Reflections on the Three Lines of Defense

Internal Audit Service, European Commission
November 27, 2019, Brussels

Prof. Flemming Ruud, PhD, CPA (Norway)

Professor of Business Administration, especially Internal Control / Internal Audit

Institute of Accounting, Control and Auditing (ACA) of the University of St. Gallen & the Norwegian Business School in Oslo

Agenda of the *Three Lines of Defense Model*

1. Origin
2. Overview
3. Implementation
4. Update in 2019
5. Summary

Origin of the Three Lines of Defense Model - A Governance Model

The *Three Lines of Defense Model* was developed in 2008-10 by the Federation of European Risk Management Associations (FERMA) and the European Confederation of Institutes of Internal Auditing (ECIIA) as a guidance for the 8th EU Directive Art. 41 2b:

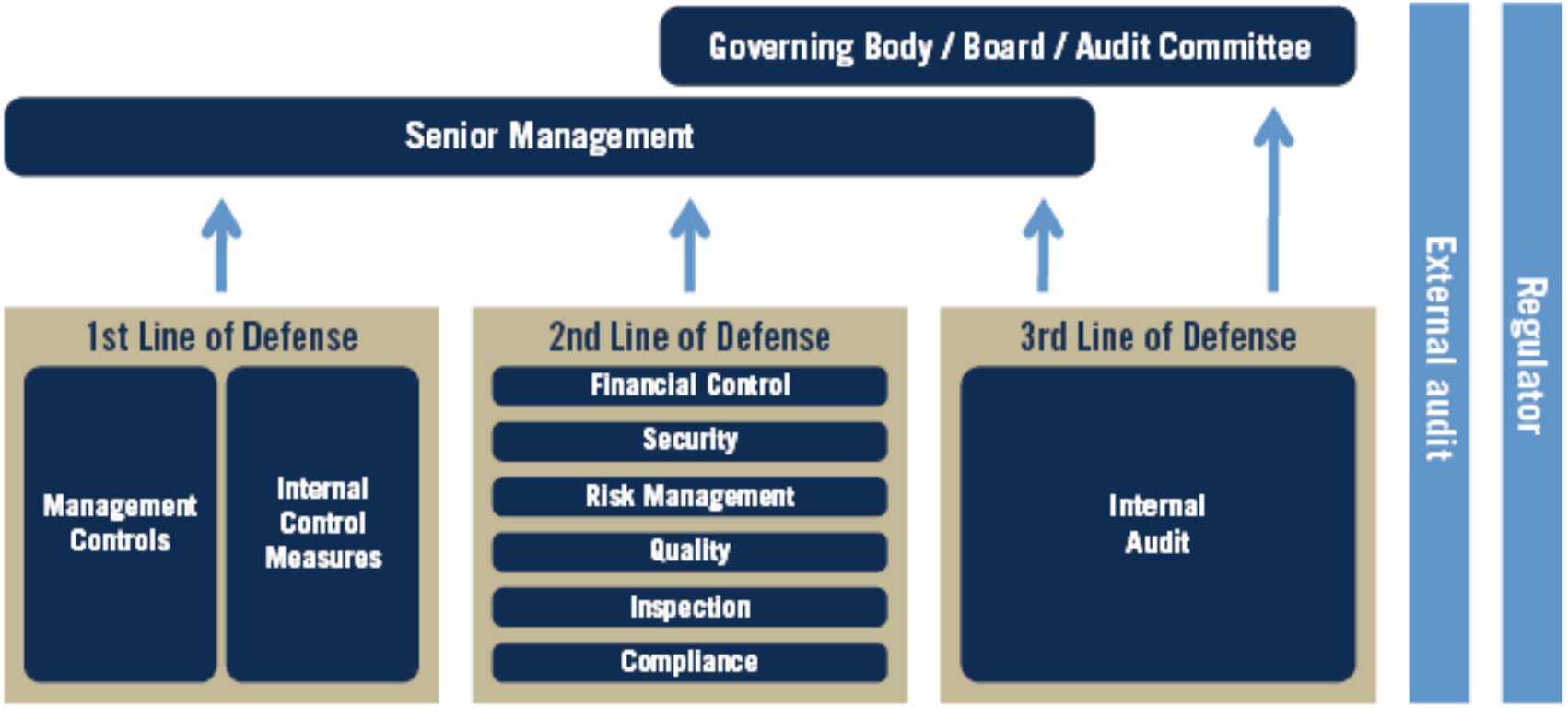
> "[…] the audit committee shall, inter alia: monitor the effectiveness of the company's internal control, internal audit where applicable, and risk management systems […]".

Although this is a relatively simple statement, the questions of "*what to monitor?*" and "*how to monitor?*" are very complex.

The model should therefore provide the board and the audit committee with a simple guidance which:

- shows together the responsibilities for risk management, internal control and internal audit;
- explains how these functions and activities relate to each other; and
- indicates what should be monitored by each function or activity.

Overview of the Three Lines of Defense Model



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

(IIA position paper: The Three Lines od Defense in Effective Risk Management and Control, 2013; IIA position paper: Leveraging COSO across the Three Lines of Defense, 2015)

Responsibilities of the Three Lines

1st Line of Defense

- The *First Line of Defense* are the process owners who manage the business risks in the organization's processes.
- The *First Line* therefore *owns* the risk and is accountable for the design and execution of the organization's internal controls.
- ***Risk ownership***

2nd Line of Defense

- The *Second Line* is put in place to support management and to provide additional expertise, process excellence, and monitoring to help ensure that the risks and controls are effectively managed.
- Its activities are separate from the *First Line of Defense* but they still report functionally to senior management.
- ***Risk Control***

3rd Line of Defense

- The *Third Line,* internal audit, provides assurance to senior management and the board over the effectiveness of the *First and Second Line*.
- The *Third Line* is not allowed to perform management functions to protect its objectivity and independence.
- It has a direct reporting line to the board.
- ***Risk Assurance***

(IIA position paper: The Three Lines od Defense in Effective Risk Management and Control, 2013; IIA position paper: Leveraging COSO across the Three Lines of Defense, 2015)

Purpose of the Three Lines of Defense Model

- The model enhances the understanding of governance, risk management and control by clarifying roles and duties.
- When an organization has properly structured the *Three Lines*, and they operate effectively, there should be no gaps in coverage, no unnecessary duplication of effort, and risk and control has a higher probability of being effectively managed.
- Furthermore, the board of directors will have increased opportunity to receive unbiased information about the organization's most significant risks – and about how management is responding to those risks.
- Senior management and board of directors should clearly communicate the expectation that information be shared and activities coordinated among each of the *Three Lines* where this supports the overall effectiveness of the effort and does not diminish any of the Line's key functions.

Example: Many organizations have put in place board or management level risk policies to articulate these expectations.

(IIA position paper: The Three Lines od Defense in Effective Risk Management and Control, 2013; IIA position paper: Leveraging COSO across the Three Lines of Defense, 2015)

Implementation of the Three Lines of Defense Model

- Activities and functions within each of the Lines of Defense will vary from organization to organization, and some activities or functions may be combined or split across the Lines of Defense.
- Each organization should implement the model in a way that is suitable for their industry, size, operating structure, and approach to risk management.
- All organizations should strive to implement a governance structure that is consistent with the *Three Lines of Defense Model* such that all *Three Lines* exist in some form, regardless of size or complexity of the organization.
- In some situations, such as some smaller companies or where certain activities or functions are in transition, the *Lines of Defense* may not be clearly separated.

Example: In some organizations, parts of a compliance activity or function in the *Second Line* may be involved in designing controls for the *First Line*.

(IIA position paper: The Three Lines od Defense in Effective Risk Management and Control, 2013; IIA position paper: Leveraging COSO across the Three Lines of Defense, 2015)

Implementation of the Three Lines of Defense Model - Implications

- The separate *Lines* should not operate in silos.
- The *Lines* should share information and coordinate efforts regarding risk, control and governance.
- Careful coordination is necessary to avoid unnecessary duplication of efforts while assuring that all significant risks are addressed appropriately.
- In operationalizing this coordination, it is critical that the key roles of executives such as a chief risk officer, a chief compliance officer, or a chief audit executive are carefully established.

(IIA position paper: Leveraging COSO across the Three Lines of Defense, 2015)

Which Helps…

- Assisting management in design and development of processes and controls to manage risks.
- Defining activities to monitor and how to measure success as compared to management expectations.
- Monitoring the adequacy and effectiveness of internal control activities.
- Escalating critical issues, emerging risks and outliers
- Providing risk management and control frameworks.
- Identifying and monitoring known and emerging issues affecting the organization's risks and controls.
- Identifying shifts in the organization's implicit risk appetite and risk tolerance.
- Providing guidance and training related to risk management and control processes.

(IIA position paper: The Three Lines od Defense in Effective Risk Management and Control, 2013; IIA position paper: Leveraging COSO across the Three Lines of Defense, 2015)

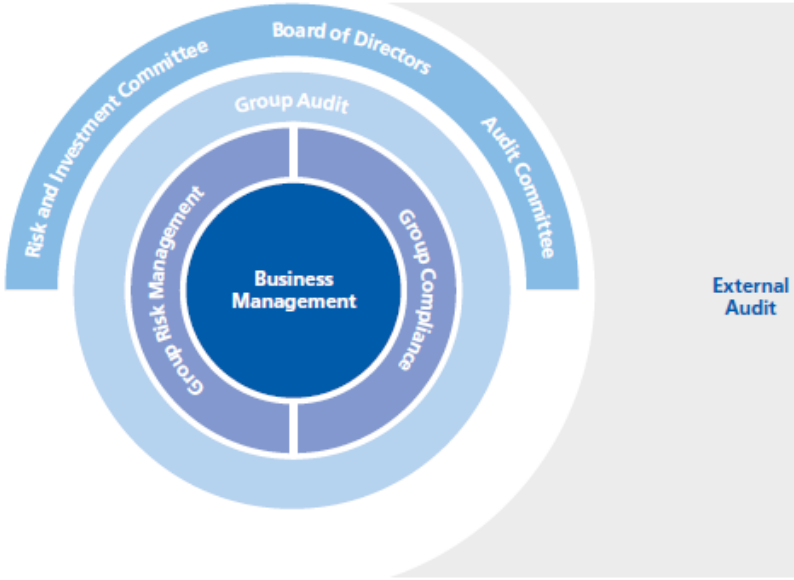
Implementation of the Three Lines of Defense: The Example of *Zurich Insurance Group*

Financial Services - Insurance

Governance, controls and assurance at Zurich Insurance Group

At Zurich, various governance and control functions help to ensure that risks are identified and appropriately managed and internal controls are in place and operating effectively. The Board is ultimately responsible for the supervision of these activities. Although each governance and control function maintains its distinct mandate and responsibilities, the functions are closely aligned and co-operate with each other through a regular exchange of information, planning and other activities. This approach supports management in its responsibilities and provides confidence that risks are appropriately addressed and that adequate mitigation actions are implemented.

Three lines of defense at Zurich Insurance Group
as of December 31, 2018



Zurich uses the three- lines-of-defense model in its approach to governance and enterprise risk management. Zurich's three-lines-of-defense approach runs through Zurich's governance structure, so that risks are clearly identified, assessed, owned, managed and monitored.

(Zurich Insurance Group Annual Report, 2018)

Implementation of the Three Lines of Defense: The Example of *LafargeHolcim*

Industrials – Building/ Construction Materials

Roles & responsibilities

LafargeHolcim established a clear organization structure to ensure the implementation of the risk management and internal control system, following the governance, policies and framework defined by the Group. This organization is built on the concept of three lines of defense.

Under the first line of defense, operational management has ownership, responsibility and accountability for identifying, assessing, managing and mitigating risks. They are equally responsible and accountable for the deployment of the mandatory controls standards defined by the Group. Further information is provided in the Internal Control section on page 79. A risk lead is appointed in every country where we operate to support local management with the yearly risk assessment process, to coordinate activities with other assurance functions, especially the local Internal Control and Compliance teams, and to monitor mitigation actions. Country risk assessment reports are signed off by the Country CEOs and progress on mitigation actions is regularly reported to the Group.

The second line of defense consists of Group corporate functions such as Legal, Compliance, Sustainable Development, Internal Control, Risk Management, Security and Health & Safety. These functions monitor and facilitate the implementation of effective risk management processes and Internal controls by operational management. The objective is to ensure the first line of defense is properly designed and operating as intended. The second line of defense also assists in the development of policies, processes and controls to mitigate risks and issues.

The third line of defense is formed by Group Internal Audit (GIA). As an independent function, GIA provides assurance to the Board of Directors and Executive Committee on the effectiveness of the first and second lines of defense and on governance, risk management and internal controls.

Through the Audit Committee and the Health, Safety and Sustainability Committee (HSSC), the Board of Directors oversees LafargeHolcim risk management, Internal Control and climate change-related risks. The Audit Committee mandate includes the review of compliance and risk management processes and review of management's and internal audit reports on the effectiveness of internal control systems and on the performance of the annual risk assessment process.

The HSSC mandate is to support and advise the Board of Directors on the development and promotion of a healthy and safe environment for employees and contractors, as well as on sustainable development and social responsibility. More details of the Audit Committee and HSSC are disclosed in the Corporate Governance section on pages 94 and 96.

The risks on pages 70 to 78 are considered material and fundamental to our strategy for value creation. This list is not exhaustive and represents the principal risks and uncertainties faced by LafargeHolcim at the time of 2018 annual report preparation. Other risks may emerge in the future and/or the ones stated here may become less relevant.

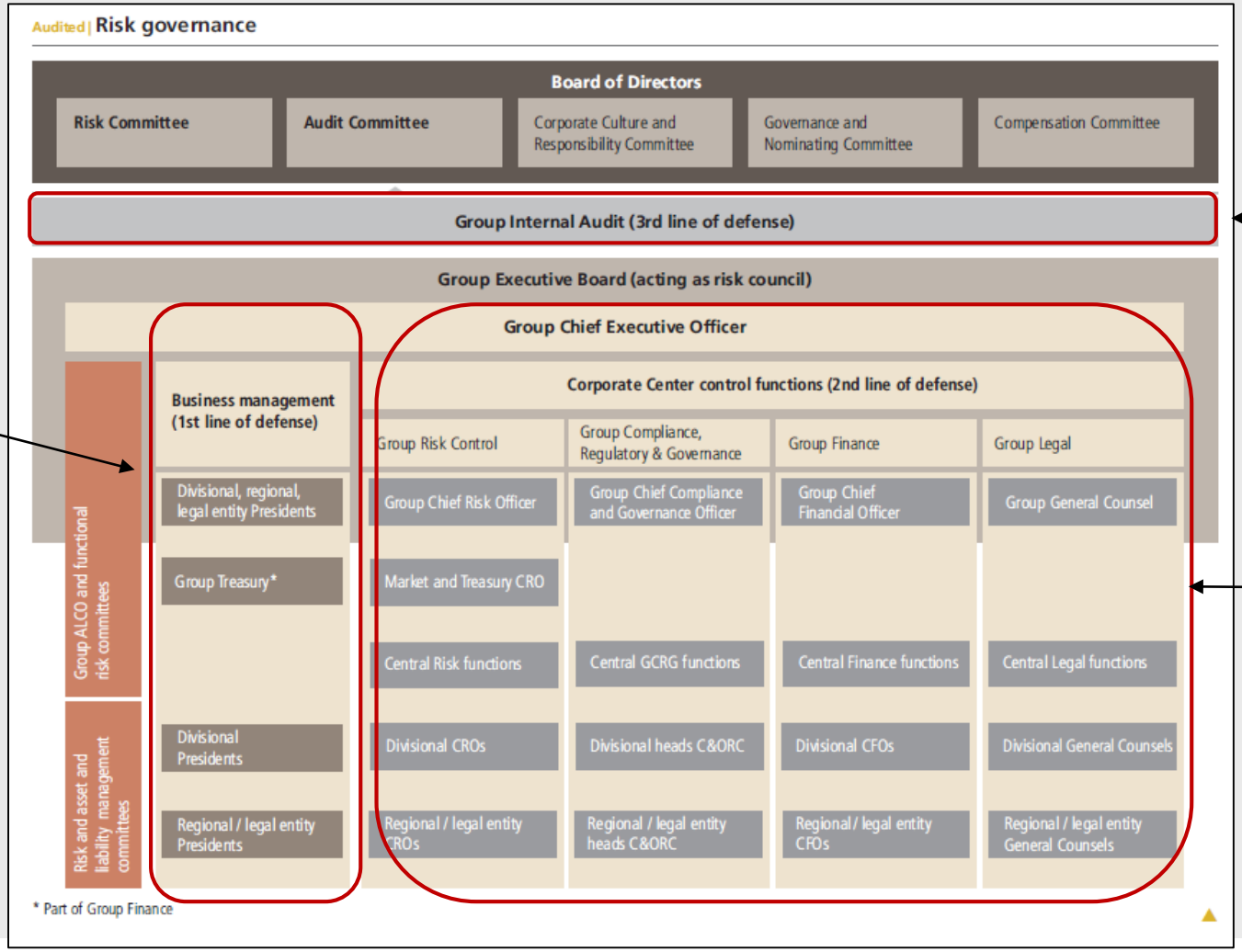
Further information is provided in the Corporate Governance section (pages 90 to 113), Management Discussion & Analysis (pages 142 to 157) and note 14.5 of the consolidated Financial Statements ("Group risk management," page 227).

LafargeHolcim

(LafargeHolcim Annual Report, 2018)

Implementation of the Three Lines of Defense: - The Example of *UBS*

Financial Services - Banks



1st Line

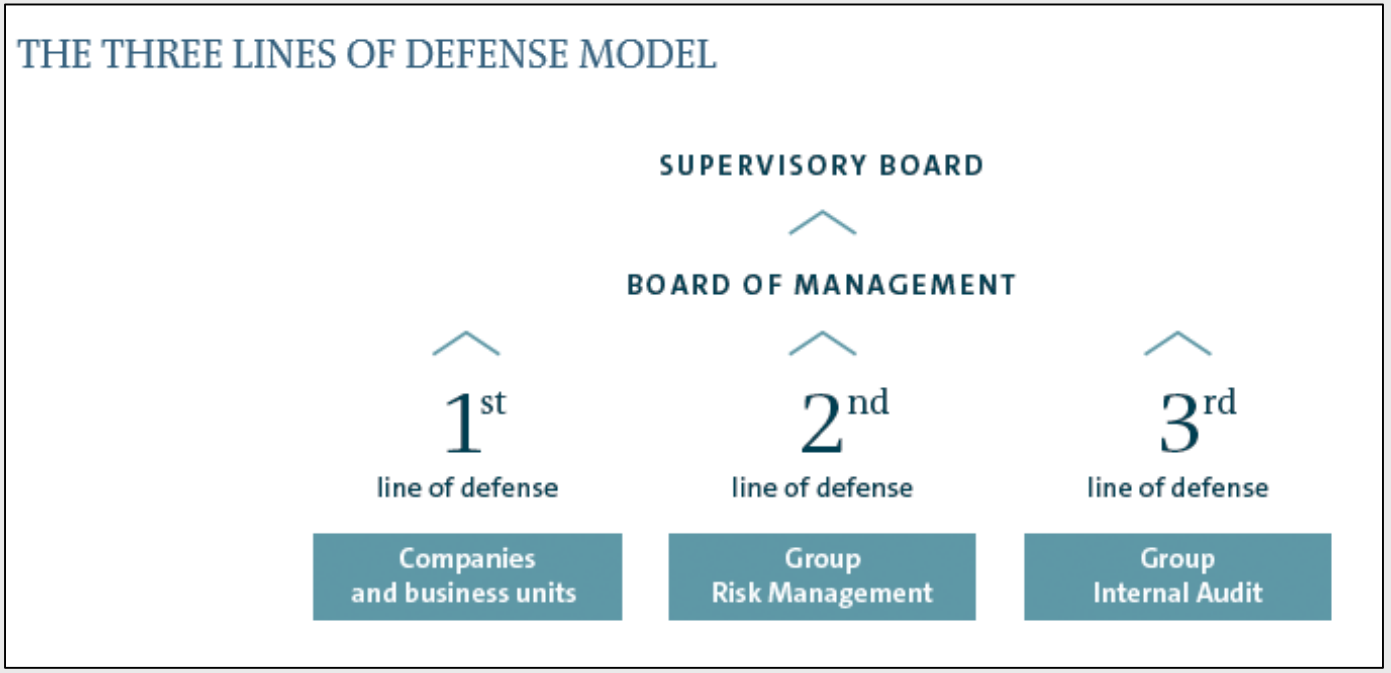
3rd Line

2nd Line

(UBS Annual Report, 2018)

Implementation of the Three Lines of Defense: The Example of *Volkswagen*

Industrials – Car Manufacturing



First line of defense: operational risk management

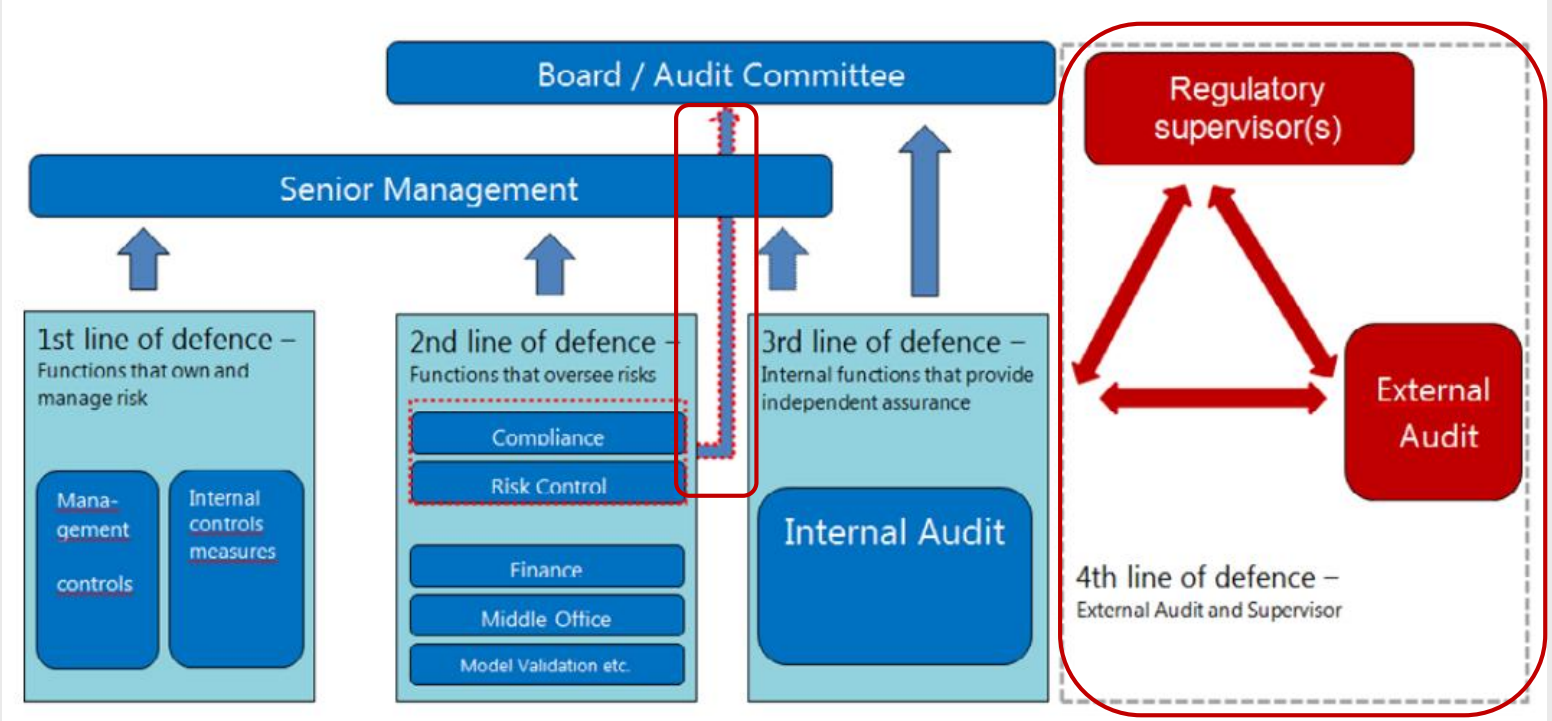
Second line of defense: identifying and reporting systemic and current risks using Group-wide processes

Third line of defense: checks by Group Internal Audit

(https://annualreport2018.volkswagenag.com/group-management-report/report-on-risks-and-opportunities/risk-management-and-control-system.html)

Implementation of the Three Lines of Defense for Financial Institutions – 4th line of Defence

"The "Four Lines of Defense" model is meant to improve cooperation between internal auditors and external parties (i.e. external audit and supervisors)."



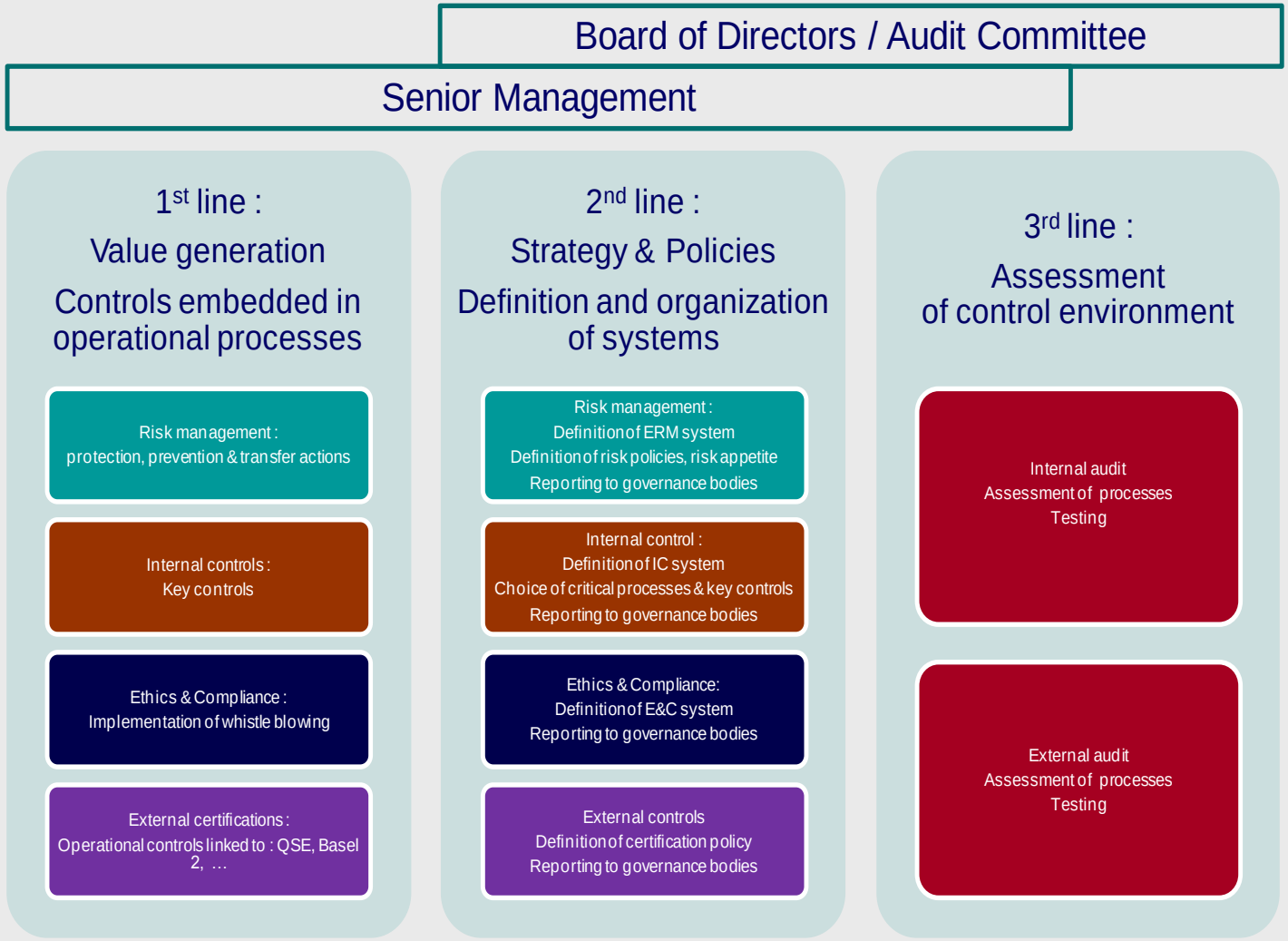
Graph 2: Four-lines-of-defence model for financial institutions

(Financial Stability Institute, Occasional Paper No. 11, The Four Lines of Defense Model for Financial Institutions)

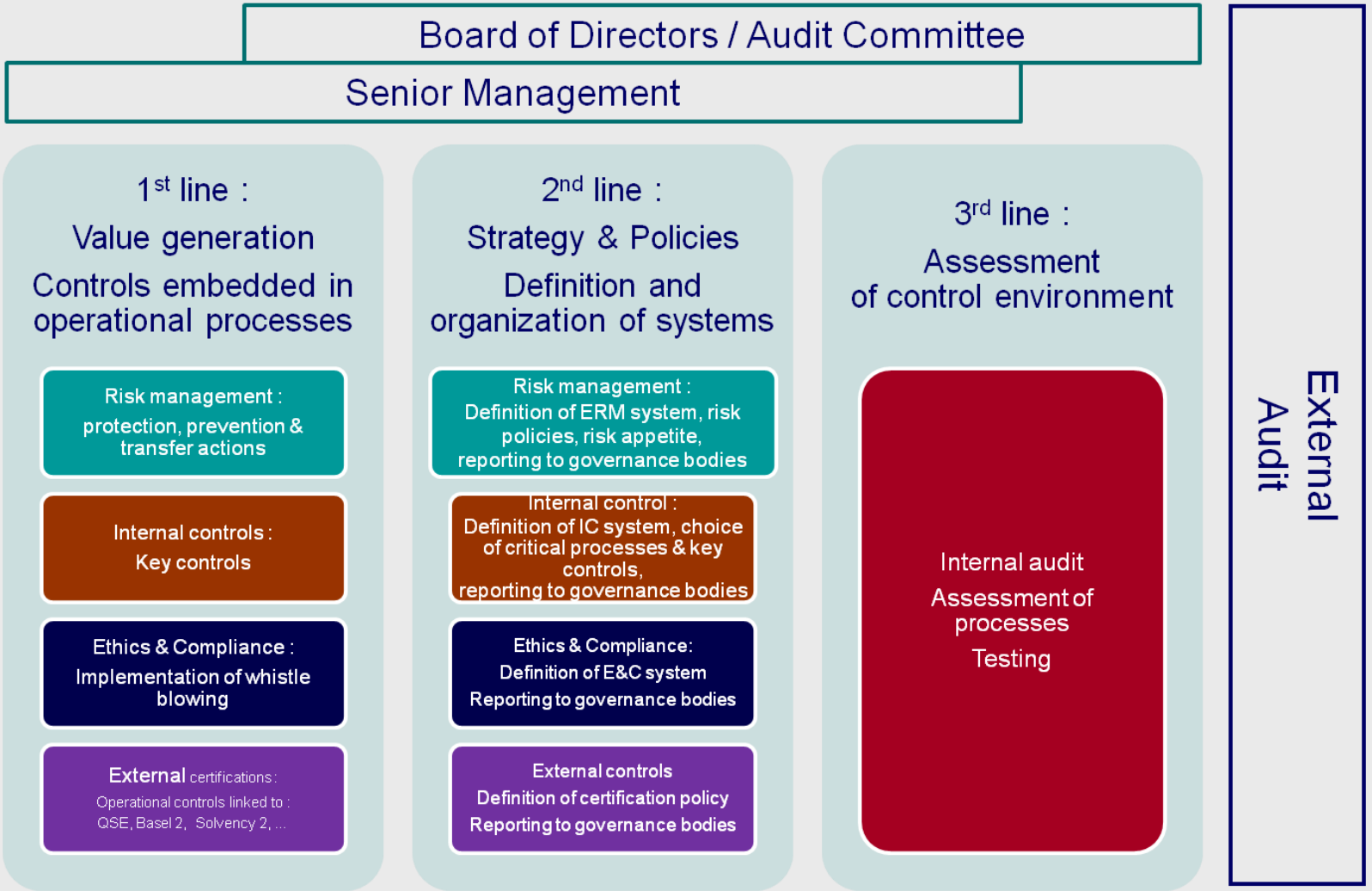
Evaluation of the Three Lines of Defense Model

- A model is merely a simplification of reality
- Which variables are selected and included in the model?
  - Analysis and choice of the governing body
- Further development – New elements or variables?
- Should the *Lines* be separate or more integrated?
- Objectivity and independence?
- Skills in the different *Lines of Defense*?
- Understanding the role of other cnotributors - language
- Value added perspective

Development of the Three Lines of Defense Model - Choice of Activities, Functions and Variables – Ed. 1



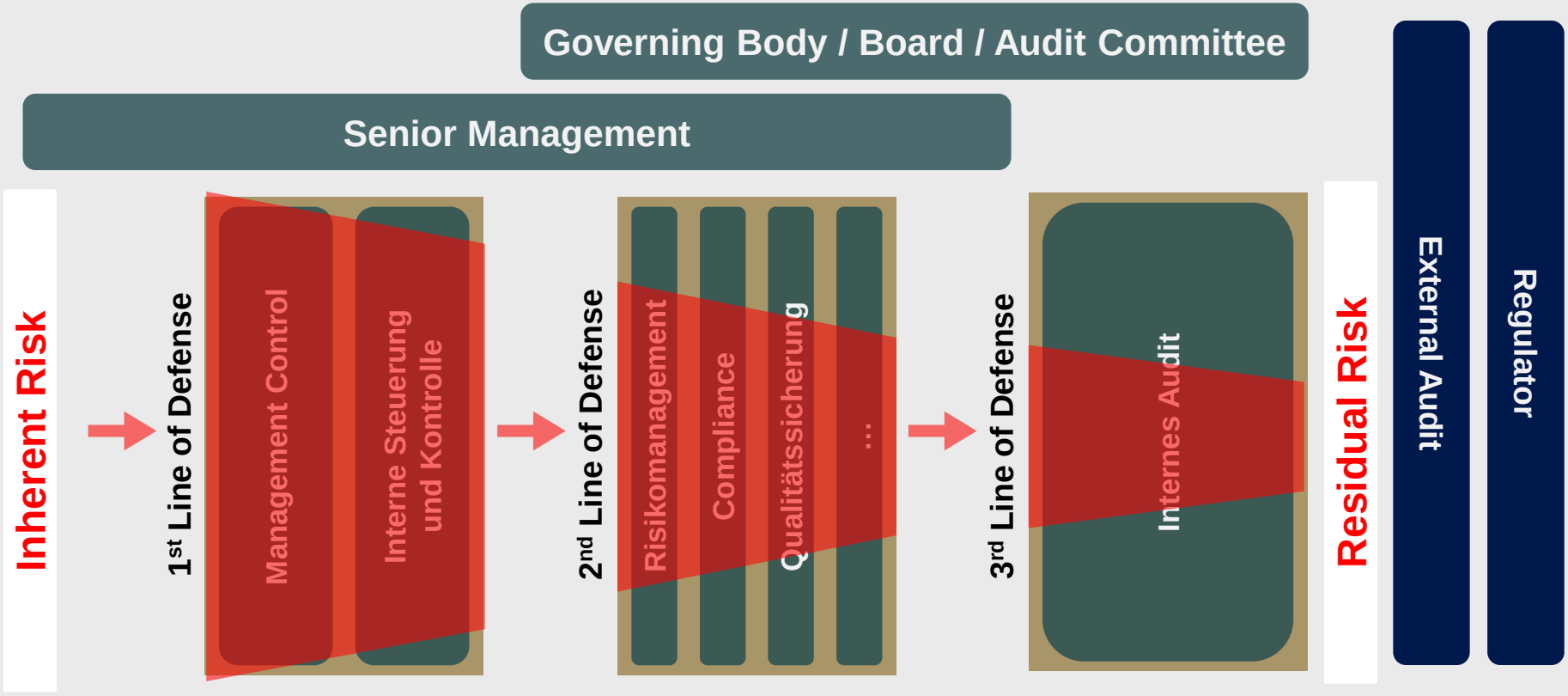
Development of the Three Lines of Defense Model - Choice of Activities, Functions and Variables – Ed. 2



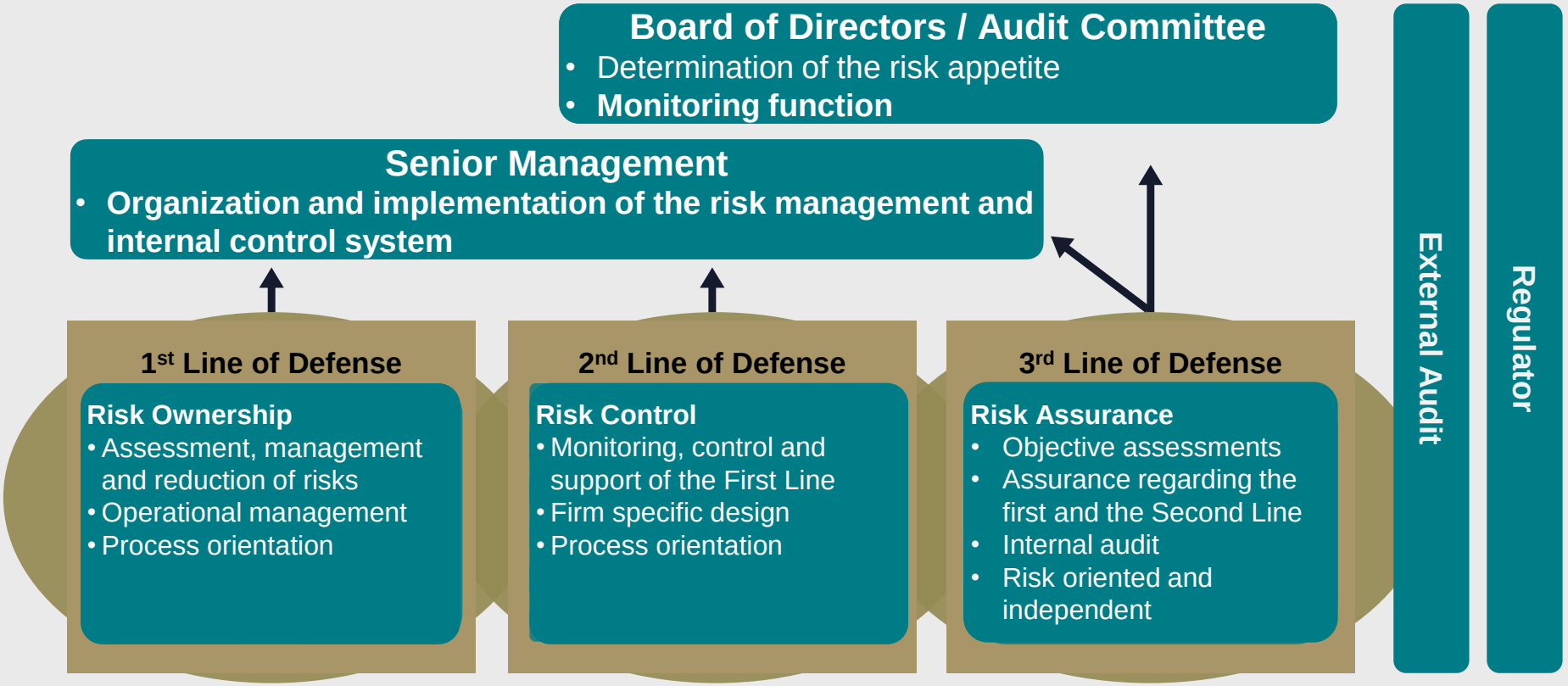
The Meaning of "Defense"

- French: *la defense*, originating from Latin: *defensa* – *"protection"*
- Protect yourself from attacks, - from someone, prevent something
- Argue for a person, case – that is exposed to criticism
- In a trial – accused in a criminal case, defend himself in a trial
- Defense in sports… Rather *offence*…?
- Defend who – who against whom?
  - Management? - Board? - Owners? - Creditors? - Employees?
- *Control* or *defense* – linguistic aspects
- Traditional thought pattern: Internal audit as the "police" for management and governance
  - Traditional image of internal audit? Compliance vs strategic assurance?
  - "Upstream" and less "downstream"?
- Lines of Control? Lines of Responsibility? Lines of Accountability?
- 3rd Line-Assurance? 4th Line-Assurance?

Who is Responsible for what? - Risk Reduction through the 3 Lines of Defense



Implementation of the Three Lines of Defense - Considering new Developments and Trends



"Digitalization, Big data, Data Science & Analytics, Continuous Assurance, Governance & Culture, Tone at the Top,…"

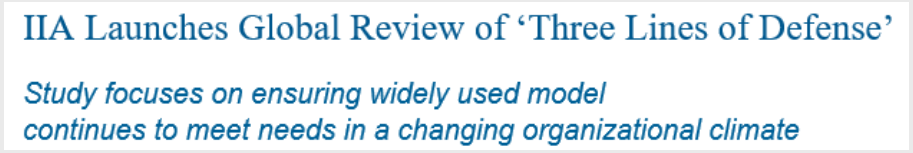
Thank you for your attention!

Prof. Flemming Ruud, PhD, CPA (Norway)

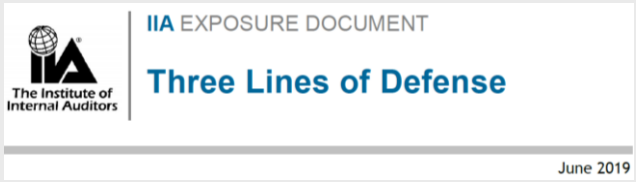
Professor of Business Administration, especially Internal Control / Internal Audit at the Institute of Accounting, Control and Auditing (ACA) of the University of St. Gallen and the Norwegian Business School in Oslo

Update of the Three Lines of Defense Model in 2019 led by the IIA

- The *Three Lines of Defense Model* is currently reviewed and revised by the IIA.
- The main objectives of the review and update of the model are:
  - To make the model more flexibel and easier to implement also for smaller and medium-sized businesses;
  - To improve the coordination and cooperation between the *Lines*, even if it means to «Blur the Lines» if necessary;
  - To promote a proactive and holistic understanding of risk management and to lessen the connotation of «Defense».


IIA Launches Global Review of 'Three Lines of Defense'

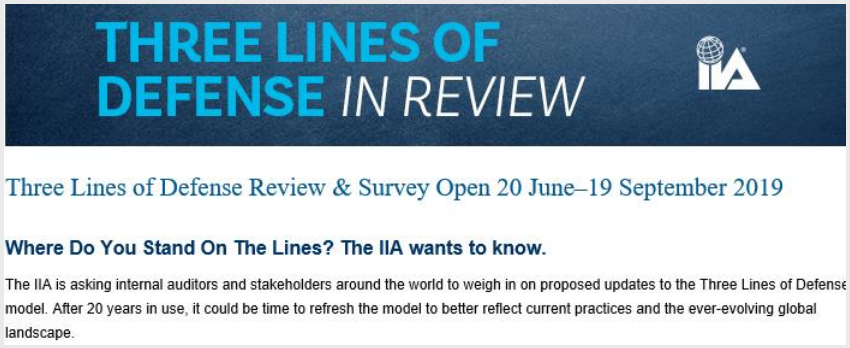
Study focuses on ensuring widely used model continues to meet needs in a changing organizational climate


The Institute of Internal Auditors

IIA EXPOSURE DOCUMENT

Three Lines of Defense

June 2019


THREE LINES OF DEFENSE IN REVIEW

Three Lines of Defense Review & Survey Open 20 June–19 September 2019

Where Do You Stand On The Lines? The IIA wants to know.

The IIA is asking internal auditors and stakeholders around the world to weigh in on proposed updates to the Three Lines of Defense model. After 20 years in use, it could be time to refresh the model to better reflect current practices and the ever-evolving global landscape.

(IIA Exposure Document, Three Lines of Defense, June 2019)

Update of the Three Lines of Defense Model in 2019 – Strengths and Opportunities for Development

In an *Exposure Document*, the IIA provides an overview of the strengths and opportunities for development of the current *Three Lines of Defense Model*:

Strengths of the *Three Lines of Defense Model*	Opportunities for Development
• Is simple, easy to understand, and easy to communicate.	• To maintain these qualities.
• Provides focus on the importance of effective risk management and control.	• To contextualize risk management and control as part of governance, supporting organizational success and value creation.
• Supports an organization's efforts in responding to opportunities and threats.	• To encourage both a proactive and a reactive approach to advancing the goals of an organization.
• Offers a basis for clarity and efficiency when organizing the activities and resources of risk management and control.	• To emphasize the importance of coordination and collaboration aligned to strategic priorities and operational needs.
• Describes the roles played by each of the key functions and relevant external stakeholders with respect to risk management and control.	• To provide additional clarity to the roles and responsibilities of individual functions and to their joint contribution to governance, organizational success, and value creation.

(IIA Exposure Document, Three Lines of Defense, June 2019)

Update of the Three Lines of Defense Model in 2019 – Strengths and Opportunities for Development (Continued)

Strengths of the *Three Lines of Defense Model*	Opportunities for Development
• Describes a means of structuring key functions.	• To highlight the opportunities for a more flexible and agile adoption of the model.
• Has been widely adopted, especially by organizations and regulators in financial services.	• To take account of organizational differences, especially with respect to size, sector, and maturity; demonstrate relevance; and enable ready adoption by any organization.
• Recognizes the roles of external auditors and regulators in risk management and control.	• To consider other external stakeholders and their contribution to governance, organizational success, and value creation without over-complicating the model.
• Allows for a ready explanation of the role of internal audit as the *Third Line of Defense*.	• To expand this description to embrace the role of internal audit as a strategic partner and trusted advisor.
• Provides a useful framework for discussions about independence, objectivity, and assurance.	• To account for and explain «blurring of the lines» and describe appropriate safeguards.
• Is illustrated by a well-known and simple graphic.	• To evolve the graphical representation to reflect evolution and enhancement of the model itself.

(IIA Exposure Document, Three Lines of Defense, June 2019)

Update of the Model and Expansion of the Role of Internal Audit?

The *IIA Exposure Document* also touches upon a potential expansion of the role of internal audit in the revised model, stating:

> "Internal audit can play an important role in leading efforts toward a more integrated approach. This includes assurance mapping to ensure that the coverage across the organization from various functions and other bodies – whether internal or eternal – is consistent, adequate, efficient, reliable, and aligned. […] As a major provider of objective assurance, internal audit can be the one that provides better assurance management in the organization and act as a guarantor that the governing body and the organization as a whole receives the required level of assurance across all activities and capabilities."

Compare:
IIA Standard 2050 – Coordination and Reliance and Practice Guide "Internal Audit and the Second Line of Defense" (2016)

However, in order to ensure internal audit's independence and objectivity, certain safeguards have to be implemented and regarded, including:

- Regular information of the board about internal audit's additional responsibilities;
- Clear definition of the non-assurance roles and possible time restriction;
- Refraining from assuming management responsibility;
- Other measures, such as a "cooling off" period.

(IIA Exposure Document, Three Lines of Defense, June 2019)

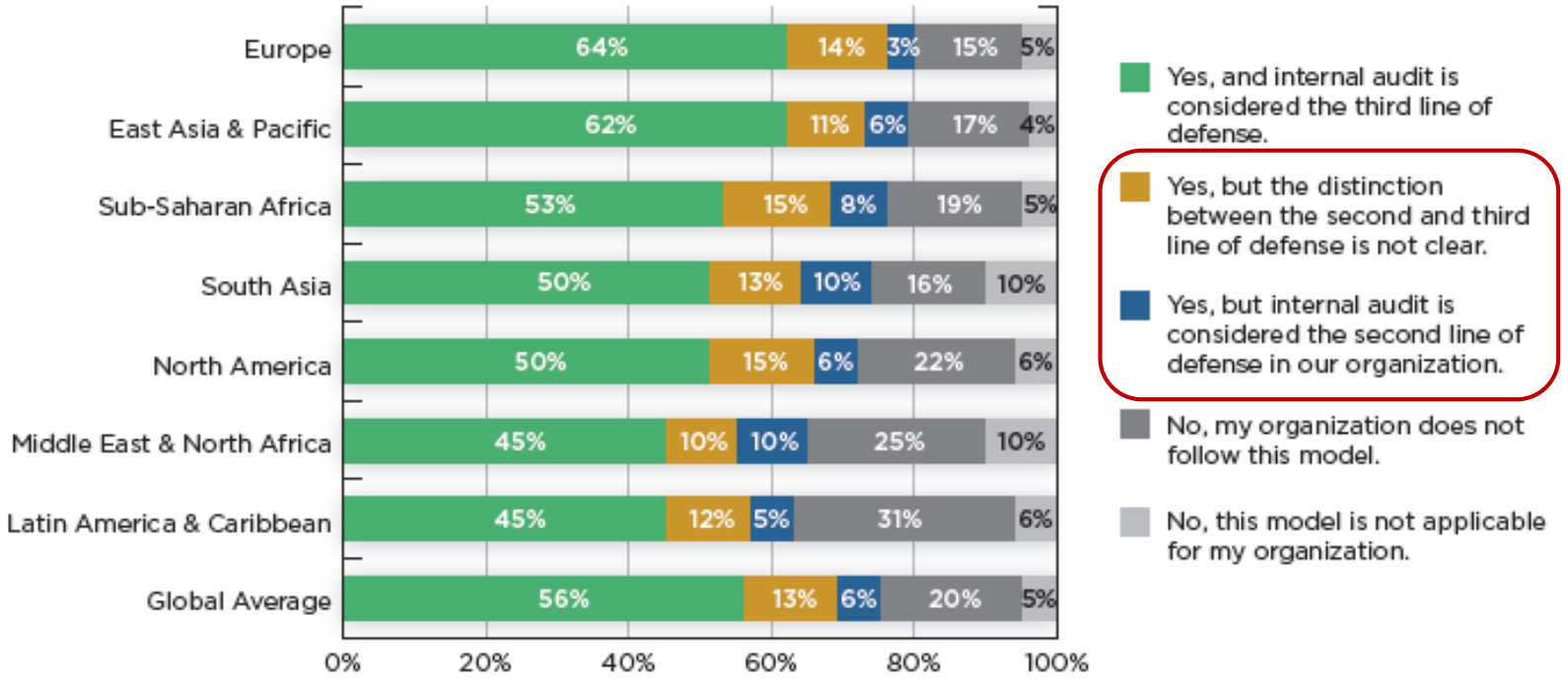
Summary

- The *Three Lines of Defense Model* is a useful model providing a simple and intuitive guidance for the board, respectively the audit committee, to monitor the effectiveness of the company's risk management, internal control and internal audit.
- Like every model, the *Three Lines of Defense Model* is only a simplification of reality so that the underlying assumptions and the graphical representation of the model can be changed if necessary.
- Update in 2019:
  - The current update of the model, led by the IIA, aims to make the model even more flexible, to further promote its adoption beyond the financial services sector, to consider closer cooperation between the *Lines* (and even "blurring of the lines") and to convey a proactive, rather than only a reactive, perspective on risk management.
  - Through the update, the model might help to ensure good corporate governance and value creation and not just convey a «defense» against risks.
  - If the role of internal audit will be expanded towards being a coordinator for the different governance functions and activities, certain safeguards for its independence and objectivity have to be in place.

In Practice the Second and the Third Line of Defense Often Overlap

Exhibit 10 Usage of the Three Lines of Defense Model

(CBOK Study, 2015)



Note: Q63: Does your organization follow the three lines of defense model as articulated by The IIA? Those who responded "I am not familiar with this model" were excluded from these calculations. Due to rounding, some region totals may not equal 100%.
n = 9,093.

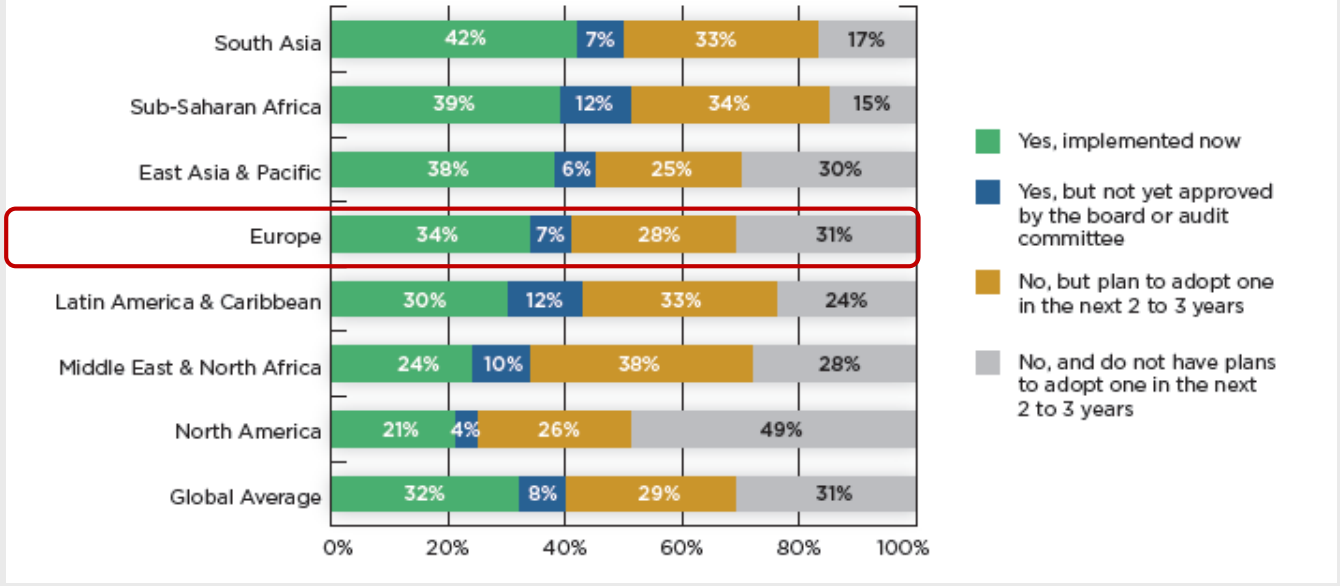
(CBOK, 2015, Combined Assurance: One Language, One Voice, One View)

The IIA Concept of Combined Assurance

"Combined assurance can help solve the problem of assurance fatigue by integrating and aligning assurance processes so that senior management and audit and supervisory committees obtain a comprehensive, holistic view of the effectiveness of their organization's governance, risks, and controls to enable them to set priorities and take any necessary actions."

Exhibit 5 Implementation of Combined Assurance

(CBOK Study, 2015)



SURVEY FACTS

Respondents	14,518*
Countries	166
Languages	23

EMPLOYEE LEVELS

Chief audit executive (CAE)	26%
Director	13%
Manager	17%
Staff	44%

*Response rates vary per question.

(CBOK, 2015, Combined Assurance: One Language, One Voice, One View)

Ways of Implementing and Coordinating Combined Assurance

Coordination takes place through audit activities; specifically, performing audits jointly with supporting activities/functions and/or the external auditor.

Coordination takes place through the planning and reporting processes. The risk-based audit plan is fully aligned with second-line governance activities or functions.

Coordination takes place through align-ment of activities, on a structured or an ad hoc basis.

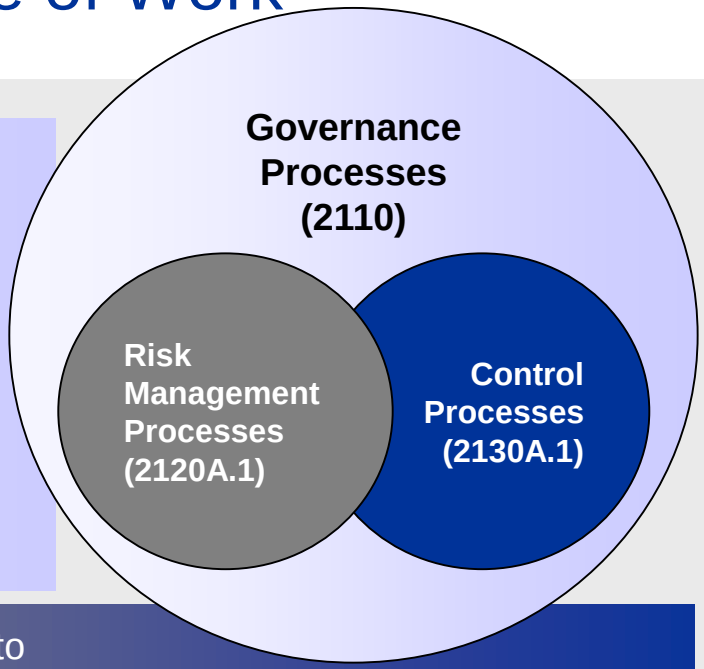
Coordination takes place by combining internal audit and activities/functions that support management, such as risk management, internal control, and compliance.

(CBOK, 2015, Combined Assurance: One Language, One Voice, One View)

Int'l Professional Practices Framework for Internal Auditing Standard 2100: Nature of Work

The IAA must assess and make appropriate recommendations to improve the organization's governance processes for:

- Making strategic and operational decisions.
- Overseeing risk management and control.
- Promoting appropriate ethics and values within the organization.
- Ensuring effective organizational performance management and accountability.
- Communicating risk and control information to appropriate areas of the organization.
- Coordinating the activities of, and communicating information among, the board, external and internal auditors, other assurance providers, and management.



The IIA must evaluate risk exposures relating to the organization's governance, operations, and information systems; .....and based on the risk assessment ... must evaluate the adequacy and effectiveness of controls in responding to the risks within the organization's governance, operations and information systems regarding the:

- Achievement of the organization's strategic objectives
- Reliability and integrity of financial and operational information;
- Effectiveness and efficiency of operations;
- Safeguarding of assets; and
- Compliance with laws, regulations, policies, procedures, and contracts.