

Associated of Credit Union Internal Auditors

The Three Lines Model

July 20, 2021

National Strength.
SOUTHERN ROOTS.



CRI CARR
RIGGS &
INGRAM

CPAs and Advisors

CRICpa.com

Today's Presenter



Doug has over 30 years' experience (10 years with PwC) providing internal audit and assurance services to both private and publicly held financial institutions ranging in size from de novo status to regional bank holding companies. He has extensive experience in Internal Audit, Enterprise Risk Management (ERM), Sarbanes-Oxley Compliance (SOX) and Anti-Money Laundering (AML).

Doug has a BS in Accounting and MBA from the Sorrell College of Business at TROY University. He is a Certified Public Accountant (CPA), Certified Internal Auditor (CIA), Certified Anti-Money laundering Specialist (CAMS) and is Certified in Risk Management Assurance (CRMA).

Doug serves on the Board of Governors of the Atlanta Chapter of the IIA and is an Advisory Board Member for the Kennesaw State University Internal Audit Center. He is an active TROY alumni, serving in a variety of capacities, including as a member of the Board of Directors for the TROY University Foundation.

Firm Facts



FOUNDED IN 1997 • **10 STATES**  • **25+ MARKETS**



1900+
PROFESSIONALS



300+
PARTNERS



TOP 25 CPA FIRM

(as ranked by Accounting Today)



20+ YEARS
OF CONSISTENT GROWTH
SINCE FORMATION







SERVICES

- Accounting & Auditing
- Advisory
- Business Support & Transactions
- Business Tax
- Employee Benefit Plans
- Governance, Risk & Assurance
- Individual Tax & Planning
- IT Audits & Assurance

INDUSTRY EXPERTISE

- Captive Insurance
- Construction
- Financial Institutions
- Governments
- Healthcare
- Institutional Real Estate
- Insurance
- Manufacturing & Distribution
- Nonprofits

CRI FAMILY OF COMPANIES

-  **Auditwerx**
-  **CRI Advanced Analytics**
-  **CRI Capital Advisors**
-  **CRI Solutions Group**
-  **CRI TPA Services**
-  **Level Four Advisory Services**
-  **Paywerx**
-  **Preferred Legacy Trust**

CARR, RIGGS & INGRAM, LLC

Financial Institutions

175+



Financial
Institution
clients

with assets totaling nearly

\$75+ billion

2 in 5



Banking clients

are subject to FDICIA

*(Federal Deposit Insurance Corporation
Improvement Act)*

CRI'S FINANCIAL INSTITUTIONS EXPERTISE



%

Perform Bank Secrecy
Act services for:

25% of Bank & Credit
Union clients

%

Internal audit and compliance
for approximately:

50% of Bank & Credit
Union clients

%

Tax services for:

30% of Financial
Institution clients

%

FFIEC IT review and
penetration testing for:

25% of Financial
Institution clients

CARR, RIGGS & INGRAM, LLC

The Three Lines Model

Overview



- Where have we been?
- Where are we going?
- Key terms
- Principles of the Three Lines Model
- Key Roles in the Three Lines Model
- Relationships among core roles
- Applying the model

Where have we been?

The Three Lines of Defense Model



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

Where are we going?

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.

Key Terms

- **Organization** - An organized group of activities, resources, and people working toward shared goals.
- **Stakeholders** - Those groups and individuals whose interests are served or impacted by the organization.
- **Governing body** - Those individuals who are accountable to stakeholders for the success of the organization

Key Terms

- **Management** - Those individuals, teams, and support functions assigned to provide products and/or services to the organization's clients.
- **Risk-based decision-making** - A considered process that includes analysis, planning, action, monitoring, and review, and takes account of potential impacts of uncertainty on objectives.
- **Assurance** - Independent confirmation and confidence.

Key Terms

- **Internal audit** - Those individuals operating independently from management to provide assurance and insight on the adequacy and effectiveness of governance and the management of risk (including internal control).
- **The Three Lines Model** - The model previously known as the Three Lines of Defense.
- **Internal control** - Processes designed to provide reasonable confidence over the achievement of objectives.

Key Terms

- **Chief Executive Officer (CEO)** - The most senior individual in the organization with responsibility over operations.
- **Chief Audit Executive (CAE)** - The most senior individual in the organization with responsibility for internal audit services, often known as the Head of Internal Audit or similar title.

Principle 1: Governance



Governance of an organization requires appropriate structures and processes that enable:

- **Accountability** by a governing body to stakeholders for organizational oversight through integrity, leadership, and transparency.

Principle 1 : Governance

- **Actions** (including managing risk) by management to achieve the objectives of the organization through risk-based decision-making and application of resources.
- **Assurance and advice** by an independent internal audit function to provide clarity and confidence and to promote and facilitate continuous improvement through rigorous inquiry and insightful communication.

Principle 2: Governing body roles

The governing body ensures:

- Appropriate structures and processes are in place for effective governance.
- Organizational objectives and activities are aligned with the prioritized interests of stakeholders.

Principle 2: Governing body roles

The governing body:

- Delegates responsibility and provides resources to management to achieve the objectives of the organization while ensuring legal, regulatory, and ethical expectations are met.
- Establishes and oversees an independent, objective, and competent internal audit function to provide clarity and confidence on progress toward the achievement of objectives.

Poll Question #1



Governance is responsible for executing first line roles on a day to day basis.

True or False

Principle 3: Management and first and second line roles

- Management's responsibility to achieve organizational objectives comprises both first and second line roles.
- *First line roles* are most directly aligned with the delivery of products and/or services to clients of the organization, and include the roles of support functions.
- *Second line roles* provide assistance with managing risk.

Principle 3: Management and first and second line roles

- First and second line roles may be blended or separated.
- Some second line roles may be assigned to specialists to provide complementary expertise, support, monitoring, and challenge to those with first line roles.
- Second line roles can focus on specific objectives of risk management, such as: compliance with laws, regulations, and acceptable ethical behavior; internal control; information and technology security; sustainability; and quality assurance.
- Alternatively, second line roles may span a broader responsibility for risk management, such as enterprise risk management (ERM).
- However, responsibility for managing risk remains a part of first line roles and within the scope of management.

Principle 4: Third line roles

- Internal audit provides independent and objective assurance and advice on the adequacy and effectiveness of governance and risk management.
- It achieves this through the competent application of systematic and disciplined processes, expertise, and insight.
- It reports its findings to management and the governing body to promote and facilitate continuous improvement. In doing so, it may consider assurance from other internal and external providers.

Principle 5: Third line independence

- Internal audit's independence from the responsibilities of management is critical to its objectivity, authority, and credibility.
- It is established through: accountability to the governing body; unfettered access to people, resources, and data needed to complete its work; and freedom from bias or interference in the planning and delivery of audit services.

Principle 6: Creating and protecting value

- All roles working together collectively contribute to the creation and protection of value when they are aligned with each other and with the prioritized interests of stakeholders.
- Alignment of activities is achieved through communication, cooperation, and collaboration.
- This ensures the reliability, coherence, and transparency of information needed for risk-based decision making.

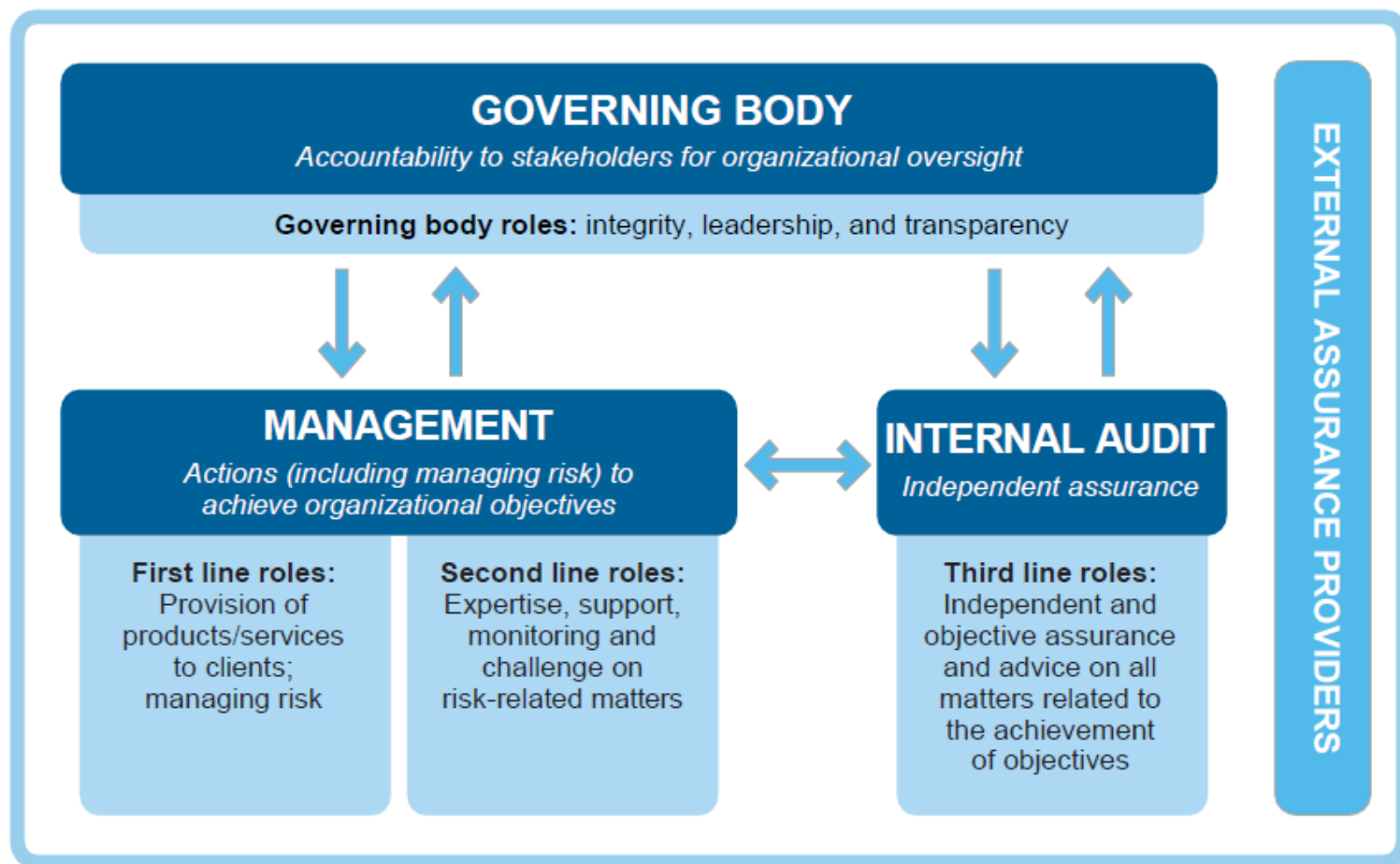
Poll Question #2



Internal audit's independence from management functions is critical to maintain objectivity.

True or False

The IIA's Three Lines Model



KEY:



Accountability, reporting



Delegation, direction, resources, oversight



Alignment, communication coordination, collaboration

Governance roles

- Accepts accountability to stakeholders for oversight of the organization.
- Engages with stakeholders to monitor their interests and communicate transparently on the achievement of objectives.
- Nurtures a culture promoting ethical behavior and accountability.
- Establishes structures and processes for governance, including auxiliary committees as required.
- Delegates responsibility and provides resources to management for achieving the objectives of the organization.
- Determines organizational appetite for risk and exercises oversight of risk management (including internal control).
- Maintains oversight of compliance with legal, regulatory, and ethical expectations.
- Establishes and oversees an independent, objective, and competent internal audit function.

Management: First line roles

- 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, and reports on: planned, actual, and expected outcomes linked to the objectives of the organization; and risk.
- Establishes and maintains appropriate structures and processes for the management of operations and risk (including internal control).
- Ensures compliance with legal, regulatory, and ethical expectations.

Management: Second line roles

Provides complementary expertise, support, monitoring, and challenge related to the management of risk, including:

- The development, implementation, and continuous improvement of risk management practices (including internal control) at a process, systems, and entity level.
- The achievement of risk management objectives, such as: compliance with laws, regulations, and acceptable ethical behavior; internal control; information and technology security; sustainability; and quality assurance.

Provides analysis and reports on the adequacy and effectiveness of risk management (including internal control).

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 on the adequacy and effectiveness of governance and risk management (including internal control) to support the achievement of organizational objectives and to promote and facilitate continuous improvement.
- Reports impairments to independence and objectivity to the governing body and implements safeguards as required.

External Assurance Providers

Provide additional assurance to:

- Satisfy legislative and regulatory expectations that serve to protect the interests of stakeholders.
- Satisfy requests by management and the governing body to complement internal sources of assurance

Poll question #3



First line roles must be approved by external assurance providers.

True or False

Relationships – Governance & Mgmt

- The governing body typically sets the direction of the organization by defining the vision, mission, values, and organizational appetite for risk. It then delegates responsibility for the achievement of the organization's objectives to management, along with the necessary resources.
- The governing body receives reports from management on planned, actual, and expected outcomes, as well as reports on risk and the management of risk.

Relationships – Governance & Mgmt

- Organizations vary as to the degree of overlap and separation between the roles of the governing body and management.
- The governing body can be more or less “hands on” with respect to strategic and operational matters. Either the governing body or management may take the lead in developing the strategic plan, or it may be a shared undertaking.
- In some jurisdictions, the Chief Executive Officer (CEO) may be a member of the governing body and may even be its chair. In all cases, there needs to be strong communication between management and the governing body.
- The CEO is typically the focal point for this communication, but other senior managers may have frequent interactions with the governing body.
- Organizations may wish, and their regulators may require, leaders of second line roles such as a Chief Risk Officer (CRO) and a Chief Compliance Officer (CCO) to have a direct reporting line to the governing body. This is fully consistent with the Principles of the Three Lines Model.

Relationships – Mgmt & Internal Audit

- Internal audit's independence from management ensures it is free from hindrance and bias in its planning and in the carrying out of its work, enjoying unfettered access to the people, resources, and information it requires. It is accountable to the governing body.
- However, independence does not imply isolation. There must be regular interaction between internal audit and management to ensure the work of internal audit is relevant and aligned with the strategic and operational needs of the organization.
- Through all of its activities, internal audit builds its knowledge and understanding of the organization, which contributes to the assurance and advice it delivers as a trusted advisor and strategic partner.
- There is a need for collaboration and communication across both the first and second line roles of management and internal audit to ensure there is no unnecessary duplication, overlap, or gaps.

Relationships – IA & Governance

- Internal audit is accountable to, and sometimes described as being the “eyes and ears” of, the governing body.
- The governing body is responsible for oversight of internal audit, which requires: ensuring an independent internal audit function is established, including the hiring and firing of the Chief Audit Executive (CAE); serving as the primary reporting line for the CAE; approving and resourcing the audit plan; receiving and considering reports from the CAE; and enabling free access by the CAE to the governing body, including private sessions without the presence of management.

Relationships - among all roles

The governing body, management, and internal audit have their distinct responsibilities, but all activities need to be aligned with the objectives of the organization. The basis for successful coherence is regular and effective coordination, collaboration, and communication.

Poll question #4



Effective and efficient coordination amongst stakeholders is critical to the success of the three lines model.

True or False

Structure, roles and responsibilities

- The Three Lines Model is most effective when it is adapted to align with the objectives and circumstances of the organization.
- How an organization is structured and how roles are assigned are matters for management and the governing body to determine.
- The governing body may establish committees to provide additional oversight for particular aspects of its responsibility, such as audit, risk, finance, planning, and compensation.
- Within management, there are likely to be functional and hierarchical arrangements and an increasing tendency toward specialization as organizations grow in size and complexity.

Structure, roles and responsibilities

- Functions, teams, and even individuals may have responsibilities that include both first and second line roles.
- However, direction and oversight of second line roles may be designed to secure a degree of independence from those with first line roles — and even from the most senior levels of management — by establishing primary accountability and reporting lines to the governing body.
- The Three Lines Model allows for as many reporting lines between management and the governing body as required. In some organizations, most notably regulated financial institutions, there is a statutory requirement for such arrangements to ensure sufficient independence. Even in these situations, those in management with first line roles remain responsible for managing risk.

Structure, roles and responsibilities

Second line roles may include monitoring, advice, guidance, testing, analyzing, and reporting on matters related to the management of risk. Insofar as these provide support and challenge to those with first line roles and are integral to management decisions and actions, second line roles are part of management's responsibilities and are never fully independent from management, regardless of reporting lines and accountabilities

Structure, roles and responsibilities

- A defining characteristic of third line roles is independence from management.
- The Principles of the Three Lines Model describe the importance and nature of internal audit independence, setting internal audit apart from other functions and enabling the distinctive value of its assurance and advice.
- Internal audit's independence is safeguarded by not making decisions or taking actions that are part of management's responsibilities (including risk management) and by declining to provide assurance on activities for which internal audit has current, or has had recent, responsibility.
- For example, in some organizations, the CAE is asked to assume additional decision-making responsibilities over activities utilizing similar competencies, such as aspects of statutory compliance or ERM. In such circumstances, internal audit is not independent of these activities or of their results, and therefore, when the governing body seeks independent and objective assurance and advice relating to those areas, it is necessary for its provision to be undertaken by a qualified third party.

Oversight and assurance

- The governing body relies on reports from management (comprising those with first and second line roles), 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 (also referred to as attestations) on planned, actual, and forecast outcomes, on risk, and on risk management by drawing upon direct experience and expertise.
- Those with second line roles provide additional assurance on risk-related matters.
- Because of internal audit's independence from management, the assurance it provides carries the highest degree of objectivity and confidence beyond that which those with first and second line roles can provide to the governing body, irrespective of reporting lines.
- Further assurance may also be drawn from external providers

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.

**All content herein was extracted directly from “The IIA’s Three Lines Model”.*

Questions?

Join Our Conversation

CONNECT @CRlcpa



#tryCRI #CRlcpa

TODAY'S PRESENTERS

Doug Mims
Partner
Atlanta, GA
770-255-6043
dmims@cricpa.com

Text **CRI** to **66866** to receive CRI News and Alerts.

CARR, RIGGS & INGRAM, LLC