Update to the three lines of Defense in effective Risk Management & Control

Presented by – CA Nikhil Singhi
Email id – nsinghi@singhico.com
Date - 19th September 2020

Content

SL No.	Particulars
1)	Introduction
2)	The three lines of Defence
3)	The Launch of the Three Lines Model
4)	Principles & Application of the Three Lines Model
5)	Future of Internal Audit

POLL

Are you fully conversant with:

A. The Three Lines of Defence
B. The Three Lines Model
C. NO – I am not conversant with either

Introduction

Background

The Three Lines of Defense model first emerged more than 20 years ago and has since become widely recognized, especially in the financial services sector where it originated. The IIA formally adopted it in a Position Paper ***"The Three Lines of Defense in Effective Risk Management and Control,"*** published in 2013. Since then it has become a valuable tool for those charged with governance.

Coverage

The Three Lines of Defense model provides the following:

- ✓ Direct and simple explanation of the various roles and activities that comprise risk management and control,
- ✓ A simple and effective way to enhance communications on risk management,
- ✓ Provides a fresh look at operations, helping to assure the ongoing success of risk management initiatives,
- ✓ Appropriate for any organization — regardless of size or complexity,
- ✓ Also applicable for organizations where a formal risk management framework or system does not exist.

The Role of Three Lines of Defense

All three lines exists in some form at every organization, regardless of size or complexity. Risk management normally is strongest when there are three separate and clearly identified lines of defense:

First Line of Defense	Second Line of Defense	Third Line of Defense

• **Risk Owners/Managers**
  • Operating Management
	• **Risk Control and Compliance**
	  • Limited Independence
	  • Reports primarily to management
		• **Risk Assurance**
		  • Internal Audit
		  • Greater Independence
		  • Reports to Governing Body

A Classic Example - Wells Fargo

https://www.youtube.com/watch?v=c4I3SyLmfNM

What do we know-

- ❑ Wells Fargo was long seen as the "golden child" of banking.
- ❑ Involved in creation of millions of fraudulent savings and checking accounts on behalf of **Wells Fargo** clients without their consent.
- ❑ Staff at Wells Fargo opened more than 1.5 million unauthorized deposit accounts and applied for roughly 565,000 credit card accounts
- ❑ Once the accounts were opened the employees transferred money to temporarily fund the new accounts which allowed them to meet sales goals and earn extra compensation.
- ❑ The 'scam' lasted 5 years, but also Wells Fargo had to fire about 2% of total 2.65 lacs employees
- ❑ **US Bank was fined with $185 million.**

Questions being asked-

- ✓ Was the top management asleep or did they just have their eyes and ears closed?
- ✓ Should risk management have done something?
- ✓ Where was internal audit?
- ✓ Where was the Board and Governance?

Lessons learnt

- ✓ The extensive set of risk governance practices imposed on the largest banks in the country failed miserably
- ✓ The bank clearly was unable to identify the degree to which employee business practices were creating extensive operational, reputational and regulatory risk for the firm
- ✓ Each line of Defense was inadequately implemented
- ✓ How the internal audit, risk management and anti-fraud professions failed to rise to the occasion and prevent a simple fraud from occurring in the first place.

Launch of the Three Lines Model

Background

The IIA's Three Lines Model have been launched **July 20, 2020**, and supersedes the **2013 Position Paper** The Three Lines of Defense in Effective **Risk Management and Control.**

Coverage

It is intended to serve a very similar purpose (i.e., to help organizations and others understand how various components, including internal audit, contribute to risk management, in order to optimize value creation and avoid confusion, duplication, overlap and inefficiencies).

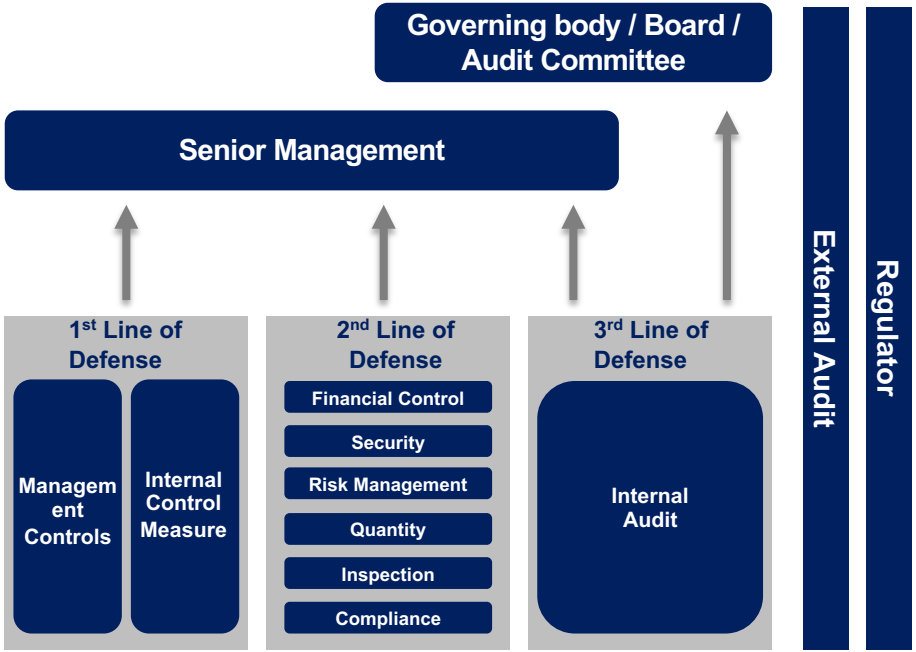
Future State & Opportunities

The Three Lines Model helps organizations identify structures and processes that best assist the achievement of objectives and facilitate strong governance and risk management. The model applies to all organizations and is optimized by:

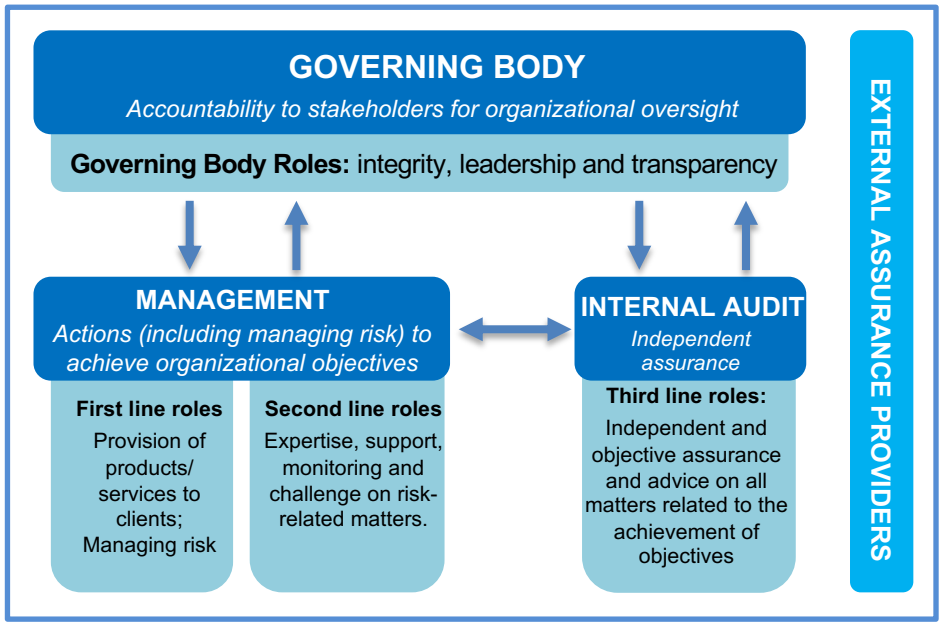
- ✓ Adopting a principles-based approach and adapting the model to suit organizational objectives and circumstances.
- ✓ Focusing on the contribution risk management makes to achieving objectives and creating value, as well as to matters of "defense" and protecting value.
- ✓ Clearly understanding the roles and responsibilities represented in the model and the relationships among them.
- ✓ Implementing measures to ensure activities and objectives are aligned with the prioritized interests of stakeholders.

Demonstrating the two Models

The three Lines of Defense



The three Lines Model



KEY: ↑ Accountability, Reporting | ↓ Delegation, Direction, resources, oversight | ↔ Alignment, communication, coordination, coordination

Similarities and Differences

Key Similarities

- ✓ Applicable to all organizations
- ✓ Designed to help organizations when planning and structuring resources and activities that support the management of risk to avoid overlap, gaps and confusion
- ✓ Focus is primarily internal to an organization
- ✓ Considers the roles and relationships between the governing body, management (including risk-related functions), and internal audit.
- ✓ Maintains the language and numbering of “three lines” in the interests of familiarity
- ✓ The model is simple and is supported by a simple graphic

Key Differences

- ✓ “Defense” is omitted to reflect this is not the sole or primary focus of the model or organizations.
- ✓ Instead of referring to “the first line” and “the second line” as if they were structural elements, the model describes first, second and third line roles that may be combined or separated in various ways
- ✓ Defines principles underpinning the model allowing for flexibility
- ✓ Contextualized more broadly as a tool for governance to include value creation and protection, the offensive and the defensive aspects of managing risk.
- ✓ Governance is defined as requiring three necessary components:
  - ❖ Accountability
  - ❖ Actions
  - ❖ Assurance and advice
- ✓ Encourages a principles-based approach to match the needs and circumstances of the organization.

Challenges that limit its effectiveness

Unclear Roles And Responsibilities

Example: The cyber attack on a health care company that compromised the personal information of more than 2 millions patients.

Reasons:

1. A middle manager in cyber security had misconceptions of what counted as a cyber security incident, leading to a delay in reporting the intrusions.
2. the ISO did not appear to show an appropriate level of concern when a potential breach became clear.

Lack Of Knowledge And Motivation At The First Line

1. Giving the proper training and accountability to the first line
2. Designing a proper rewards policy such that the motivation at the first line is aligned with the organization's overall long-term objectives
3. The long-term objectives should be a balance between financial targets and risk controls.

History is littered with cases of the damage done to an organization that has failed to manage the delicate balance between its lines of defense.
– source www.forbes.com (July 2020)

Challenges that limit its effectiveness

Natural Conflict Between The First And Second Line

1. Natural order that the first line will always want to take on more risks,
2. The second line will always want to keep risks below perceived thresholds of tolerance
3. Key to managing the conflict properly is in having a strong, mature and decisive leadership team that solicits inputs from all lines and considers them equally.

Management place too much reliance on the third line of defense

1. The last line of defense is the primary source of assurance.
2. Management lacks ownership for risk and controls. 3LOD seen as the compliance function.

POLL

Which role is responsible for managing risks?

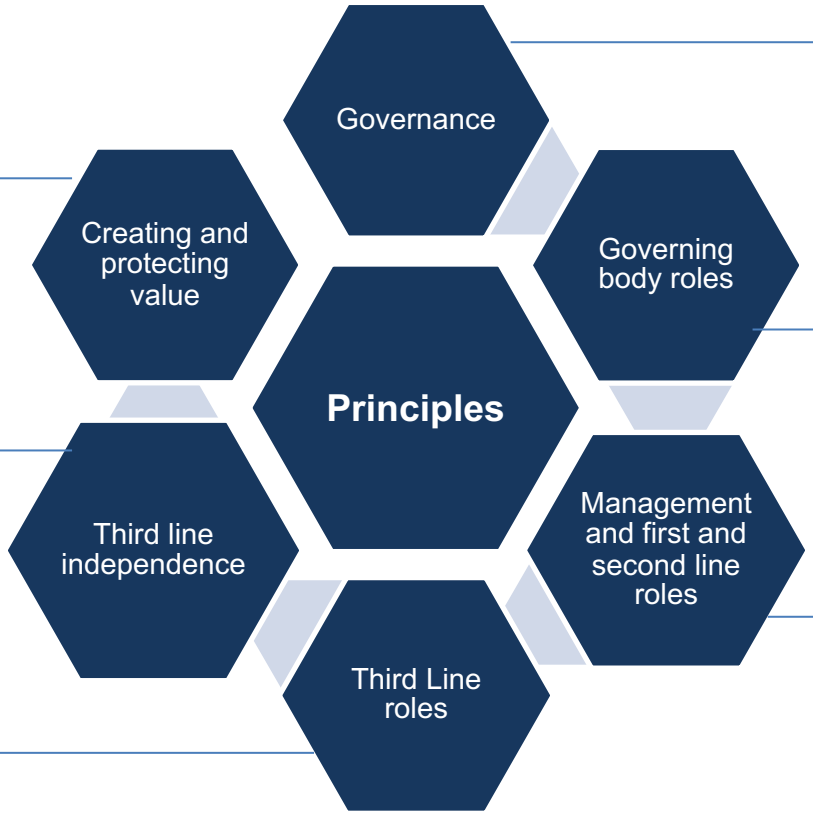
A. First Line
B. Second Line
C. Third Line

Principles

- ✓ All roles working together with the prioritized interests of stakeholders,
- ✓ Ensures the reliability, coherence, and transparency of information needed for risk-based decision making.

- ✓ Includes Internal audit's independence from the responsibilities of management ,
- ✓ Established through accountability to the governing body and freedom from bias or interferences

- ✓ Independent and objective assurance to governance and risk management,
- ✓ systematic and disciplined processes, expertise and insight,
- ✓ Reports its findings to management and the governing body



- ✓ Accountability to stakeholders
- ✓ Risk-based decision-making and application of resources.
- ✓ Assurance and advice by an independent internal audit function

- ✓ Ensures appropriate structures and processes are in place
- ✓ Objectives are aligned with the interests of stakeholders.
- ✓ Establishes independent and competent IA Function

- ✓ First line roles are most directly aligned with the delivery of products and/or services
- ✓ Second line roles provides complimentary expertise to the management of risk

Key Roles of various stakeholders

The Governing Body	✓ Accepts accountability to stakeholders for oversight of the organization. ✓ Engages with stakeholders to monitor their interests and communicate transparently on the achievement of objectives. ✓ Determines organizational appetite for risk and exercises oversight risk management (including internal control)
Management-First line	✓ Leads and directs actions (including managing risk) and application of resources to achieve the objectives of the organization ✓ Maintains a continuous dialogue with the governing body ✓ Establishes and maintains appropriate structures and processes for the management of operations and risk
Management-Second line	✓ Provides complementary expertise, support, monitoring and challenge related to the management of risk ✓ Provides analysis and reports on the adequacy and effectiveness of risk management
Internal audit	✓ Maintains primary accountability to the governing body and independence from the responsibilities of management ✓ Communicates independent and objective assurance and advice to management and the governing body ✓ Reports impairments to independence and objectivity to the governing body and implements safeguards as required
External assurance provider	✓ Provide additional assurance to satisfy legislative and regulatory expectations that serve to protect the interests of stake holders ✓ Provide additional assurance to satisfy requests by management and governing body to complement internal sources of assurance

Symbiotic relationship among core stakeholders

Governing Body & Management

- ✓ Sets the direction of the organization by defining the vision, mission, values,
- ✓ Defines organizational appetite for risk,
- ✓ Receives and reviews reports from management on planned vs actual outcome

- ✓ Have frequent interactions with the governing body,
- ✓ Delegates responsibility for the achievement of the organization's objectives
- ✓ Sends report to governing body on planned, actual, and expected outcomes.

Management & Internal Auditor

- ✓ Regular interactions with the internal auditors
- ✓ Ensures internal audit work is aligned with operational and strategic needs
- ✓ Receives and reviews reports

- ✓ Builds its knowledge and understanding of the organization
- ✓ Advice as a trusted advisor and strategic partner
- ✓ Ensures collaboration and communication to ensure there is no duplication/ overlap/ gaps

Governing Body & Internal Auditor

- ✓ Responsible for oversight of internal audit,
- ✓ Ensures an independent internal audit function is established
- ✓ Serving as the primary reporting line for the Head of IA

- ✓ Act as "eyes and ears" of the governing body.
- ✓ Prepares and submits reports for review

Applying the Model

Structure, Roles & Responsibilities

- ✓ Direction and oversight of second line roles may be designed to secure a degree of independence from those with first line roles .
- ✓ Second line roles may include monitoring, advice, guidance, testing, analyzing, and reporting on matters related to the management of risk.
- ✓ In some organizations, there is a statutory requirement for such arrangements to ensure sufficient independence.

Oversight and Assurance

- ✓ The governing body relies on reports from management, internal audit, and others in order to exercise oversight and achievement of its objectives, for which it is accountable to stakeholders.
- ✓ Management provides valuable assurance on planned, actual, and forecast outcomes, on risk by drawing upon direct experience and expertise.

Coordination and alignment

- ✓ Effective governance requires appropriate assignment of responsibilities as well as strong alignment of activities through cooperation, collaboration, and communication.
- ✓ The governing body seeks confirmation through internal audit that governance structures and processes are appropriately designed and operating as intended.

POLL

Does first line and second line always need to be separate?

A. Yes
B. No
C. Maybe blended or separated

Internal Audit of the Future – Our Skills and Capabilities

Feedback-oriented
Willing to give and receive difficult, feedback, and adapt based on feedback received

Collaborative
Works closely with others, particularly with non-technical backgrounds

Communicative
Comfortable packaging and presenting information in different ways

Business-oriented
Driven to execute against business objectives, finding the right path to achieve them

Analytical
Sees and interprets connections between information

Innovative
Creatively approaches problems, embracing new techniques

Inquisitive
Asks productive questions and focuses on delivering clear and compelling answers

Entrepreneurial
Comfortable working through ambiguity and outside of formal structure

Future of Internal Audit

Assure

- Core Processes
- Truly Greatest Risk
- Decision governance
- Behaviours
- 3LM
- Digital Technologies

Advice

- 3LM Enhancement
- Control effectiveness
- Assurance by design
- During change

Anticipate

- Risk sensing
- Risk learning

Use Digital Assets

- Analytics
- RPA
- Automated QA
- Dashboards

Enablers

- Automated core assurance
- Agile
- High impact reporting
- Response teams
- Change catalyst

ANY QUESTIONS

CA Nikhil Singhi
Partner
M: +91 9769922532
E: nsinghi@singhico.com