

Making 3 Lines of Defense Work as a Compliance Strategy

Susan Roberts, Corporate VP & Chief Compliance Officer
Hospira

Jose Tabuena, Chief Compliance Officer
Next Health

Tom O'Reilly, Director of Internal Audit
Analog Devices



Making 3 Lines of Defense Work as a Compliance Strategy

Susan Roberts, Corporate VP & Chief Compliance Officer
Hospira

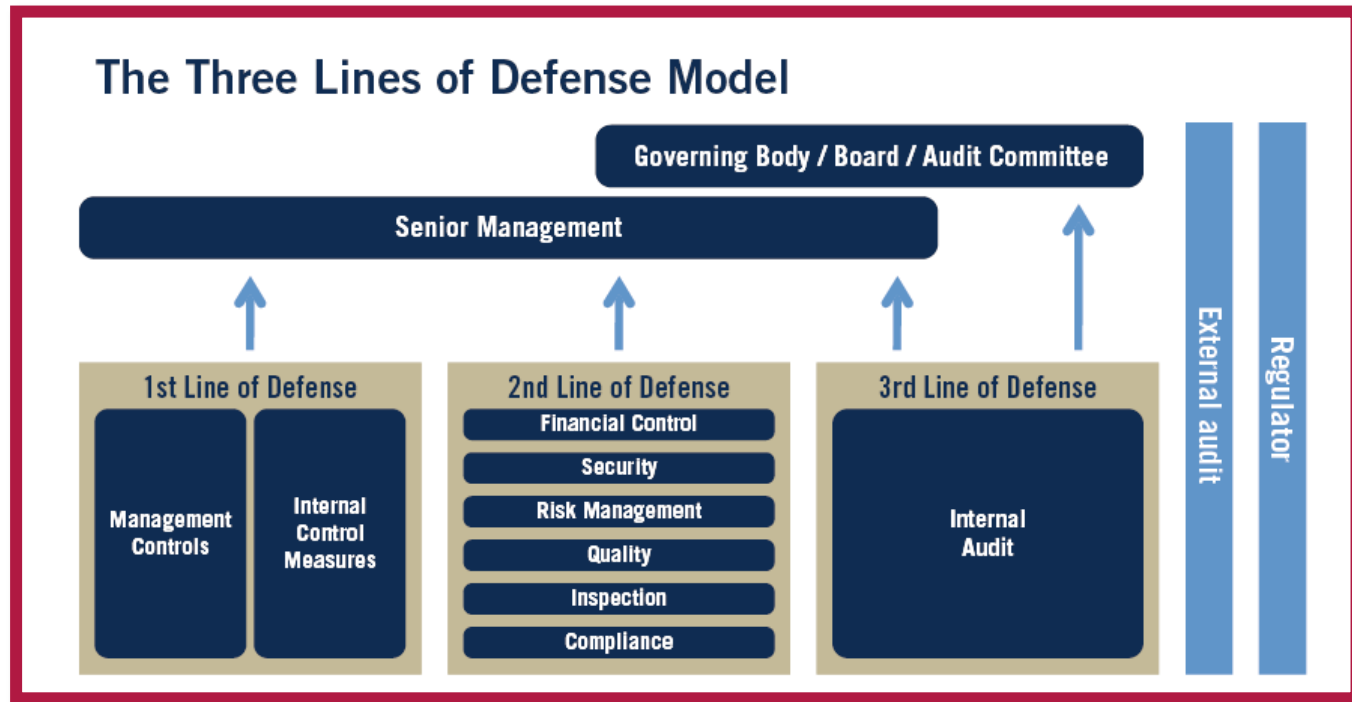




Increasing
Constantly Changing
Interconnected
Internal
External
Vulnerability
Opportunity

Companies with
effective risk
management – that is
coordinated, proactive,
& aligned to business
strategies – will not only
protect their businesses
but will enhance them
and **create growth and
value**

3 Lines of Defense Model



‘Because every organization is unique... there is no one ‘right’ way to coordinate the Three Lines of Defense.’ -- Institute of Internal Auditors 2013

Various approaches have emerged depending on companies’ risks and challenges....

An Approach to Consider ...

Rather than just focusing on the 1st, 2nd and 3rd Lines of Defense...

Focus on the risks presented by the business and let the risk management activities flow from the risks.

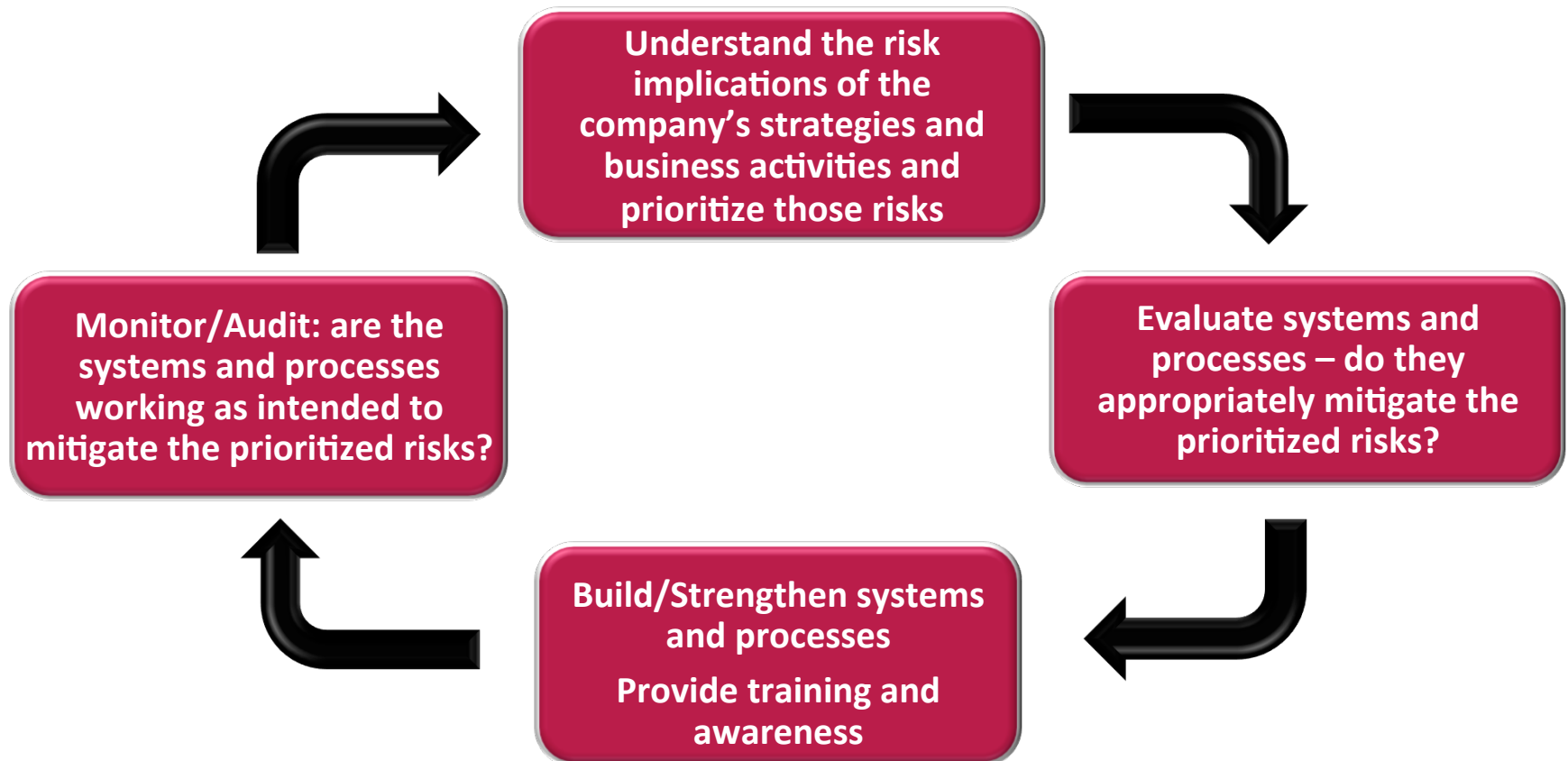
- What are the company's business objectives?
- What are the biggest risks associated with these objectives?
- How can we, as a Company, best mitigate the risks?
- Who can best mitigate the risks?
- Who can best provide objective assurance that the risks have been appropriately mitigated, given the company's risk appetite?

Map the risk activities to the Lines of Defense, ensuring clarity on accountability.

Coordinated Risk Management Process

A Strategic, Comprehensive, Coordinated Risk Management Process

Together with the business, we:

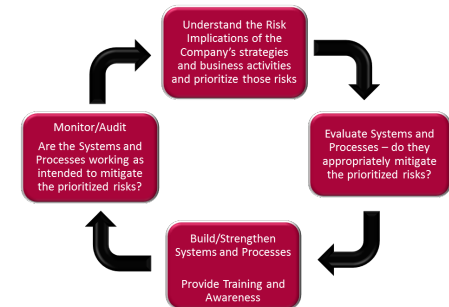


Coordinated Risk Management Process

A Strategic, Comprehensive, Coordinated Risk Management Process

As our business changes...

- As we continue our global expansion
- As we acquire new businesses
- As we continue to launch new products



As laws and industry codes change around the world...

As increased enforcement continues around the world...

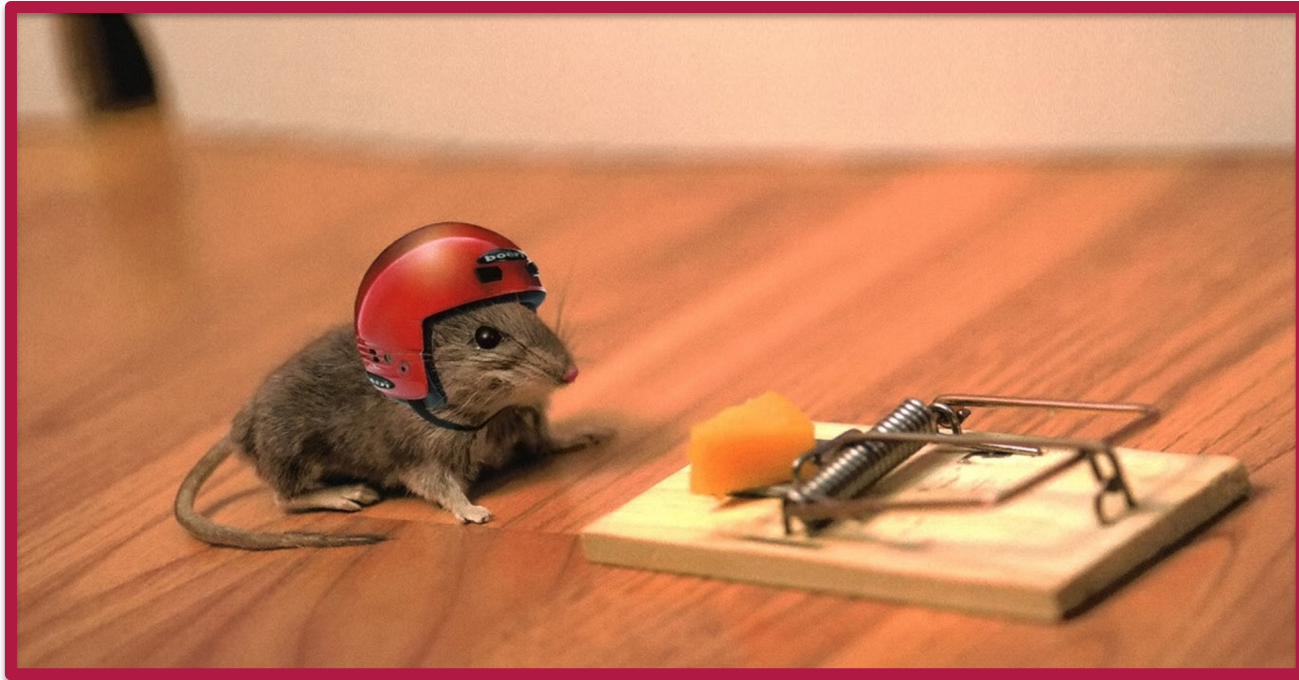
Our working together via this continuous process drives our initiatives and helps ensure that our management of risks is comprehensive, effective, robust and dynamic.

Coordinated Risk Management Process

For this approach to work...

- It may require a culture change: Embed awareness and ownership of risk throughout the organization
- Shift your attitude and approach to risk: Focus on the business objectives first, then turn to risk and risk implications
- Collaboration, coordination and communication among risk management functions are essential for the benefit of the entire organization

This approach enables the organization to make better, more efficient decisions, better anticipate and mitigate risk, seize opportunities, reduce costs and create value, profitability and growth



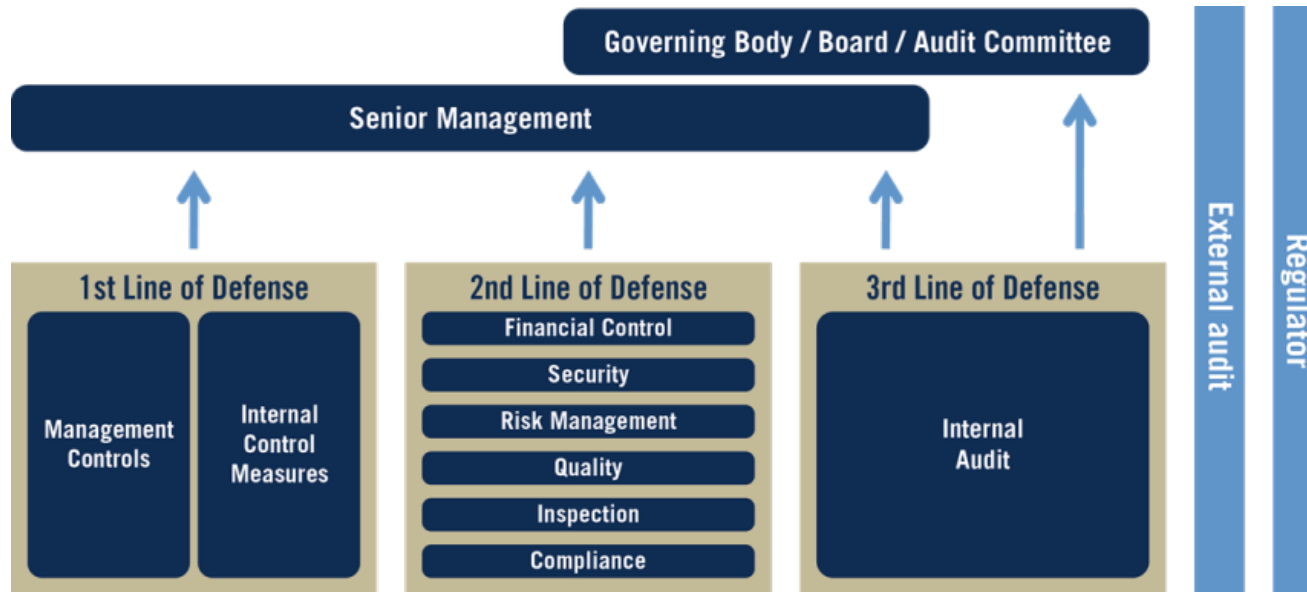
View risk strategically: Focus not just on **risk avoidance** but
also focus on **risk-taking**
(with effective controls, of course!)

Making 3 Lines of Defense Work as a Compliance Strategy

Jose Tabuena, Chief Compliance Officer
Next Health



COSO and the TLD Model



The Second Line of Defense

Internal Monitoring and Oversight Functions

Monitoring Activities

- 16. Conducts ongoing and/or separate evaluations
- 17. Evaluates and communicates deficiencies

Ongoing
Monitoring



2nd Line of Defense

Financial Control

Security

Risk Management

Quality

Inspection

Compliance

Possible Permutations

Compliance and Legal separate and equal

- Audit and compliance (*Boeing*)
- Risk and compliance (*Bank of America*)
- Audit and risk (*Cisco*)

Compliance reports to Legal?

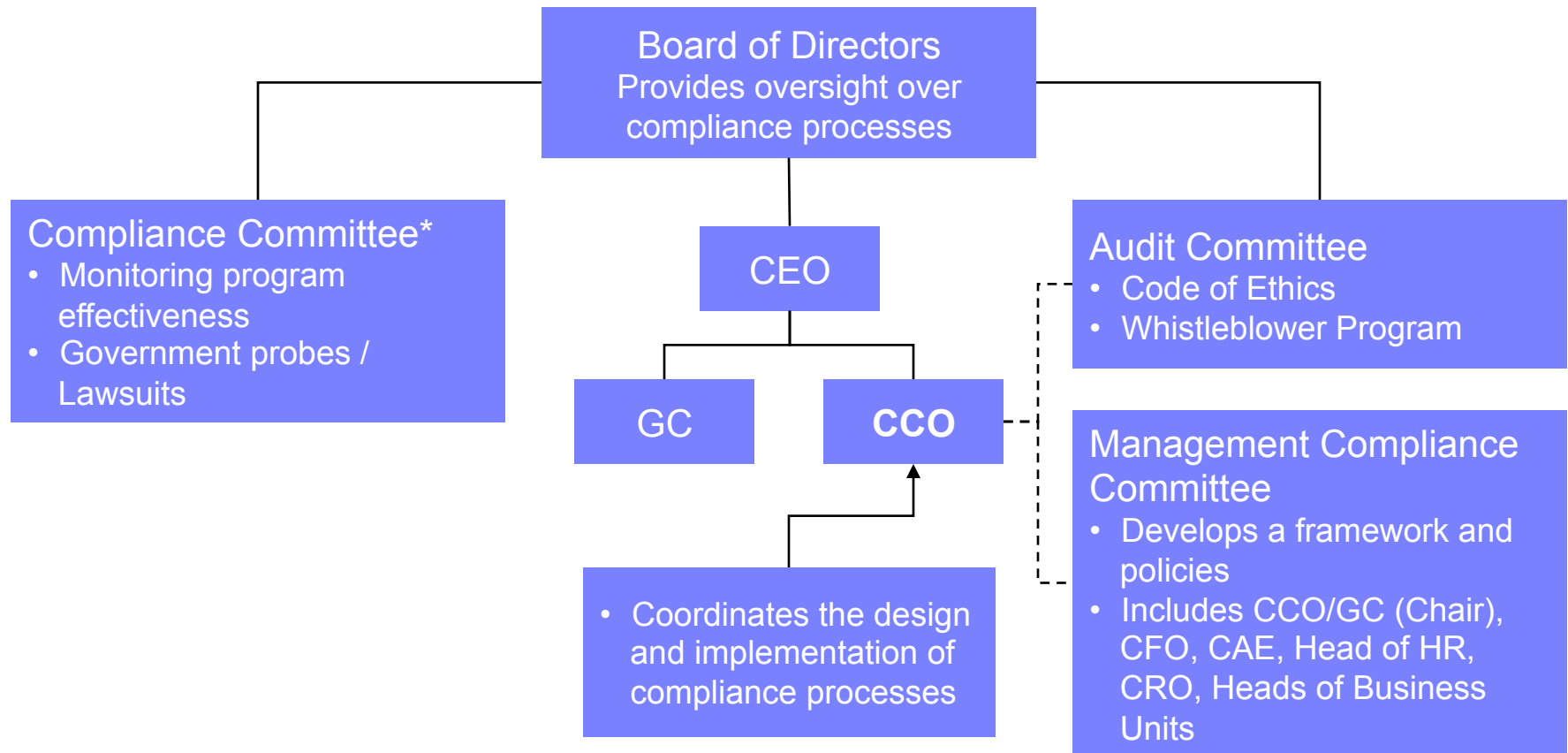
Compliance and Ethics separate?

Internal Audit reports to Finance?

Office of Governance (*Walmart*)

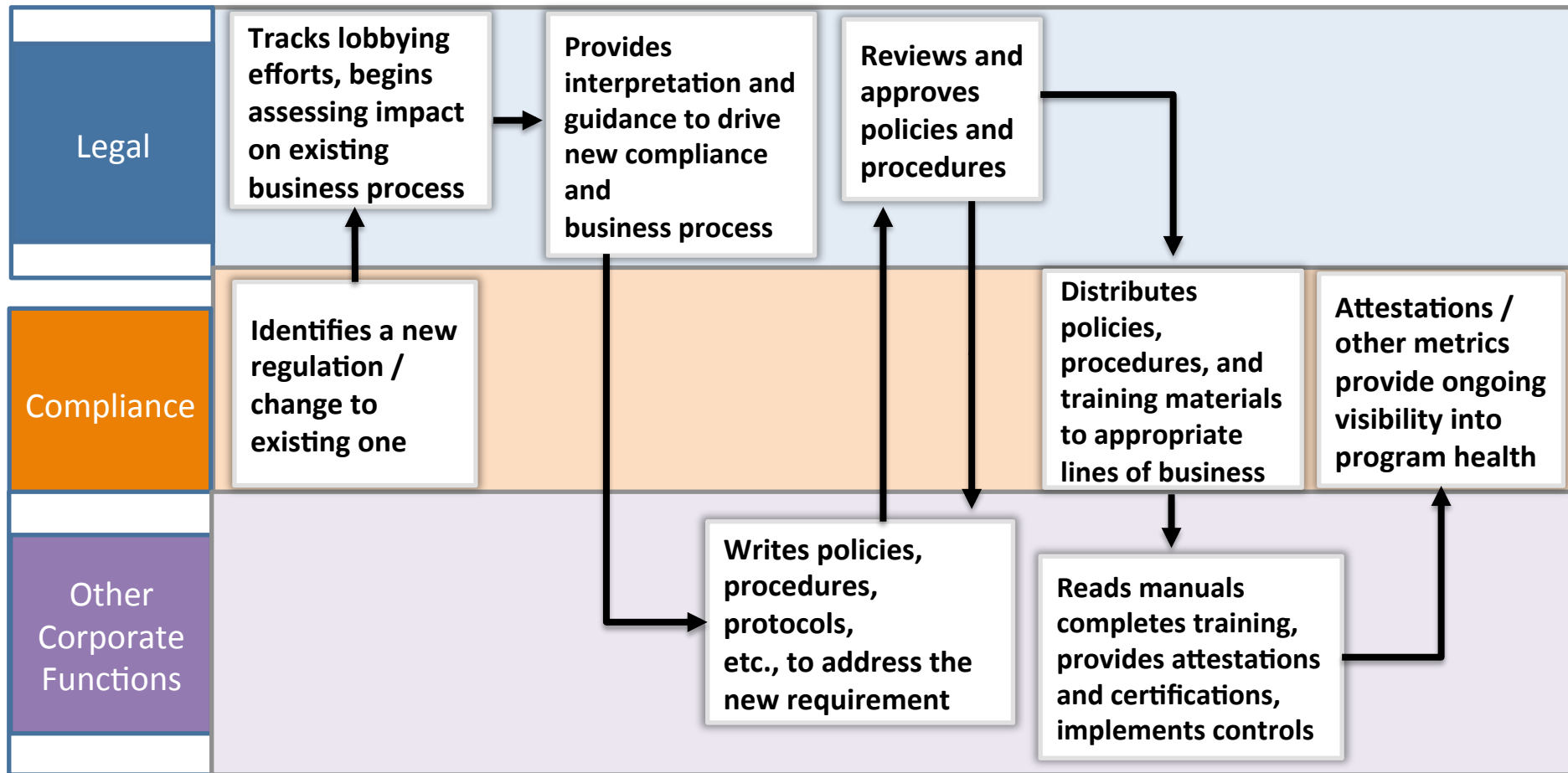
Separate and Complementary

Compliance and Ethics Responsibilities



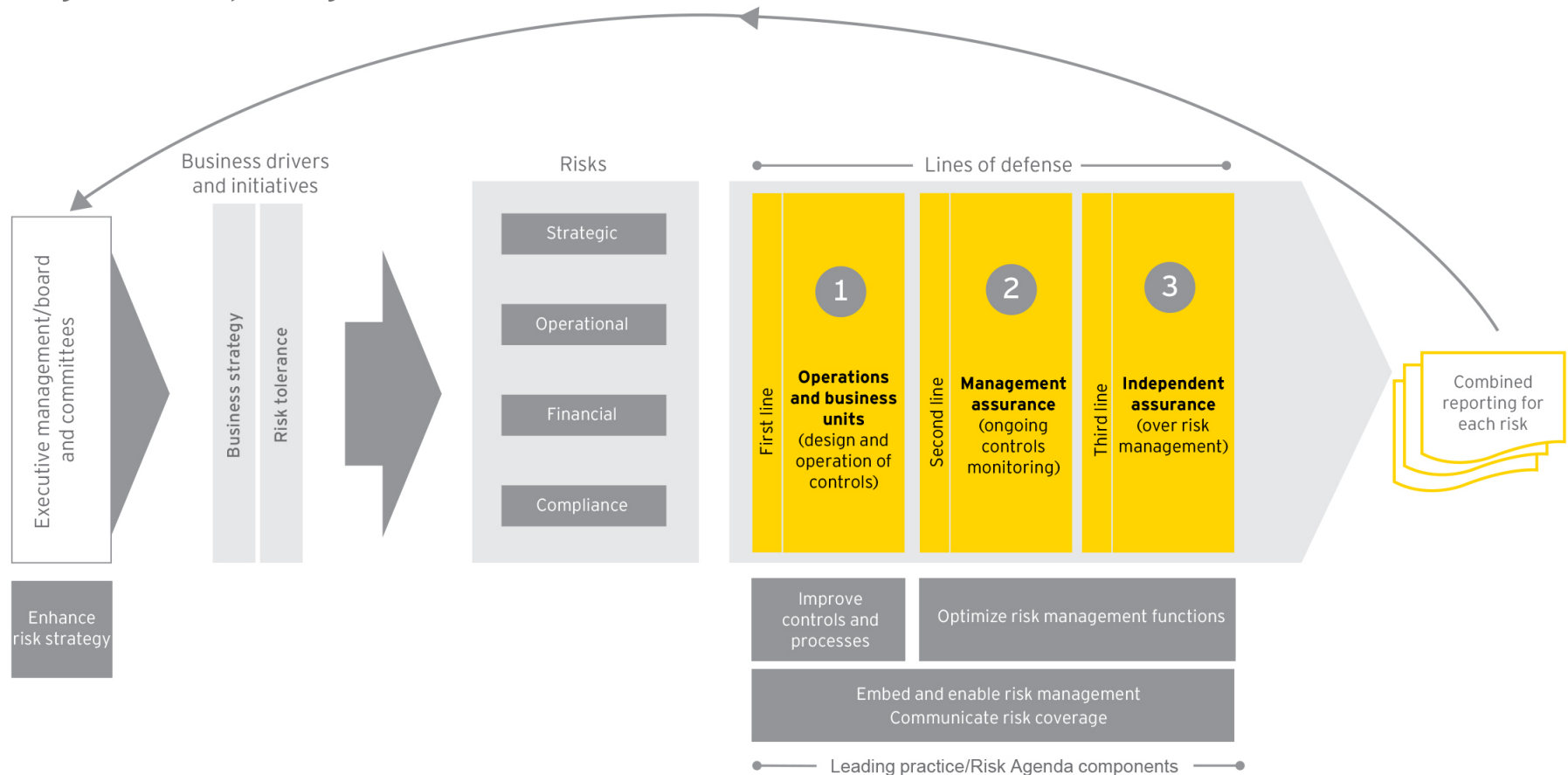
* Compliance oversight may be assigned to an additional board-level committee—especially if the Audit Committee is over burdened. Such a committee would include panels organized primarily to address government or pending litigation (e.g., **Qualified Legal Compliance Committees**)

Regulatory Intelligence | Policy Management



Lines of Defense Operating Model

Integrated LOD operating model



Source: EY

Risk Coverage Map and Plan

Example of a risk coverage plan

					1st line of defense		2nd line of defense						3rd line of defense								
Critical risk	Link to business strategy	Risk ranking	Risk owner	Root causes	Critical controls to mitigate critical risk	Control owner	Management monitoring of controls						Independent assurance providers								Assurance gap?
							Management reviews	Control self-assessment	KPIs/KRIs	Group compliance	Group risk	Group legal	Internal audit	External audit	Independent performance evaluation	External legal specialists	Department of labor	Department of environmental affairs	Insurance	Special projects	

Source: EY

Making 3 Lines of Defense Work as a Compliance Strategy

Tom O'Reilly, Director of Internal Audit
Analog Devices



Context

Three Lines of Defense (TLOD)

- A simple way to **IMPROVE COMMUNICATIONS** on risk management and control

Internal Audit

- Independent and objective assurance
- **EVALUATE** risk management and **CONTROL**
- **IMPROVE BUSINESS OPERATIONS**

Opportunity #1

When could Internal Audit use the TLOD Model to **IMPROVE COMMUNICATIONS** to **AUDIT CLIENTS** when **EVALUATING CONTROL**?

Opportunity:

- Internal Audit kick-off meetings

Opportunity #2

When could Internal Audit use the TLOD Model to
IMPROVE COMMUNICATIONS to **MANAGEMENT**
when **EVALUATING CONTROL**?

Opportunity:

- Providing context for control recommendations

Opportunity #3

When could Internal Audit use the TLOD Model to **IMPROVE COMMUNICATIONS** to **THE BOARD** when **EVALUATING CONTROL**?

Opportunity:

- Reporting themes of Internal Audit observations

Opportunity #4

When could Internal Audit use the TLOD Model
to **IMPROVE COMMUNICATIONS** to **AUDIT**
CLIENTS to **IMPROVE BUSINESS**
OPERATIONS?

Opportunity:

- Providing control awareness training to Business Unit Managers

Opportunity #5

When could Internal Audit use the TLOD Model to
IMPROVE COMMUNICATIONS to **MANAGEMENT**
to **IMPROVE BUSINESS OPERATIONS**?

Opportunity:

- Obtaining approval to carry-out a GRC project

Opportunity #6

When would Internal Audit use the TLOD Model to **IMPROVE COMMUNICATIONS** to **THE BOARD** to **IMPROVE BUSINESS OPERATIONS**?

Opportunity:

- Convincing the board to stop Internal Audit resources from being spent on second LOD monitoring activities