG / YBG persons into high productive teams. For those who are reluctant to change, **the system would hold them accountable**. Every IBG / YBG decision would be reconcile by the system to determine if there's a pattern to favor short-term over the long-term benefits of the organization.

Lastly but not least, it is the responsibility of senior management to **efficiently deploy sufficient resources** in support of the 3LOD revitalization. Equip them with a robust control and preventive system, so they'll:

- **Stop bugging senior management with internal conflicts**.
- It'll minimize the frequency of step-in for direct oversight of particular risk situations that deems unnecessary.
- There'll be **timely risk treatments handled by staffs closest to the problems**, hence mitigates reputational risks.
- Stop regulatory fines, win the race over rogues, and enhance comfort level to provide compliance attestation.

*** END ***