FIRMA National Conference – Optimizing the 2nd Line of Defense

May 12, 2021

TRUIST

© 2020 Truist Financial Corporation. Truist, Truist purple, and the Truist logo are service marks of Truist Financial Corporation.

Agenda

Agenda

1. Introductions – Anna Pray, 2nd Line Bank Compliance, and Charlie Durham, 2nd Line RIA Compliance
2. Three Lines of Defense
3. Independence and Objectivity
4. Business Fatigue
5. Optimization Tips

The speakers today are presenting their own views and opinions and not those of Truist Corporation.

Speakers

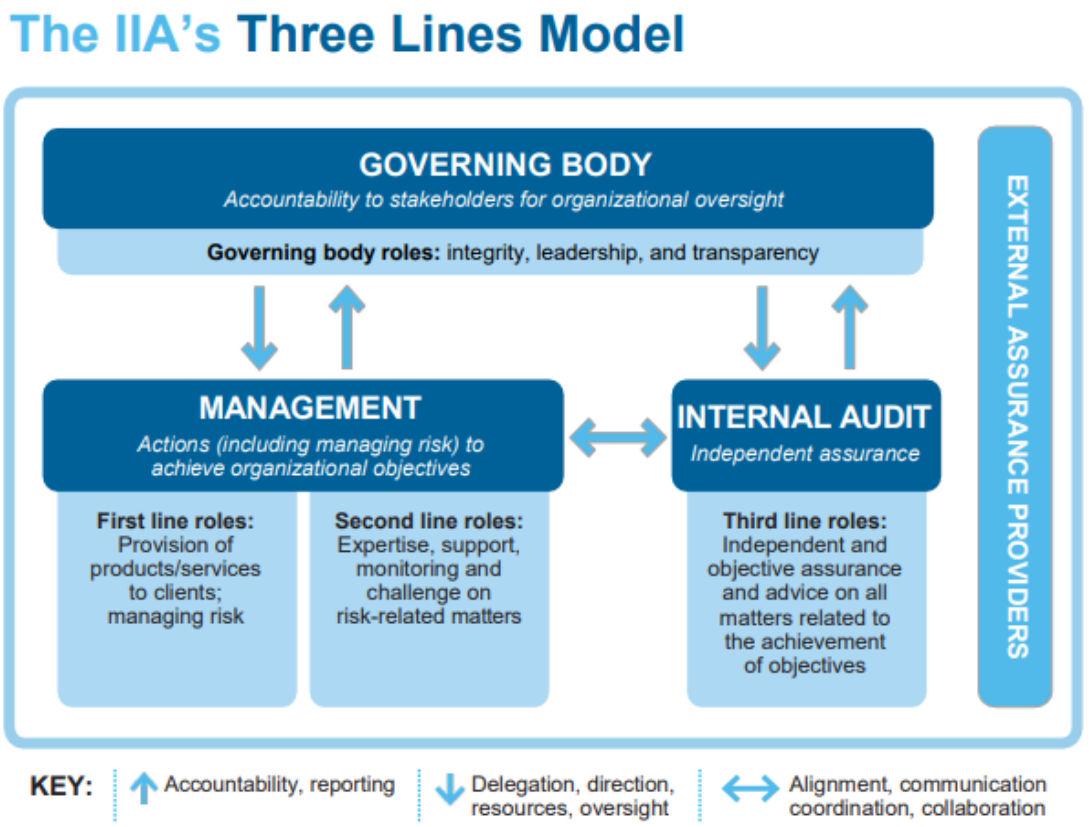
Anna R. Pray
TRUIST
Senior Vice President
Wealth Compliance Director
Louisville, Kentucky
anna.pray@truist.com

Charlie A. Durham
Sterling Capital Management
Chief Compliance Officer
Charlotte, North Carolina
cdurham@sterlingcapital.com

TRUIST

Three Lines of Defense

What is it?



The IIA's Three Lines Model: An Update of the Three Lines of Defense. July 2020

TRUIST

Where did it come from?

- The Great Recession highlighted deficiencies in risk management – identification, ownership, oversight.
- The 3 Lines of Defense clarifies risk management roles.
- The goal is to proactively uncover risks and either mitigate or accept those risks.

IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control. January 2013

Finextra. The Three Lines of Defense: Time to Recall the Kraken? By Richard Dupree. June 23, 2020

TRUIST

What does each line do?

1st Line Business Units

Ownership, strategy, execution, and accountability for identifying, assessing, controlling, mitigating, and communicating risks associated with business processes and decisions

2nd Line Risk Management

Provides independent oversight and challenge of risk management/taking activities of 1st line of defense includes governance, guidance, establishing policy, and monitoring, testing, surveillance.

3rd Line Audit

Provides assurance that risks are properly governed, identified, assessed and managed by 1st and 2nd lines of defense.

But what do they really do?

- The 1st line of defense is the team of players - the offense, defense, first string, second string. Like the Cardinals, they are trained, skilled, and ready to play the game.
- The 2nd line of defense is the coaching staff. The coaches provide guidance and input as the game is being played as well as between games.
- Audit Services are the analysts and they observe the game and review game film to identify ways in which the team can improve before the next game.

Same church, different pews. Compliance is the practice team getting the first line ready for Friday Night Lights (aka Audit and Examiners). First Line is offense and Second Line is defense.

TRUIST

Who are they?

1st Line

- Business Unit Risk Manager (BURM)
- First Line Risk
- 1st Line of Defense
- Risk

2nd Line

- Risk Management Organization (RMO)
- Second Line Risk
- 2nd Line of Defense
- Compliance
- Chief Risk Officers (CRO)
- Credit Risk
- Operational Risk
- Market Risk
- Liquidity Risk
- Technology Risk
- Strategic Risk
- Reputational Risk

3rd Line

- Audit Services

TRUIST

First Line

- The 1st line of defense is where risk is originated. Risk is inherent in all activities, client-facing and otherwise.
- Each business unit's 1st line risk group is responsible for identifying the risks inherent to their business and then assessing, controlling, monitoring, and reporting risk.
- 1st line engages in risk-taking activities, which include developing and implementing strategies to drive revenue opportunities and then takes ownership and accountability for business risks and control design/effectiveness to operate within the policies, standards, and limits set by the second line of defense.
  - 1st line escalates changes in the business or the risk environment that could affect the company's risk profile and control environment.
  - 1st line manages activities to meet strategic objectives within Risk Appetite.
  - 1st line identifies, measures, monitors, assesses, controls, and reports on risks associated within its activities.
  - 1st line provides input to, and then accepts, established Risk Appetite.
  - 1st line ensures business activities operate within policies, standards, and limits.
  - 1st line facilitates ongoing risk and control self-assessments to identify key risks and document, monitor, and evaluate control design & effectiveness.

Second Line

- The 2nd line of defense is formed by the Risk Management Organization (RMO) and provides independent risk management oversight and guidance to the 1st line across the enterprise. The RMO is responsible for ensuring risks are managed appropriately within a strong and comprehensive risk governance framework. Regulation interpretation and compliance oversight is included within the RMO responsibility.
- The 2nd line of defense is tasked with establishing the Enterprise Risk Management Framework and providing independent risk challenge and oversight of the 1st line of defense.
  - 2nd line establishes policies, procedures, processes, and standards to guide risk management execution.
  - 2nd line oversees the first line of defense's identification and assessment of current and emerging risks, as well as the effectiveness of processes and controls to manage risks.
  - 2nd line facilitates the integration of Risk Appetite within strategic planning processes.
  - 2nd line independently monitors (includes testing and surveillance), challenges, and reports on business unit alignment with the Risk Appetite Framework (RAF).
  - 2nd line independently escalates risk management gaps and issues.
  - 2nd line evaluates credit risk and the potential exposure to loss associated with managing credit products and processes.
  - 2nd line will identify, measure, monitor, assess, control, and report on risks within its own activities (separate from the business line).

TRUIST

Third Line

The 3rd line of defense is Audit Services. Audit Services provides independent and objective internal audit assurance for an organization. Audit Services is responsible for evaluating the design and operating effectiveness of the risk management framework, practices, and effectiveness of internal controls. Audit Services is accountable to the Board of Directors.

Compare and Contrast

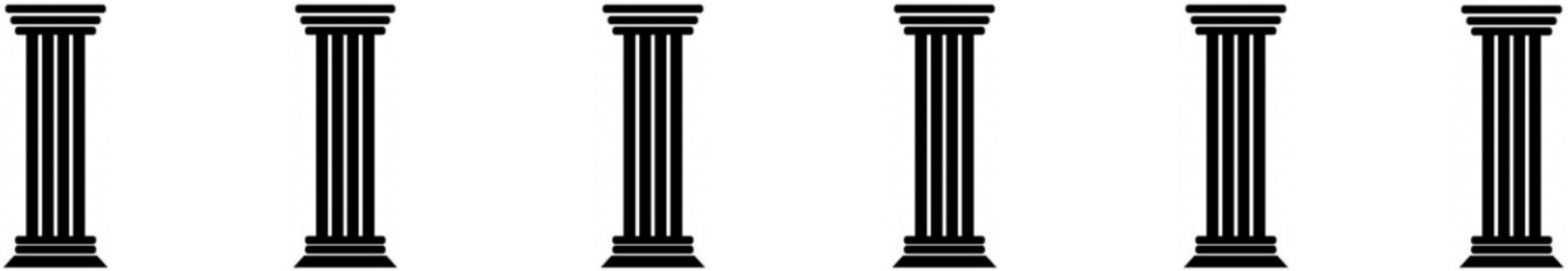
First Line Risk	Second Line Compliance
Owns and Manages Risk	Oversees Risk
Identify, assess, control, and mitigate risk	Monitor the implementation of risk management practices
Execute day to day risk and control procedures	Monitor adequacy and effectiveness of internal controls
Development of controls and supervise execution	Ensure first line is properly designed, in place, and operating as intended
Maintain internal controls	Monitor accuracy and completeness of reporting
When there are process or control issues, implement corrective action	Monitor timely remediation of deficiencies
Development of policies and procedure Guide the	Monitor non-compliance with applicable laws and regulations

Example from 2nd Line: Day to Day Compliance Activities

- We assist first line with solving issues that they raise
- We assist first line with solving issues that we raise
- We don't solve complaints, we review them for trends
- We don't draft policies and procedures, we monitor for compliance with established routines
- We don't draft policies and procedures, we evaluate if they are good enough to ensure regulatory compliance and adequate risk management
- We are not part of a process, we are not in the boxes and flow charts, we monitor if the process is working as intended, was developed correctly to produce results, and if the results are reducing risk adequately
- We monitor for process breaks – we see these in loss reports, issues management, hear about them in committees or from our business partners
- When there is a break, we ask what went wrong, how it happened, how did we not see it coming, and how we will prevent it in the future
- We monitor whether the line of business is staffed correctly to execute on their risk management plan
- We ask questions and effectively challenge was has been built by the first line
- We interface with regulators
- We report to Risk Management and Line of Business oversight through board and management committees
- We review and provide training related to risk management to the first line and alert first line to emerging issues and changes in the regulatory environment
- We alert the first line to emerging risks in the industry or within the company

TRUIST

Second Line Compliance Program Pillars



Regulatory Review & Analysis

Policies & Procedures

Risk Assessment

Monitoring & Testing

Training and Education

Compliance Corrective Action

- Compliance Training and Communications
- Governance Oversight including Committee & Board Advisory Support
- Compliance Policy Manual Governance and Management
- Annual Adviser and Funds Report of the Chief Compliance Officer
- Employee Personal Trade Surveillance
- Client Portfolio Compliance Monitoring
- Code of Ethics Monitoring and Reporting
- Compliance with Electronic Communications Retention Requirements

- Compliance Review of Marketing Material
- Conflicts of Interest Monitoring, Reporting and Disclosure Review
- Compliance Risk Assessment Process
- Compliance Testing and Monitoring
- Regulatory Reporting and Oversight
- Tracking and Reporting Regulatory Developments
- Anti-Money Laundering Control & Advisory Support
- Compliance with Record Keeping and Retention Requirements

TRUIST

Independence and Objectivity

Federal Reserve SR08-8, October 16, 2008, Rev 2/26/21

Compliance, Second Line, requirements related to banking organizations are suggested to be firm wide. The Federal Reserve recognizes that the guiding principles of all second line risk management is consistent across risk types, but can be particularly challenging related to compliance risk which does not lend itself easily to quantitative metrics.

The Federal Reserve emphasizes the need for firm wide risk management and oversight which they expect would take the form of:

1. A firm wide approach to compliance risk management and oversight;
2. Independence of compliance staff;
3. Compliance monitoring and testing; and
4. Delineation of board and senior management oversight responsibilities related to compliance risk

Over the 3 Lines of Defense

Board of Directors and Executive Leadership

- Provides oversight of the effectiveness of the Enterprise Risk Management Framework;
- Provides oversight of the management of Risk; and
- Approves Risk Appetite

Hallmark of 3 Lines of Defense - Independence

- The 2nd Line may independently identify issues and require the 1st Line to create documented action plans. Such issues/action plans may be tracked and reported as appropriate to oversight committees both for the 1st and 2nd lines.
- The 2nd Line provides independent oversight of the business units and applicable business committees, risk management processes/procedures, and execution to ensure compliance with corporate Policies and Risk Appetite.
- The 2nd Line also acts in a consultative role to assist business units in identifying risks, developing action plans to manage those risks, and monitoring execution.
- The 3rd Line will audit all parties.

Organizational Structure Example From Truist

Business Fatigue

Challenges With the 3 Lines of Defense

- The lines of defense may discourage collaboration. While clear responsibilities are necessary, more robust engagement between the lines of defense is critical to understanding and peer exchange.
- The lines of defense may create three levels of management over one issue – what is a priority for Audit, becomes a priority for Second Line, and then become a priority for the First Line.
- Inconsistent expectations or levels of skill or expertise may lead to the 2nd or 3rd line being too deferential or too restrictive.
- Insufficient emphasis on the first line's responsibility to manage risk and implement corrective actions.
- There is an inherent conflict in the first line between profit and risk. Surveillance and monitoring may find issues but likely that the more meaningful control is a culture that encourages challenge of risk behavior and speaking up.
- Culture can drive misconduct. If this is true, it is often missing from metrics which are mass produced by the three lines of defense.

TRUIST

Reuters – Three lines of defense – failed promises and what comes next by Erich Hoefer, Mark Cooke, Thomas Curry. September 8, 2020. Finextra. The Three Lines of Defence Time to Recall the Kraken? By Richard Dupree. June 23, 2020. Forbes. Three Common Problems With The Three Lines of Defense Framework by Frans Wiwanto. July 6, 2020.

Behaviors That Don’t Work

- Gotcha.
- Thinking you know it all.
- Unreasonable action plans.
- Too much focus on the academics of an issue.
- Too much rigidity.
- Using compliance lingo.

TRUIST

Reuters – Three lines of defense – failed promises and what comes next by Erich Hoefer, Mark Cooke, Thomas Curry. September 8, 2020. Finextra. The Three Lines of Defence Time to Recall the Kraken? By Richard Dupree. June 23, 2020. Forbes. Three Common Problems With The Three Lines of Defense Framework by Frans Wiwanto. July 6, 2020.

Behaviors That Do Work

- Full Disclosure.
- Talk early, talk often.
- “Hope” is not a plan.
- Be a partner, a teammate.
- Being flexible when you can.

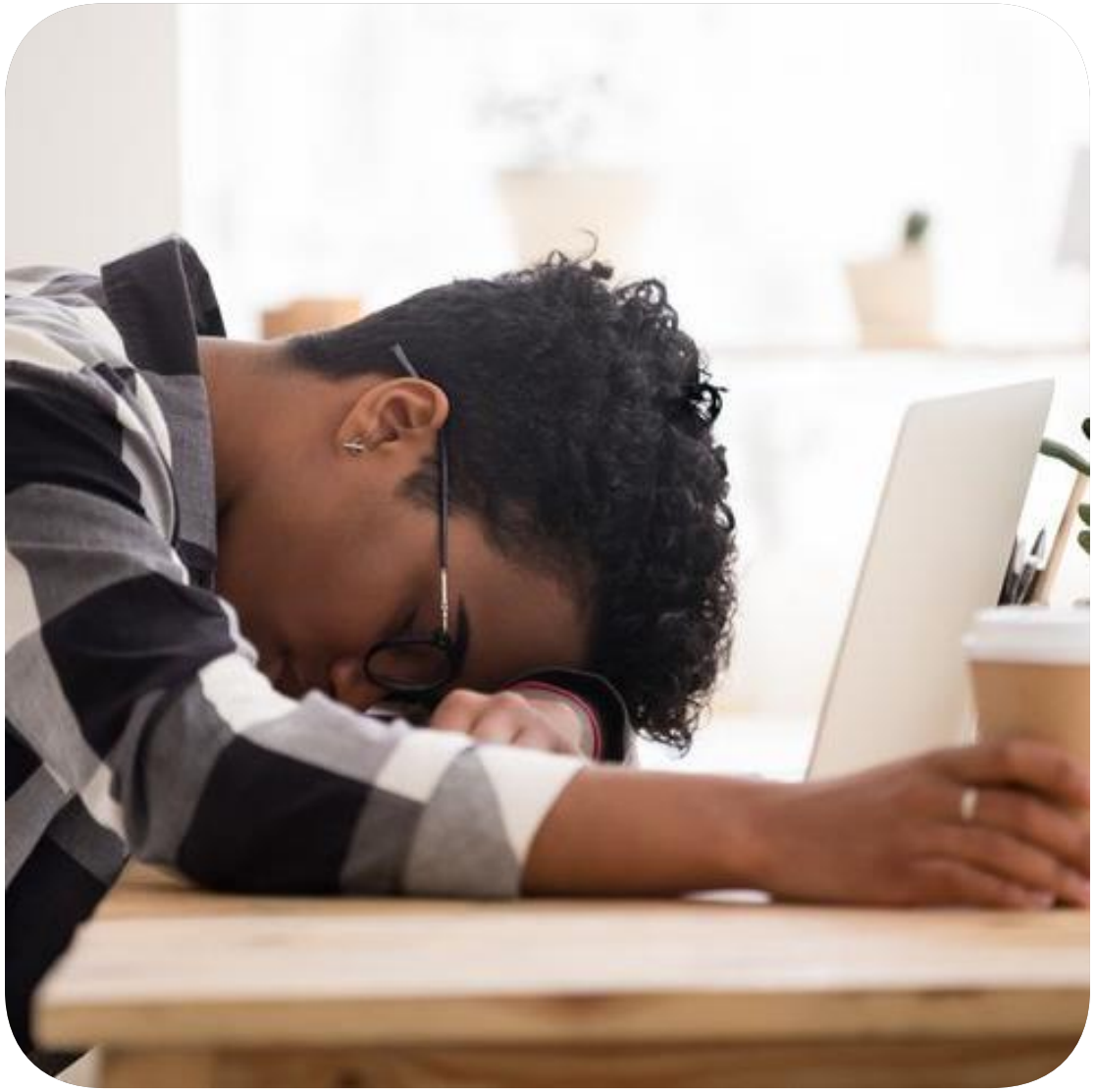
TRUIST

Reuters – Three lines of defense – failed promises and what comes next by Erich Hoefer, Mark Cooke, Thomas Curry. September 8, 2020. Finextra. The Three Lines of Defence Time to Recall the Kraken? By Richard Dupree. June 23, 2020. Forbes. Three Common Problems With The Three Lines of Defense Framework by Frans Wiwanto. July 6, 2020.

But Really? Three Lines?

Regardless of the challenges inherent in three lines of defense, examiners and regulators have an expectation to see this framework especially in the financial services industry.

Each organization strives to be agile, to proactively identify risks, and to change in reaction to the environment. Few achieve these goals, especially sizeable organizations, but there are some tips for best use of your lines of defense.



TRUIST

Optimization Tips

- **Line of business connection**
  - Know your line of business:
    - Who are they: review organizational charts.
    - What do they sell or produce: attend strategy and product meetings.
  - Reach out proactively, ask questions.
  - Attend meetings and listen instead of multi-tasking:
    - Prepare for meetings by reviewing the deck, even the appendix, ahead of time.
    - Prepare questions that you may have about how risk is being managed.
    - Be involved in working groups.
  - Know key projects for the business – their status and their risks.
  - Know key issues being managed.
  - Be responsive – be quick but thorough and thoughtful.
  - Be someone that can be relied upon to give good advice regardless of where you sit in the organization.

TRUIST

- **Learn**
  - Know the policies and procedures in your area and your supported area.
  - Know what regulators expect.
  - Keep up to date on industry trends.
  - Keep up to date on regulatory changes.
  - Join peer groups and keep up to date on the challenges for industry partners.
  - Talk to your business, compliance, and audit teammates and learn from them.
  - Don’t reinvent the wheel – do look in the organization for best practices and to ensure consistency.
  - Know the oversight structures, committees and working groups.

- **Don’t Wait**
  - Lean In
  - Be Engaged
  - Volunteer to Help
  - Ask Questions
  - Be Organized
  - Keep Notes
  - Create Risk Routines
  - Be Alert to Risk

Risk Management is not a passive endeavor.