The Three Lines Model

Table of contents

Executive summary

Recently, the 'Three Lines Model' has come under scrutiny and criticism as to whether it remains fit for purpose for financial institutions, against the background of today's business environment and risk landscape. New technologies such as Artificial Intelligence (AI), machine learning (ML) and robotic process automation (RPA) have emerged, and are being deployed in areas such as testing, monitoring, and surveillance. Amongst other influences, these developments present possible opportunities for organizations to adopt a more integrated and effective risk oversight and risk governance model. Many organizations, especially those that are embarking on digital transformations, or ones who are embracing the adoption of new technology and analytics, have developed the means to automate areas of risk oversight. Technology is also paving the way for controls, control-testing and risk-monitoring to evolve so as to be embedded within a new modern infrastructure augmented by data, analytics and automation. Consequently, the Three Lines Model also must evolve from its traditional interpretation and application in order to take into account changing business models and enable a more dynamic risk governance, which ultimately will reinforce the safeguarding of long-term commitments made to customers, while assuring full compliance with the increasing rigor and number of regulatory requirements.

In the future, it is very likely we will see a fundamentally more agile and dynamic approach to the Three Lines Model, whereby technology-enabled risk controls are largely "built-in by design".

The demanding risk environment has also seen the organization's risk profiles grow increasingly more complex and more interconnected alongside risks that are becoming fast moving. As a consequence, the remit of risk management has expanded and additional risk and assurance functions have been established without taking a holistic view of risk governance: indeed, depending on where risk expertise lies within an organization, these new functions could lie within 1st or 2nd lines. This has led to collaboration challenges across functions, and a blurring of roles and responsibilities across the three lines.

Notwithstanding these observations, the Three Lines Model has firmly become an integral part of most organizations across the Financial Services Industry (FSI). And, despite the model not being deployed as a result of regulatory requirements, supervisory authorities have come to both embrace as well as rely upon it. Its relative simplicity allows it to be applied across different organizations and business models; it lends greater structure to the often-challenging risk-control trade-off discussions; and it does an adequate job in bolstering shareholder value-creation, while fostering greater managerial accountability and risk ownership. Given the underpinnings evidenced by such merits, the Three Lines Model continues to be viewed as an important risk-governance model.

The purpose of this paper is to present the collective views of the CRO Forum members (obtained by evaluating survey responses) on the **S**trengths, **W**eaknesses, **O**pportunities and **T**hreats of the Three Lines Model. The paper further synthesizes some key design principles for the implementation of a successful Three Lines Model. The paper also highlights the benefits of an evolution toward an Enterprise Risk Management (ERM)/(IRM) Integrated Risk Management Framework, and provides insights as to how to best adapt and position the risk-controls lens to be better prepared for emerging, innovative business models and a rather constantly evolving risk landscape.

2. Introduction

Over the last decade, risk management, as a discipline and a function within the Financial Services Industry, has progressed from stand-alone risk management practices toward fully embedded risk management frameworks. Within these frameworks, the Three Lines Model[1] is a well-established organizational model leveraged to describe the division of responsibilities between business and the control functions. This paper evaluates the model and provides an overview of its strengths, weaknesses, opportunities and threats (SWOT), and the changing nature and evolution of the model.

The focus of this paper is on governance aspects, while tangentially addressing related elements of the risk management framework, such as risk culture and other elements that are closely related.

As Chief Risk Officers continuously reflect upon the ever-changing business environment and its challenges, the CRO Forum has opted to evaluate the Three Lines Model and its use within the insurance sector. The underlying objectives of the review included information-sharing, leveraging potential best practices, addressing possible gaps and/or shortcomings of the model and of the application of the model in practice.

It is important to stress that an effective risk management and internal controls framework ultimately helps bolster the risk culture, including reinforcing a strong tone at the top. An effectively designed Three Lines Model, ultimately, would help to adequately assign accountabilities, while enforcing sound consequence management when necessary.

The evaluation started with a survey to explore the validity of the assumption that the Three Lines Model is the prominent model for risk management systems in the insurance industry. This assumption was confirmed through the survey, conducted by the CRO Forum, among its members.

[1] Previously referred to as three lines of defense model: https://global.theiia.org/about/about-internal-auditing/Public%20Documents/Three-Lines-Model-Updated.pdf.

While the Three Lines Model is not a regulatory or supervisory framework per se, supervisory authorities have come to embrace the model.[2] Furthermore, it is seen as more business friendly and, as a result, the Three Lines Model has become a generally accepted model across many industries, including financial services.

The Three Lines Model represents a principle-based approach targeting effective risk management governance by defining roles and responsibilities within an organization and the relationships among them. The definitions presented in this document are based on "The IIA's Three Lines Model" publication by the Institute of Internal Auditors (IIA). The IIA has recently updated and renamed the model from 'Three Lines of Defense' to the "Three Lines Model" based on an acknowledgment that risk-based decision-making is as much about seizing opportunities as it is about defensive moves, and recognition that the need for collaboration and alignment between the different parts of the model so as to create pragmatic and effective structures should be further emphasized, taking into account the objectives and circumstances of companies.

The Three Lines Model is structured as follows:

The **governing body** is ultimately accountable for governance and setting up appropriate structures and processes to enable the achievement of the goals of the organization. It, therefore, delegates responsibility and competencies to **the management** (among others), in order to set up an adequate risk management system. Furthermore, the governing body establishes an internal audit function and supervises the activities of the management (in particular, risk management and internal control systems), which takes decisions and allocates resources to achieve business and risk management goals. It may form committees to allow for specialized oversight of specific areas. In large and complex organizations, the management may establish functional departments and hierarchies to meet the required specialization.

The management is responsible for the deployment of resources in the **1st line** and the **2nd line** and regularly reports to the governing body on risks and results. 1st line roles typically provide products and services to internal and external clients, but they are also managing the risks inherent in their activities (front-office and back-office activities). 1st line roles may include support functions.[3] The 2nd line conducts analyses, prepares guidelines and advises the management, as well as the 1st line roles, with respect to risk management issues. Their goal is the development, implementation and continuous improvement of the risk management framework and methodology across all levels of the organization. Experts in either the 1st or the 2nd line may also pursue specialized objectives of risk management, e.g. compliance with laws or regulations or information security. Consequently, both lines take responsibility regarding risk management for the organization. 1st and 2nd lines may be intertwined or separated.

Internal audit forms the **3rd line**, which must be independent of the 1st and the 2nd lines of the organization. It reports to and is overseen by the governing body, and ensures an independent audit of the activities and results of the management of the other two lines. The 3rd line therefore does not take decisions in areas that are in the remit of the management, but rather maintains regular communication and collaboration with the other lines in order to promote improvements. In order to achieve its tasks, unrestricted access to relevant persons and information must be guaranteed. Given its position within the organization, as internal audit is removed from defining frameworks and operational activities, it has a unique position of being able to provide a holistic level of assurance underpinned by robust audit procedures that assess both design and operating effectives of internal controls.

[2] For instance by the IAIS in the recent update of the Insurance Core Principles and COM-Frame, adopted in November 2019, https://www.iaisweb.org/page/supervisory-material/insurance-core-principles-and-comframe//file/91154/iais-icps-and-comframe-adopted-in--november-2019

[3] Such as a Legal, Regulatory, Finance, Tax or HR function. Support functions may be considered either 1st 2nd line functions.

3. A SWOT analysis of the Three Lines Model

Evaluating the Three Lines Model, with the ultimate goal of proposing recommendations as to the extent and areas of possible modification (so as to evolve such a Model), invariably requires an objective assessment of its current status.

This evaluation was carried by way of a SWOT analysis (**S**trengths, **W**eaknesses, **O**pportunities and **T**hreats) of the Three Lines Model, based upon responses to a dedicated survey collected from the Working Group participants.

The survey was structured along six dimensions, by way of the following main topics:

1. Application of the Three Lines Model and the positioning of the regulatory required Control Functions;
2. The model's fitness for purpose, strengths, weaknesses, flexibility and its linkages with risk culture and the risk and business strategies;
3. Clarity and balance of the roles and responsibilities across the three lines;
4. 1st line risk and control ownership;
5. Application of the Three Lines Model in less stringently regulated business models such as Fin- and Insure-Techs;
6. Best practices regarding the application of the Three Lines Model (both inside and outside the insurance industry).

Respondents provided the respective view on above-noted topics, providing examples and engaging in best-practices sharing to promote improvement ideas and suggestions. This was done against the context that each/all have unique and/or different corporate governance structures, as well potentially minor to major different regulatory requirements.

Summarized on the next page are the key outputs from the survey responses, highlighting the Three Lines Model attributes along a SWOT approach.

Strengths

- **The Model is widely used and understood** by all parties. It is generally considered to appropriately depict the demands and requirements applicable to the Financial Services industry
- **It relies on a clear definition of Roles and Responsibilities** of all stakeholders in risk governance and internal controls
- **The Model enables evaluation, assessment, clear communication, escalation channels and effective risk reporting**. It creates a focus on the **importance of effective risk management** (including risk culture) and the need for a robust internal control framework
- It stresses **Managerial accountability** by way of enforcing holistic risks-controls ownership, since all the 3 lines must cooperate to achieve end-to-end business results in a balanced way. Thus, it helps structure **targeted discussions** (risks-controls tradeoffs) and facilitates a better understanding of **independence & objectivity** and how they support better controls-assurance activities

Weaknesses

- The Three Lines Model might appear **rigid** in some situations, when focusing on defense and compliance with internal control system and regulation
- The Three Lines Model envisages a clear distinction and independence between 3 Lines, which means that risks-controls assessments are executed ex-post in most cases, making the Model appear **reactive** at some levels and **potentially preventing the early involvement of control functions** in the decision-making process
- The Three Lines Model works well in huge and complex institutions, while may become difficult and costly to implement, deploy and maintain in smaller organizations. However, the Three Lines Model does not recognize proportionality and is **challenging to be customized**
- Involving more than one control function, the Three Lines Model may **create overlaps** in terms of scope or perimeter of activities between Risk Management, Compliance and Actuarial Function, Business Continuity Management and IT functions, that generate the lack of ownership and clear responsibility for risks, controls or activities.

Threats

- As the model is widely used and accepted, it is subject only to limited challenges: there is a **risk of complacency**
- Real-life implementations sometimes lead to situations where boundaries between the lines are not always so clear cut as the Model would imply. The **emergence of a "1.5" line**, whose roles and responsibilities are not always clearly formalized, **might add complexity** to the Model. Maintaining the 1st line's ownership and accountability for both risks and controls can thus be challenging
- The ever **changing internal and external business environment** is also perceived as a threat to the model, it being perceived by respondents as more adapted to stable environments. The Three Lines Model may not be situationally relevant so as to support a flexible and adaptable risk-rewards tradeoff decision-making framework

Opportunities

- By **linking control objectives with business performance**, the Three Lines Model could gain more flexibility and make a step up versus being a proper business support mechanism rather than a primary compliance exercise
- **Earlier involvement of 2nd line** i.e., already in the design phase of any business activity, would enable a more robust risk evaluation, leave space for a more forward-looking risk perspective and would save time and energy in the validation and compliance assessment process for the 1st and 2nd lines before a product and/or a process is launched
- The Three Lines Model could be further adapted to enable **stronger interaction between the 1st and the 2nd lines**, by creating opportunities for the 2nd line to know and understand the business better (i.e., through internal rotation and ad hoc training), and by embedding risk management performance objectives to the variable compensation schemes of the 1st line
- The Three Lines Model could **be calibrated to better "fit" regulated versus non-regulated entities**, in order to reflect organizational complexity and size and evaluate if certain control functions are required

The use of the Three Lines Model is widespread across all participants within the financial services industry, regardless of differences in specific regulatory environments. As a result, it is a well-known organizational Model, familiar to all stakeholders such as governance bodies and supervisory authorities, as well as market participants such as rating agencies, analysts and investors.

Strengths

One of the main strengths of the Three Lines Model resides in its clear definition of roles and responsibilities across the business in the management of risks. It elaborates well the role of the Board, Top Management, Operational Management, and Control Functions (Risk Management, Compliance, Actuarial, and Internal Audit), which are considered as necessary components of an effective system of risk management and internal controls. These Control Functions, as introduced by the Insurance Core Principles of the IAIS[4], are named "Key Functions" within the Solvency II Regime. All respondents have implemented these functions, with some variations. *Note: some of these functions may be combined, e.g. Risk Management and Compliance, or Risk Management and Actuarial.*

Due to its pervasiveness, and its clarity in establishing roles and responsibilities, the Three Lines Model facilitates evaluation, assessment, communication and reporting on risks and internal controls, regardless of organizational complexity. It supports clear discussions among stakeholders on risk and control tradeoffs, in a way that enables governance bodies to fulfill their role and underlying objectives, as an important part of the internal control system. Additionally, it is a primary enabler of ensuring managerial accountability.

One of the main strengths of the Three Lines Model resides in its clear definition of roles and responsibilities across the business in the management of risks. It facilitates evaluation, assessment, communication and reporting on risks and internal controls.

Weaknesses

Despite its merits, most of the respondents shared a common view on the weaknesses of the Three Lines Model, asserting that the Model (in its current set up) appears unduly rigid, mostly reactive and strongly focused on defense and compliance with internal control system requirements and regulations.

The linkage between Business Strategy / Ambitions and Risk Management Objectives, to be ideally interlinked and framed by the Risk Appetite, sometimes can be seen as a compliance tick-the-box exercise which is produced in isolation rather than as a result of the two lines closely working in tandem.

The Model (in its current set up) appears unduly rigid, mostly reactive and strongly focused on defense and compliance with internal control system requirements and regulations.

[4] https://www.iaisweb.org/page/supervisory-material/insurance-core-principles-and-comframe//file/91154/iais-icps-and-comframe--adopted-in-november-2019

Threats

Along with weaknesses, respondents also identified threats to the Model. Being a well-established model, the Three Lines Model carries, as a flipside, a potential risk of complacency: challenges to the Model itself, and its adequacy, are limited. Yet, actual implementation of the Model may lead to practical difficulties, which can be considered as "threats" to its initial design.

For example, respondents recognize that the actual attribution of responsibilities and accountabilities between the 1st and 2nd lines can be less clear at times, especially as "oversight" activities may sometimes be purposefully or inadvertently seen as "approval" activities. Maintaining the 1st line's ownership and accountability for both risks and controls can thus be challenging. It is especially true in an environment where 2nd and 3rd lines are considered by supervisors to be gate keepers, and business line owners may lose sight of their inherent risks as the accumulation of rules blurs the vision.

Maintaining the 1st line's ownership and accountability for both risks and controls can thus be challenging.

The emergence of a "1.5" line , while aimed at assisting the 1st line for specific activities, adds complexity to the Model and, simultaneously, seems to indicate that the boundaries among the three lines may not always be as distinct as the titles '1st, 2nd, 3rd would imply. This is especially noticeable when the roles of such 1.5 lines are often not formally defined. Examples of these 1.5 line functions in respondent firms include the Independent Valuation Units, Protection & Resilience Functions (like Business Continuity Management, etc.), as well as Information Security (IT Security) or Cyber Defense Units. Such 1.5 lines may potentially create overlaps in roles and responsibilities and, thus, inadvertently and adversely impact the assignment of accountabilities.

Consequently, striking a balance between maintaining independent control and audit functions, and avoiding isolation of said functions, can be rather challenging at times.

The ever changing internal and external business environment is also perceived as a threat to the Model, since striving to keep up with these changes can be a costly process. Indeed, the Model is perceived by respondents as more amenable to stable environments. Depending upon deployment strategies, the Model may be quite rules-driven and is seen as being not agile enough to take into account the needs of more innovative business models, taking into consideration business scale, possible value-chain fractionalization and the consequences thereof, etc. Thus, the Three Lines Model may not be situationally relevant enough to support a pragmatic and realistic risk-rewards tradeoff decision-set. Its administration may be seen as quite bureaucratic and, thus, may slow down the business decision-making process.

The Three Lines Model may not be situationally relevant enough to support a pragmatic and realistic risk-rewards tradeoff decision-set.

In sum, it is evident from the survey that granting more flexibility to the Three Lines Model and proper deployment would naturally drive further integration and cross collaboration / objectives alignment between the 1st and the 2nd lines, enabling the 1st line to be more risk aware, while providing knowledge and means to the 2nd line to be a valued and appreciated business support function, all the while supporting a forward-looking perspective.

Opportunities

The following concrete actions to drive this transformation were proposed by the respondents so as to address weaknesses of the Model and support the transformation of Threats into capturing Opportunities instead:

- Adequately identify and elaborate a system of governance: enable a calibration of the Three Lines Model to better "fit" regulated versus non-regulated entities; consider proportionality to reflect organizational complexity and size; evaluate if certain Control Functions are required (i.e., such as Actuarial for non-insurance and non-regulated enterprises); scale control procedures to better fit technologically-geared entities;
- Promote a more formalized establishment of risk-and-control "intermediaries" (whose functions have been coined as the 1.5 lines) and, among other activities, define clear objectives to be undertaken by them, such as "translating" controls requirements into business / laymen terms;
- Install explicit compensation linkages to the number of closed and/or open governance, risk and control deficiencies (for the business: demonstrate that with empowerment, comes accountability; for the controls-function: create clear metrics and levers to demonstrate the cause-effect of controls failures and to assist the business in benefitting from lessons learned);
- Name control-champions who sit directly in the 1st line functions: a resource for day-to-day business enablement without the appearance of potentially divisive "controlling" or monitoring activities;
- Define and deliver targeted as well as broader trainings, or other similar measures, designed to elevate risk-awareness and support a stronger risk culture; including the upskilling of controls-functions to bridge the "language gap" and not shield themselves behind regulatory levers to exert "power".

Indeed, the potential choices available with respect to the Opportunities of the Three Lines Model are various, with only some of the key ones mentioned above. Not only are these "opportunities" aimed at refining and adapting the Model to support better risk-and-control efforts, but they also aspire to clarify specifically to business owners and Regulators that the Model itself must remain flexible to adapt to an ever-changing business environment.

Further, the design principles highlighted above are geared toward an empowerment of business owners (1st line) so as to support their taking control at reducing if not outright eliminating the risks that may have an adverse impact on the achievement of business goals.

4. The changing nature of the roles & responsibilities of the Three Lines

We mentioned earlier that there can be a blurring of roles and responsibilities among and between the various lines.

Lack of clarity between the 1st and 2nd Lines often comes from capacities and capabilities constraints which have created an imbalance over time. Business and Line owners are consistently mandated to be more efficient; to increase productivity; to focus more on customers and business processes; to let the technical experts take over the less "client-facing" activities and to focus more on their core, which is often seen as business creation and growth, whether it be through increased sales or enhancing products innovation or increasing customer satisfaction, etc. Indeed, this focus is correct: These are their core strengths.

Nevertheless, what has transpired over the last decade with the Three Lines Model, pervasively making its way through the organization, is that technical expertise alone cannot compensate for client-facing expertise and vice versa. "Safeguarding-procedures" manifested within policies like anti-fraud, anti-money-laundering, anti-corruption, data privacy, IT Security, etc. are activities very closely linked to the business. The controls response to risk vectors like Fraud, Cyber, Corruption, etc., while perhaps seen as "technical", in so far as they must comply with sometimes very specific and prescriptive rules and regulations, must be embedded into the business processes themselves. And, as Business and Line Owners have come to "delegate" these responsibilities to their 2nd line of defense controls counterparts, the blurring of these lines becomes an inevitable eventuality.

Interestingly, the current movement to rebalance the ownership between the 1st Line and Controls functions is also being driven somewhat by regulations. Executive Accountability Regimes or some flavor thereof by way of "consequence" management levers requested by regulators, are instruments to reinforce business ownership of business risks. The risk vectors that are part of business operations are seen as ones the business must own and be held accountable for. Control functions have the lead role in defining frameworks and policies, and in monitoring that such frameworks are designed and operated effectively, while the actual controlling of these risks and a consistent living of the risk strategy is expected as the Line function deploys and executes its business strategy. Fundamentally, one must recognize that these tenets have been the guiding principles of the Three Lines Model since the beginning.

The shifting of regulatory focus back-to-basics is indeed a recognition that there is presently a need for rebalance between 1st and 2nd Line accountabilities.

Among other factors, the above dilemmas have, primarily for efficiency reasons, led to a rise in 1st line dedicated expert control monitoring functions/ departments, such as e.g. Anti-Fraud Officers, Information Security Officers or Business Continuity Managers. Tasks performed by these functions are typically a 1st line responsibility as they relate to risks in primary business processes and to business objectives, with the countervailing power in the 2nd line (for the aforementioned examples, this is usually Operational Risk Management). Some companies refer to these organizational choices within the 1st line as the 1.5 line functions. Functionally, these functions may design some controls and undertake 1st line controls-assurance activities when called upon. We would encourage such dedicated functions (as this needs specialist expertise) to reside within the 1st line rather than have the appearance that 2nd line occupies this role.

That said, we also note that in several jurisdictions, regulators press for more 'purity' within the Three Lines Model: to such an extent that such 'purity' may actually decrease effectiveness of the model. One area of concern is regulators encouraging strict operational independence between 1st line and 2nd line functions. Indeed, such insistence may actually hamper sometimes robust and collaborative current relationships that exist amongst the stakeholders as they aim to benefit from and leverage upon each other's expertise. Another area of concern is what some would deem as regulatory overweighting of form over substance: e.g. by stressing the importance of detailed written documentation and evidencing assurance / challenging activities. As the insistence on documentation is often the prevailing reasons cited within regulatory reports, this may distract from the value adding work of the 2nd line so as to 'push' them sometimes more on the form, rather than the content. Indeed, this is aggravating to the already existing perception of 2nd and 3rd lines being bureaucratic and/or dogmatic, formalistic and/or non-business enabling.

Lack of clarity also exists within the 2nd line. What is happening quite often, is that as the 2nd line functions co-exist and are sometimes (read as often) asked to ensure gaps do not exist. As there are some grey areas between 2nd line functions (e.g. Risk Management, Actuarial and Compliance), more than one 2nd line function may take up the challenge to close the gap. If these activities are not aligned well, it could lead to overlap. Overlaps and/or redundancies emerge by way of scope creep as well: in the spirit of "better safe than sorry" 2nd line functions may take on more than they should, hampering risks and controls ownership within the 1st line. In addition, we also have seen signs that some regulators are requesting 2nd line functions to provide a formal opinion on the work done by another 2nd line function (e.g. an Actuarial opinion on the work done by Risk). This should be avoided as it inadvertently challenges 2nd line work, both from a content as well as independence perspective. At a minimum, this may be confusing in addition to adding little marginal value.

Finally, there seems to be some lack of clarity between the 2nd and the 3rd line functions, especially when it comes to (independent) control monitoring in the area of operational risk. As both lines tend to test the effectiveness of controls, this might be perceived as double-work by the 1st line. In addition, for financial reporting processes, the external auditor also performs control testing.

What we believe to be the root cause of this blurring is that often, organizations adapt roles and responsibilities and assign them to functions with subject matter expertise by way of linkage to individuals, rather than by organizational design: a rational and conscious as well as structured approach in terms of defining where these competences ought to sit must be the starting point. Further, degrees of independence and objectivity must be taken into account.

In several jurisdictions, regulators press for more 'purity' within the Three Lines model: to such an extent that such 'purity' may actually decrease effectiveness of the model.

5. The future of the Three Lines Model

The Three Lines Model is usually deployed to ensure a company's risk management and internal control systems are operating effectively. The future of the Three Lines Model is determined by the structured approach discussed in the previous chapter, as well as the interdependency between the Three Lines Model and an Enterprise Risk Management (ERM) framework, against the background of emerging FinTech/Insurtech partnerships, investments or holdings.

An ERM framework (sometimes referred to as IRM) recognizes that a holistic approach needs to be taken into account, in order to understand and coordinate the responsibilities of individual actors within an end-to-end organizational and process landscape. ERM aims to ensure that all three lines work together to reduce unwanted risks and, in particular, the ERM framework emphasizes that all lines have a consistent and similar methodology/ view and, in conventional means, this has been coined as having a holistic risk typology when categorizing risks and evaluating controls. ERM is not an alternative to the Three Lines Model. Rather, it is an evolution of the framework, in so far as it aims to enhance controls optimization, while reducing the potential of silo thinking and uncoordinated actions by clearly articulating the roles of each of the three lines.

To achieve these holistic and coordinated views, the ERM framework must address certain areas that call for improvement in the organizational Three Lines Model, regardless of underlying business models, established or otherwise:

- Survey respondents have observed that Business owners are asserting that they are experiencing controls-assurance fatigue. Various control functions seem to ask for similar activities, but they sometimes do so in an uncoordinated way. Aggravating this even more, is that each oversight function may have its own way of assessing risks and, some seem to require very specific controls-sets, without considering the existence of policies and procedures that may already address such risks. Thus, a key building block to achieving harmonization and optimization is the definition and deployment of a complete, consistent and comparable risk taxonomy. Regardless if this is quantitatively or qualitatively (or both) based, using a 3x3, 4x4

ERM is not an alternative to the Three Lines Model. Rather, it is an evolution of the framework.

or 5x5 matrix capturing frequency and severity, Business and Line owners want risks-definitions and assessments to be similar, regardless if it's Compliance, Risk, Actuarial or Internal Audit functions undertaking the risks-and-controls evaluation, together with the Business.

Without question, a common starting point would help the business focus its controls-design and operations efforts, reducing the potential for poor risks-prioritization or ineffective controls-operationalization.

- Fundamental to a consistent taxonomy, is a risk assessment approach that considers top-down objectives against the context of bottom-up realities. Resources are limited: an assertion that the target risk appetite of any risk vector is ultimately zero, does not take into account the economic tradeoffs linked to controls-design and deployment. For example, non-compliance toward rules and regulations must indeed aim for zero infractions and be received with zero tolerance. But, purposeful manipulations of procedures are an inevitability. Zero frequency by way of insistence for a "perfect" control design is often extraordinarily expensive, if not sometimes impractical. Rather, some "risk-acceptance" must be tolerated and, what is more important when such infractions should take place, is the installation of adequate response actions that would "kick-in" once an infraction occurs. For example, if money laundering or corruption activities have been detected, response strategies such as forensic reviews, notification to authorities, and communication strategies to both internal and external stakeholders, as well as the seriousness with which investigations are pursued and sanctions installed, are part of end-to-end controls procedures. Control procedures must continue after a control failure. In an ERM framework all areas that have a response role (to further reduce residual risk) within the entire enterprise (e.g. regulatory affairs, corporate communications, investor relations, investigations, HR management, etc.) are taken into account, not just the functions/procedures/activities wherein the failures took place.

Rather, some "risk-acceptance" must be tolerated and, what is more important when such infractions should take place, is the installation of adequate response actions that would "kick-in" once an infraction occurs.

- Already mentioned is the utilization of incentives alignment so as to reduce the risk of Agency Theory. Effective means of firmly anchoring risk ownership and accountability in the 1st line is coming more and more to the forefront of internal control systems discussions. Aside from accountability regimes linking compensation and consequence management to controls-failures, business risk-ownership must also be better enabled. One way is to encourage a positive risk culture and elevate thereof by way of promoting greater awareness. This includes the deployment of an integrated approach towards business and risk strategy evaluation, whether through a limit system that requires periodic adjustments against the context of a dynamic macro-economic environment; or the use of a segment/sector consistent leeway system; or identifying and supporting the pursuit of less risky opportunities as business strategy alternatives.

Aside from accountability regimes linking compensation and consequence management to controls-failures, business risk-ownership must also be better enabled. One way is to encourage a positive risk culture and elevate thereof by way of promoting greater awareness.

Another is to empower safeguarding functions by ensuring that they are at the table when significant business decisions are undertaken: as business partners and advisers rather than regulatorily-extended enforcement levers. This requires upskilling control functions in business acumen and real-world knowledge, encouraging them to look at opportunities and consider options/solutions beyond their immediate span of responsibility. This empowerment may take a range of forms, for example:

— The incentivization of the safeguarding functions to advise the majority of the time, while affording them the capability to escalate and, worst case, "veto" when absolutely critical. In other words, insist that safeguarding functions evaluate risks against the context of reducing them such that this would enable resources to be better deployed to pursue alternative opportunities.

- Requiring the safeguarding functions to formulate their own views, in conjunction with an explicit and formal escalation process to be utilized if there is a divergence of views.
- Requiring significant business decisions to have a formal 2nd Line view included within the formal decision approval process and documentation thereof. This approach maintains 1st line accountability for decision making, while increasing transparency by way of the involvement of the safeguarding functions, all the while ensuring that business owners proactively engage safeguarding functions earlier on in the process so as to procreate a holistic assessment of risk-reward tradeoffs.

- An important enabler of an effective ERM framework is the dedicated decision by 1st, 2nd and sometimes even 3rd Line owners to use a common tool. Consistent risk assessments, efficient and effective controls evaluation, documentation and evidence retention required therein, etc. should help ERM architects and overseers to ascertain / evaluate where and when control failures manifested, in order to support greater transparency and ensure accountability.

Furthermore, the use of a shared tool/ applications-platform also enables the "detection" of possible systemic/structural risks that may not be overtly obvious or, worse yet, lie dormant because the "dots" had not been connected as to common factors driving "root-causes".

The Working Group also considered the dilemma the Insurance Industry presently faces with the rise of Fintechs and Insurtechs. All firms reported some form of "participation" in such business models, either by way of strategic ventures, direct investments, or through co-creation partnerships. Each approach is positioned to garner the benefits of Fintech/Insurtech presence and expertise in more enhanced and dynamic delivery capabilities (both in products and distribution).

Though the Three Lines Model is still relatively "flexible", its ability to respond quickly to rapid changes in an agile manner is somewhat challenged.

While some Fintech/Insurtech companies may be regulated enterprises, many are not and, their agility in responding to consumer preferences and lifestyle stages cannot be ignored. No matter the "magnitude" of such participation, incumbent firms all report that governance and oversight of these "entities" are indeed challenging, testing and sometimes straining the limits of the Three Lines Model. While some would argue that non-regulated entities should be "left alone" to foster innovation and promote agility; this may be appropriate in the pure "start-up" phase; however, as is their "nature", Fintechs and Insurtechs, have the propensity to grow at an extremely fast pace with what may be seen as "uncontrollable" momentum. Though the Three Lines Model is still relatively "flexible", its ability to respond quickly to rapid changes in an agile manner is somewhat challenged.

In order to effectively support Fintechs and Insurtechs, architects of the organizational Three Lines Model may want to make a distinction between the initial start-up phase and the scale-up phase. In the former phase, involvement is needed to understand and assess the strategic rationale / business case. During the latter, control-by-design becomes more and more relevant. This is especially noticeable in areas such as product manufacturing and distribution. Insurance product development cycles are typically lengthy and extensive. Distribution efforts linked to many insurance products are also typically "onerous", as some can only be sold after extensive training and sometimes certification. Solutions considered to shorten such lengthy cycles come by way of using Artificial Intelligence (AI) or Machine Learning to leap-frog product development and distribution management cycles. Solutions such as these are indeed innovative but bring about their own challenges, such as Data Ethics and Data Privacy, Sales Compliance, Customer Suitability and the like.

Solutions such as these are indeed innovative but bring about their own challenges, such as Data Ethics and Data Privacy, Sales Compliance, Customer Suitability and the like.

If the industry shifts more towards using AI and Machine Learning to leap-frog traditional product development and distribution challenges, this would effectively require that compliance and risk management objectives must be embedded into the "machine" and procedures themselves. The phrase "compliance-by-design" has entered the vernacular to entail that a system or process is designed with compliance objectives/controls built into the underlying processes. As well, "risk management-by-design" is also particularly necessary for items such as AI and Machine Learning, so as to ensure that appropriate risk management procedures adapt to underlying procedural changes, while enabling the overall process to remain nimble. Controls must be installed as part of product design procedures, for example pricing/reserving rules, compliance with consumer protection rules and regulations and accumulation mitigation controls. Meanwhile, monitoring and reporting activities may be "delegated" to "machines", with periodic confirmation through sample testing, by either the 2nd or 3rd lines.

The risk lens would then need to be (re)calibrated to focus on risks related to the definition of parameters and assumptions with regard to probable risks and the embedding of automated controls. Close attention would need to be given to programming and change management procedures within an applications-based set of processes. Compliance and Risk functions must indeed be more advisory in their approaches and must influence business owners before deployment, as ex-ante controls increase in importance. In addition, risks such as those relating to data ethics, data integrity, business process delivery/availability and data privacy become more prominent.

Compliance and Risk functions must indeed be more advisory in their approaches and must influence business owners before deployment, as ex-ante controls increase in importance.

Furthermore, detective controls take on a new dynamic, as they must be virtually "real-time" in order to help reduce major mishaps, in terms of either frequency or severity of occurrences. Again, in order to operationalize this, it is important that these detective controls are built into the system in the design phase, rather than overlaid once the system has already been placed into the production environment. For this to be optimal, resources and costs associated with the installation of these controls (whether preventative or detective) must be included into design and build plans and timelines.

Hence, a "different" sort of principle of proportionality must be applied; its focus should shift from company size, geography, etc. to the "reach" of the internet-of-things. Consequently, the Three Lines Model must be further evolved to take into account these innovative business models – as a means of reinforcing the safeguarding of long-term commitments made to customers while complying with regulatory requirements – without killing innovation.

The degree of compliance and risk management-by-design required is heavily reliant upon the extent and depth of technology utilization and how such utilization may aggravate the compliance and risk-profile of the company (e.g. the level of product customization and the extent of customer interaction and servicing).

Suggested approaches could include:

- Performing risk identification focused on key design principles that enable customer-centricity while including, as seamlessly as possible, control objectives enablement: e.g. an identity check may address anti-corruption, anti-money laundering and anti-fraud risks as well as anti-sanctions risks without asking the customer multiple questions.
- Having a clear segmentation approach before the product design stages so as to reduce the risk of mis-selling or violating sales conduct.
- Having "commissions" based upon a modular product approach so that benefits accretion is transparent while being consumer friendly.
- Utilizing publicly available data whenever possible to reduce data privacy risks (e.g. publicly available driving records, etc.).
- Regularly reviewing and testing data enhancements to AI or Machine leaning algorithms, to assure adequate balance between compliance objectives without reducing risk-management aims.

This demonstrates that Control Functions must be much more business aware. They must understand efforts to deploy control procedures before launch. A clear decision to prioritize must-have control objectives will be required. Furthermore, an end-to-end procedures view is required to "anticipate" risks, with realistic challenges to address those risks against the context of real-world constraints such as limited resources.

Against the above background, firms should indeed be aware of, and responsive to, the different ways in which regulation and supervision may affect their businesses. Indeed, they must build such assessment capabilities and objectives into their strategic planning and risk mitigation activities.

This needs to be a proactive process, led by the firm itself, thinking in advance about how it can address and mitigate risks unique to Fintech and Insurtech business models. A purely reactive stance to comply with regulatory and supervisory initiatives will not be successful, as regulators aim to anticipate risks before they emerge (e.g. data ethics).

Regulators and supervisors are focusing on how Fintech and Insurtech affect the core risk governance competencies related to identifying, managing, measuring and controlling risks across the Three Lines Model. They will likely question if firms have the appropriate resources (e.g. technology), skills and expertise to ensure adequate risk-mitigation efforts so as to ensure that consumer protection measures exist and are executed in an effective, efficient and transparent manner. Depending upon the business activities and Fintech applications adopted by a firm, this is likely to cover at least the development of new products and services, outsourcing, the use of artificial intelligence and the automation of both front and back office tasks, technology risk, cyber security, operational resilience, AML and conduct risk.

An evolution of the traditional Three Lines Model is clearly in sight, as it is pushed to respond to the various developments taking place across the industry. This is amplified by new entrants who are strongly innovation-focused and have deep technology-enabled resources. Thus, participants from this Working Group are taking the position that the success of an organization's risk management system, in adapting to this new environment, will be dependent upon the organization's ability to apply a modified principle of proportionality as well as to move toward greater integration of risk management frameworks into the design and build of business procedures.

6. Conclusion

Over the last few decades, the Three Lines Model has firmly become an integral part of most organizations across the Financial Services Industry. In addition, despite the Model not directly being deployed as a result of regulatory requirements, supervisory authorities have come to both embrace as well as rely upon it. That the CRO Forum has posed the question as to whether or not the Three Lines Model should be revisited, and if necessary revised, indicates that perhaps the Model may no longer be sustainable, in particular given the speed and magnitude of change sweeping across the Insurance and Financial Services sectors.

Thus, our positions reflected in this paper (based on 22 CRO Forum member responses) not only consider the **S**trengths, **W**eaknesses, **O**pportunities and **T**hreats of the Three Lines Model, but further synthesize some key design principles for the implementation of a successful Three Lines Model. We also highlight the merits of the progressive implementation of the Enterprise Risk Management/Integrated Risk Management framework and provide some considerations as to how to best adapt and position the risk-controls lens to be better prepared for emerging, innovative business models.

In addition, despite the Model not directly being deployed as a result of regulatory requirements, supervisory authorities have come to both embrace as well as rely upon it.

The **SWOT** analysis reveals, on the one hand, that the main strengths of the Three Lines Model include: its relative simplicity, which allows it to be generally applicable across different organizations; the fact that it lends greater structure to the often challenging risk-control trade-off discussions; and recognition that it does a decent job in bolstering shareholder value-creation, while fostering some managerial accountability and risk ownership. On the other hand, the Model tends to lend itself to a blurring of roles and responsibilities, in particular with respect to the practical distinction between monitoring, oversight and assurance activities; is sometimes perceived as rigid and reactive; and potentially creates "silo" approaches across and among the three Lines. **T**hreats and **O**pportunities are often a result of (non)adherence to certain design principles, including: synthesizing how control objectives help to address business risk rather than "hide" behind regulatory requirements; ensuring a strong Tone at the Top thrives by a consistent living of business and risk culture objectives; and involving control functions at the appropriate stage of business decisions, with proper incentives alignment for participants from all three Lines. Indeed, vigilant attention to such principles should enable the Model to adequately and flexibly respond to organizational changes, so as to help reduce the threat of reduced Model persistency possibly hindered by unintended complacency.

Furthermore, one of the developments observed by survey respondents is a potential shift of some risk-control ownership from 1st to 2nd line

actors, whereby control performance is effectively outsourced to the 2nd line. This purported blurring of roles and responsibilities has been experienced and reported by many of the responding firms. It's no wonder then, that response strategies like Executive Accountability Regimes across Anglo-Saxon jurisdictions have emerged as a regulatory-driven attempt to rebalance the risk and control ownership by assuring that accountabilities are placed with those who take the risks (with the 1st line), while the 2nd and 3rd line must assure and, to a lesser extent, enforce.

In addition, the blurring of responsibilities has also led to the emergence of what is known as dedicated expert control monitoring functions within the 1st line, which may in fact be filling a "gap" in response to possible rigid interpretations of the Three Lines Model.

In light of the above, CRO Forum Working Group participants report that many already deploy a somewhat progressed or "enhanced" Three Lines Model, which can be interpreted as a natural step in the evolution of the model. The "enhanced" Three Lines Model envisages a broader involvement of the Risk Management function, expanding from recurrent control activities, usually managed ex-post, to supporting and challenging 1st line initiatives already in the design and/or preparation phase (e.g., M&A support, capital planning & allocation, risk appetite etc.) This approach allows a consistent, holistic and end-to-end approach, insisting upon collaboration across all three lines and between all Control Functions. Despite such maturity, survey results still highlight some remaining challenges, including assurance fatigue by the 1st line.

Despite such maturity, survey results still highlight some remaining challenges, including assurance fatigue by the 1st Line.

Integrated Risk Management needs to ensure that all three lines work together to reduce unwanted risks; heavily supported by the application of a holistic risk typology when categorizing risks and evaluating controls, which in turn also reduces the potential for silo thinking and uncoordinated actions as a byproduct. This enhancement should clearly recognize that risk management is the responsibility of all stakeholders within the organization and not just the risk management function.

To achieve this holistic and coordinated integration, Enterprise Risk Management/Integrated Risk Management framework must address a wide range of areas:

i) achieving harmonization and optimization through the definition and deployment of a complete, consistent and comparable risk taxonomy;

ii) a risk assessment approach that considers top-down objectives against the context of bottom-up realities while tolerating some "risk-acceptance" and, perhaps more important, the installation of adequate response actions that would "kick-in" once an infraction occurs;

iii) effective means of firmly anchoring risk ownership and accountability in the 1st line, which in turn will enable business risk-ownership and accountability regimes linking compensation and consequence management to governance, risk and control-failures;

iv) consistent risk assessments, efficient and effective controls evaluation, documentation and evidence retention requirements, collectively designed to oversee and spot where and when control failures manifested.

Further, while the Enterprise Risk Management/ Integrated Risk Management frameworks are clear improvements over the traditional Three Lines Model, they still faces challenges when it comes to being more agile, especially when it comes to being fit-for-purpose for newer business models such as those posed by Fin and Insurtechs. These challenges particularly reside in the framework's ability to stay in step with rapidly changing and evolving consumer demands and needs. Most noticeable are areas such as product manufacturing and distribution, where innovations such as the use of AI may significantly strain the traditional customer and delivery value-chains, not to mention the risk-controls landscape typically associated with brick-and-mortar business models.

Consequently, the CRO Forum Working Group is ultimately of the view that, while the Three Lines Model remains relatively fit-for-purpose (even against the backdrop of what the industry has coined as "digital attackers"), continuous adaptation to take into account the principle of proportionality is consistently required.

Consequently, the CRO Forum Working Group is ultimately of the view that, while the Three Lines Model remains relatively fit-for-purpose (even against the backdrop of what the industry has coined as "digital attackers"), continuous adaptation to take into account the principle of proportionality is consistently required. In this context the principle of proportionality must go beyond traditional considerations – such as organizational size, geographic location, and legal status – by furthering considering the extent and depth of technology used, in particular given the extent to which technological deployments impact the respective risk profile.

A proactive process is needed, Compliance and Risk functions must be more advisory in their approaches and must influence business owners, before new business deployments, by guiding and promoting the establishment of ex-ante controls, including detective controls that are both dynamic and effected in "real-time".

An evolution in the traditional Three Lines Model is clearly in sight. Indeed, we believe that key to the success of the Three Lines Model of the future is the ability of Control Functions to adapt to the rapidly changing socio-economic, geo-political, technology-laden business environment and changes across the industry, which effectively requires an upskilling of control talents, to stay in step with these changes so as to be ex-ante rather than ex-post focused. Ownership of business risks and 1st line accountability should be reinforced by installing resources for day-to-day business while avoiding "bureaucratic - controlling" monitoring activities.

Finally, overcoming these challenges requires an effective internal control system and collaboration within and across the 1st, 2nd and 3rd lines.

Disclaimer

The CRO Forum is supported by a Secretariat
that is run by KPMG Advisory N.V.
Laan van Langerhuize 1, 1186 DS Amstelveen, or
PO Box 74500, 1070 DB Amsterdam
The Netherlands

www.thecroforum.org

cro forum