Modern-Day Three Lines of Defense to Tackle Recent Compliance Challenges

A Financial Services Outlook
2023 and Beyond

ABSTRACT

The pandemic led to many changes in the financial services industry and everywhere else. Due to the rapid increase in digitization and the need to provide access to services remotely, the chances of fraud and inappropriate use of customer data have increased exponentially. That's why **regulatory authorities have become active in rolling out stricter compliance rules**, especially for financial services organizations, since they deal with money directly.

In 2022, different regulatory bodies in the U.S. have either proposed or announced the first draft of new **regulatory compliance rules related to consumer protection, financial inclusion, climate change, cybersecurity, and more**. In 2023, we can anticipate more refinement or finalization on many of these regulations. These new regulatory compliance rules will pose fresh challenges for financial services organizations and push them to adopt more stringent policies and frameworks.

In this e-book, we have enlisted the **top regulatory updates** on consumer protection, financial inclusion, climate change, and cybersecurity that will impact financial services businesses. These include:

- Community Reinvestment Act (CRA)
- Section 1071 of the Dodd-Frank Act
- Section 1033 of the Dodd-Frank Act
- Mandatory disclosures related to ESG by SEC
- Rule 10 for cybersecurity-related disclosure

Next, we have provided our perspective on the probable **solutions to deal with these new compliance** rules with the modern version of "**Three Line of Defense Model**," popularly known as the 3LD model and highlighted essential tips to modernize this model.

TABLE OF CONTENT

2023 – A Compliance Pressure Cooker

- Challenge 1 - Community Reinvestment Act (CRA)
- Challenge 2 - Compliance and Consumer Protection
- Challenge 3 - Climate
- Challenge 4 - Cybersecurity

Confronting Compliance Challenges

How Modernizing the Three Lines of Defense (3LD) Model can Help Manage Compliance Challenges

- The Modern Three Line of Defense Model
- Role of Internal Audit in Modernizing 3LD Model
- Modern First Line of Defense - Management
- Modern Second Line of Defense - Compliance and Risk Management Teams
- Modern Third Line of Defense - Internal Audit

Outcome of Implementing Modern 3LD Model

Key to Successful Implementation of 3LD Model - Optimizing Collaboration Between the Three Lines

Conclusion: Augment the 3LD Model with Technology to Overcome Compliance Challenges

2023: A Compliance Pressure Cooker

As we gradually move past the most severe impacts of the COVID-19 pandemic and adapt to a "new normal" in business operations, there is little respite in alleviating the burdens of actual and anticipated regulatory changes in the financial services industry.

The demand for banks and other financial service providers to demonstrate effective and sustainable risk management remains intense as regulators increasingly seek more significant levels of accountability and enforce stricter measures. Furthermore, the ongoing effects of the pandemic, marked by its evolving unpredictability, continue to contribute to the rapid pace of change within the banking sector.

Additionally, other significant global events further contribute to this climate of uncertainty. As we enter the second quarter of 2023, various initiatives are already underway that could present significant risk-related challenges for financial institutions.

The next section presents the regulatory outlook for 2023 with the top compliance challenges.

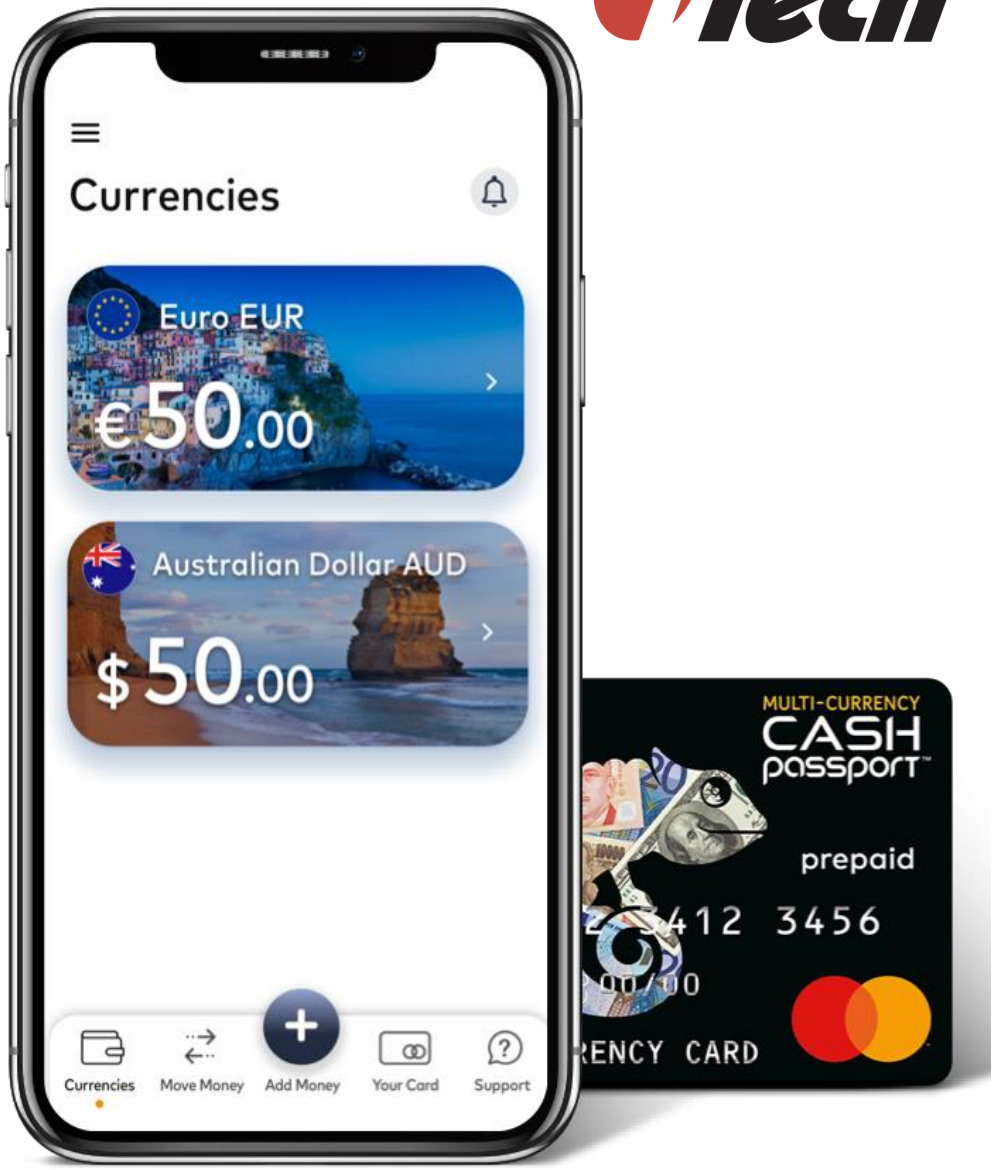
Challenge 1
Community Reinvestment Act (CRA)

This rule's finalization is anticipated through interagency collaboration in **2023.** As a result, significant modifications will be made to the information considered during evaluations based on the size of an entity and the assessment of that information.

The proposed amendment to the Community Reinvestment Act **(CRA) regulation acknowledges the diminishing significance of geographical banking boundaries** and **promotes the expanded use of digital banking through mobile applications**.

These advancements will likely lead to more accurate CRA assessments for financial institutions and improved evaluation outcomes as their activities align with the actual service area.

Another noteworthy change is the inclusion of a new category called the "Retail Services and Products Test," which will necessitate the acquisition of data-gathering capabilities that may currently be lacking within specific institutions.



Challenge 2
Compliance and Consumer Protection

On March 30, 2023, the CFPB released its final rule implementing Section 1071 of the Dodd-Frank Act. In accordance with Section 1071, the final rule **will mandate financial institutions to gather and furnish data to the Bureau regarding loans extended to small businesses.** These small businesses are defined as entities that recorded gross revenue below $5 million in their most recent fiscal year, and the Bureau will subsequently make this information publicly available.

The rule mandate various types of financial institutions to reveal data related to the race, ethnicity, and gender of small business loan recipients. Additionally, these institutions are required to disclose geographic information, lending decisions, and credit pricing details. All the credit application details will be consolidated into a comprehensive database that will be **accessible to the public.**

Also, on March 30, 2023, the Consumer Financial Protection Bureau (CFPB) published a final report prepared by the Small Business Review Panel, which assesses the impact of the Bureau's proposals concerning consumers' rights to access their personal financial data.

Challenge 3
Climate-related Financial Risks

The Securities and Exchange Commission (SEC) was expected to propose mandatory disclosures related to Environmental, Social, and Governance (ESG) factors, including climate change in 2022, which was pushed to April 2023 and has not been announced yet. However, it is highly likely that the SEC will issue a final rule in 2023.

In 2022, the Financial Stability Oversight Council (FSOC) established the Climate-related Financial Risk Advisory Committee (CFRAC) and established the Office of Climate Risk (OCR). In 2023, **CFRAC and OCR are anticipated to enhance industry comprehension of the impacts of climate-related financial risks and explore optimal risk management strategies**.

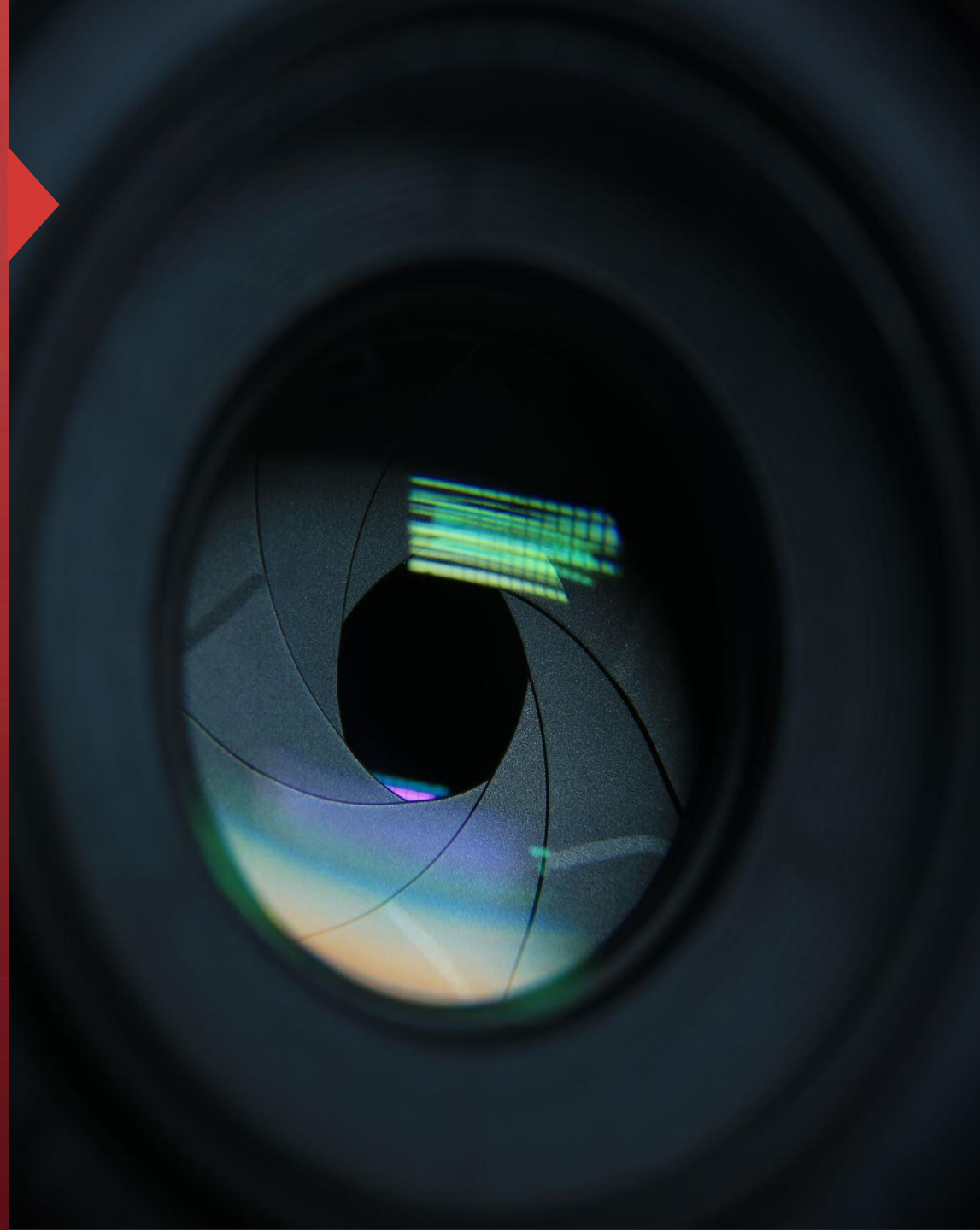
Furthermore, the Office of the Comptroller of the Currency (OCC), Federal Reserve Board (FRB), and Federal Deposit Insurance Corporation (FDIC) are expected to take definitive measures to finalize the draft Principles on climate-related financial risk management in 2023, particularly for large financial institutions. Additionally, the New York Department of Financial Services (NYDFS) will carefully evaluate the feedback received from stakeholders on the proposed Guidance on Management of Material Financial Risks from Climate Change.

Challenge 4
Cybersecurity

Continuing its momentum, the Securities and Exchange Commission (SEC) acted in March 2023 to extend the comment period for proposed rules and amendments pertaining to cybersecurity risk management and disclosure concerning registered investment advisers, registered investment companies, and business development companies.

The Securities and Exchange Commission (SEC) introduced a proposed regulation known as **Rule 10**. This rule would **mandate entities responsible for providing essential services to tackle their cybersecurity risks proactively**. Rule 10 explicitly targets "market entities" such as broker-dealers and national securities exchanges, necessitating them to develop, uphold, and enforce written policies and procedures reasonably designed to address their cybersecurity risks.

In the event of adoption, **Rule 10 would necessitate market entities to disclose cyber risks and incidents to the Securities and Exchange Commission (SEC)** using a designated "Form SCIR," with certain portions of the form made publicly accessible. Also, in 2023, NYDFS will repropose **a revised version of the Cybersecurity Regulation or adopt the final regulation**.



How Do We Approach

Confronting Compliance Challenges

When prioritizing **consumer protection and financial inclusion**, Financial institutions needs to

- Evaluate legal agreements and risk oversight pertaining to non-banks, and document these arrangements' impact on the bank's risks, controls, and other processes.
- Review their Third-Party Risk Management (TPRM) oversight program to ensure a comprehensive understanding of consumer compliance risks and requirements.
- Assess their data collection, aggregation, reporting, and analytics capabilities to meet the new requirements of regulations such as CRA, 1071, and 1033, as well as the increasing expectations in other areas.
- Ensure their change management programs operate effectively and extend beyond new product offerings to include significant operational changes, regardless of the cause.
- Conduct fair lending assessments to identify potential instances of discrimination beyond lending activities, considering the principles of unfairness.

How Do We Approach

Confronting Compliance Challenges

When addressing **climate-related financial risk**, Financial institutions needs to

- Recognize any inconsistencies in requirements across regulators with supervisory oversight responsibilities and incorporate the collective expectations into operational processes.
- Review existing scenario analysis frameworks to ensure alignment with proposed principles and draw insights from international best practices to enhance current approaches.
- Evaluate the stipulations outlined in all relevant guidance, both final and proposed, to identify areas where the requirements surpass existing risk management practices or necessitate implementing new policies, procedures, and limits.
- Establish an approach for acquiring, maintaining, and reporting data to facilitate scenario analysis and other data-driven risk management activities.

How Do We Approach

Confronting Compliance Challenges

When addressing the **risks associated with cybersecurity and information technology (IT)**, Financial institutions needs to

- Involve the board and senior leadership during and after a cybersecurity incident, ensuring adequate processes and controls to assess the severity of the incident in light of the Computer Security Incident Notification Rule.
- Conduct a reassessment of existing critical third-party relationships to ensure the implementation of appropriate ongoing monitoring measures.
- Assign cybersecurity board responsibilities to a dedicated board committee with a clearly defined mandate and directors possessing relevant IT-related skills, as necessary.
- Implement a robust policy management program that accommodates more detailed changes in laws, regulations, practices, and supervisory expectations. Regularly evaluate its efficiency, and update it as needed to ensure effective integration with IT architecture, IT risk assessments, and broader considerations of financial crime.

How Modernizing the Three Lines of Defense Model can Help Manage Recent Compliance Challenges Better

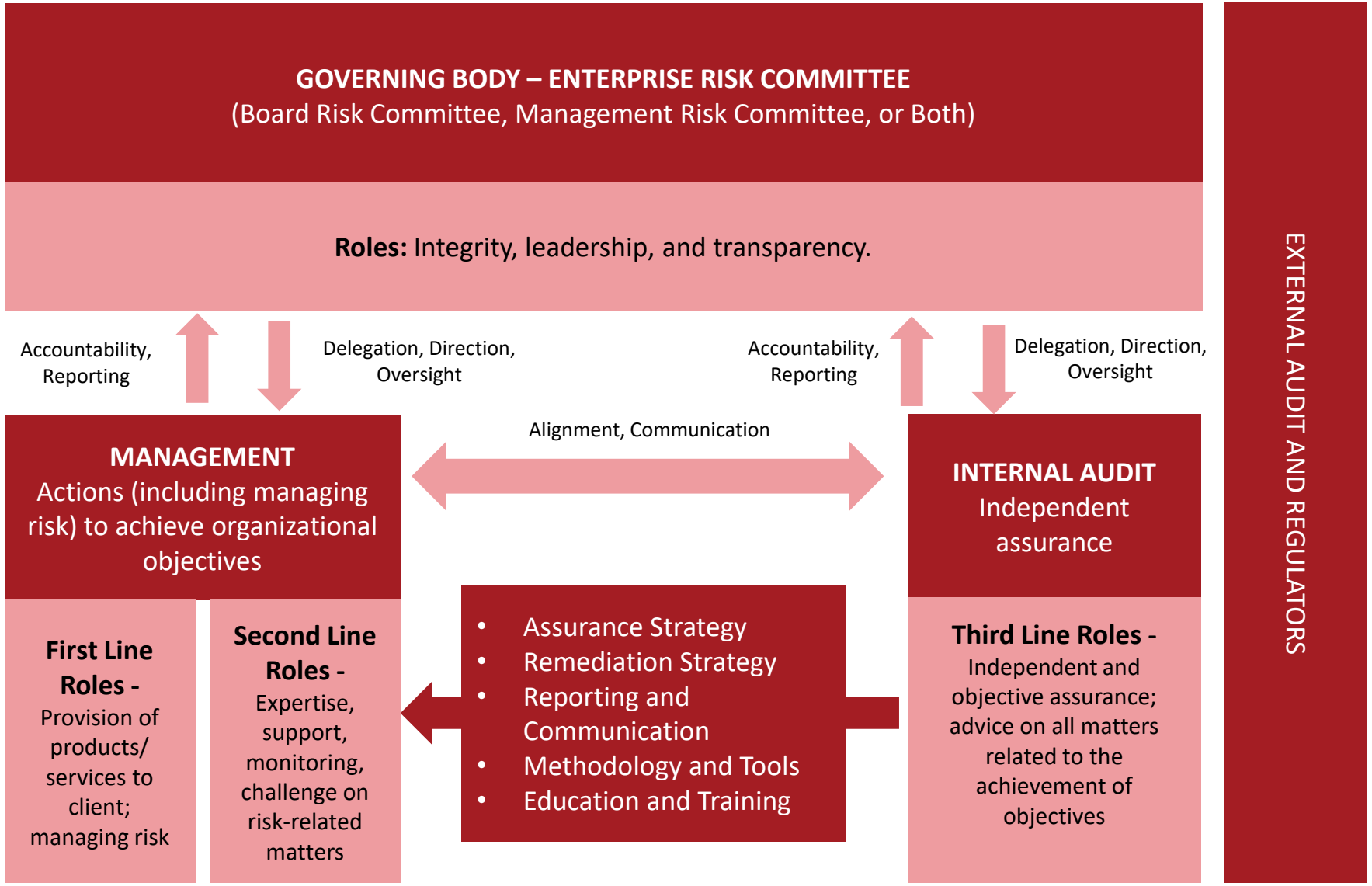
The concept of the "three lines of defense" has long served as a fundamental framework for implementing risk management programs across various industries and over time.

The Institute of Internal Auditors (IIA) has played a crucial role in offering valuable guidance on this framework, initially in 2013 (referred to as the "2013 Guidance") and later with updated guidance in July 2020 (referred to as the "Three Lines Model").

The three lines of defense (3LD) establish a structured approach to risk management and internal controls within an organization. It involves defining clear roles and responsibilities in different areas and establishing the relationships between these areas.

In the next section, we present our approach to modernizing the 3LD model.

The Modern Three Line of Defense Model



Role of Internal Audit in Modernizing 3LD Model

Amid growing regulatory pressures and the recognition by businesses to improve efficiency and effectiveness, we are witnessing a reinforcement of all three lines of defense. This drive originates from the board's emphasis on emerging risks and core control practices.

- The first line assumes an active role in risk management within its domain, with some organizations beginning to integrate first-line control monitoring.
- Risk functions adopt a forward-looking approach to assess emerging risks, scanning the horizon and employing key risk indicators to identify potential control weaknesses. They collaborate with management to enhance control designs.
- Compliance functions, in addition to advising on new regulatory risks and formulating related policies, conduct increased regulatory monitoring reviews that encompass testing of regulatory controls.

Consequently, internal audit (IA) functions find themselves conducting risk-based assurance reviews over the same risk areas as the second line, often with a similar skill set, leading to duplicative assurance activities across the three lines of defense.

While these actionable and strategic measures aim to drive the evolution of the three lines of defense, there have been negative side effects for more mature models. The first line can experience audit fatigue due to redundant testing from both the second and third lines, leaving them with limited time to focus on core business activities. Moreover, there are instances where an overemphasis on the second line's role leads the first line to reduce their own responsibilities. In times of crises, organizations can often succumb to the temptation of overreacting, leading to the inclusion of additional tasks and responsibilities for both the second and third lines.

In such situations, the third line (Internal Audit) is best positioned to help organizations avoid impulsive reactions and contribute to drafting a measured response that prioritizes risk, pragmatism, and practicality.

Modern First Line of Defense

Management

The initial level of protection is managed by business and process owners. It is the responsibility of operational management to uphold efficient internal controls and carry out risk and control procedures in their daily operations.

This entails identifying and evaluating controls, as well as mitigating risks. Moreover, business and process owners play a crucial role in directing the creation and adoption of internal policies and procedures, ensuring that activities align with the goals and objectives of the organization.

Middle-level managers may devise and implement specific procedures as controls, overseeing their execution by their staff.

Internal Audit (IA), given its prominence within an organization, holds a favorable position to aid first line in assuming greater control ownership and incorporating self-assurance mechanisms. While IA cannot solely rely on the efforts of the first line, it can leverage monitoring results, conduct agile testing of controls, and deliver assurance and guidance on the most significant risks.

To accomplish this, IA needs to elevate itself as a strategic and comprehensive assurance provider and risk advisor. It must collaborate with other departments and actively participate in the decision-making process from an early stage.

Modern Second Line of Defense

Compliance and Risk Teams

The second line of defense plays a crucial role in assisting the organization's management in efficiently managing risk and controls. Management sets up various risk management and compliance functions to provide support for the implementation and supervision of controls in the first line of defense. Essential functions in the second line include:

- A risk management function or committee that facilitates and monitors the adoption of effective risk management practices by operational management. It also assists risk owners in defining the desired level of risk exposure and provides comprehensive risk-related information across the organization.
- A compliance function that oversees specific risks, such as noncompliance with laws and regulations. This function operates independently and reports directly to senior management.
- A controllership function that monitors financial risks and issues related to financial reporting.

Through the utilization of advanced technology, the second line can modernize operations to enable real-time monitoring. Although IA cannot depend entirely on the second line, it can utilize monitoring outcomes, perform agile control testing, and provide assurance and guidance regarding the most critical risks.

To achieve this, IA must position itself as a strategic and all-encompassing provider of assurance and a risk advisor. It is crucial for IA to collaborate with other departments and engage actively in the decision-making process right from the initial stages.

Modern Third Line of Defense

Internal Audit

The third line of defense offers assurance to senior management and the board regarding the alignment of the first and second lines with established expectations. The key characteristic that sets apart the third line is its notable degree of organizational independence and objectivity.

- While Internal Audit does not directly manage or execute processes, it can provide guidance and recommendations on process-related matters.
- Furthermore, an Internal Audit may assist in enterprise risk management without implementing or performing risk management activities beyond its own function.
- Internal auditors achieve their goals by applying a systematic approach to assess and enhance the effectiveness of risk management, control, and governance processes.

In preparation for the upcoming challenges, it is crucial for management, risk, compliance, and internal audit to be receptive and actively seek more efficient ways to collaborate on activities related to internal controls management. Regulators tend to link failures in risk management within one area of the business to weaknesses in the other two areas, and they will hold individuals and groups accountable for control failures.

In order to be perceived as safeguarding, constructing, and maintaining value, IA must genuinely provide assurance, advice, and foresight. The modern IA will actively engage in educating stakeholders and sharing valuable tools, insights, and knowledge. IA functions that demonstrate an adaptable and forward-thinking mindset are likely to receive positive recognition from key stakeholders. While the level of maturity may differ among IA groups in various organizations, the crucial step is to identify current inefficiencies within the organization's three lines of defense (3LD) model and promote innovative and strategic measures. Innovation should encompass more than just technology and include improvements in coordination, communication, audit and risk assessment methodologies, as well as fostering stronger connections and engagement with first- and second-line stakeholders. With a broader vision, IA will be better positioned to enhance its influence and proactively prepare for future challenges and opportunities.

Outcome of Implementing Modern 3LD Model

Sustained CRA Performance Amidst Changing Dynamics

- The CRA poses a two-fold challenge of implementing a new rule (when it is released) while maintaining performance levels under the current rule. Modern 3LD model prioritize the current performance as examinations will continue to be conducted based on the existing rule for at least one more cycle. Also, it encourages assessing program and make necessary adjustments to adapt to these circumstances.

Effective Management of Mergers and Expansions

- If your organization is considering a merger, acquisition, or expansion in the financial industry, it is crucial to analyze your HMDA and small business lending data. With the Modern 3LD Model, you can understand what this data reveals about your institution, including any indications of bias. It helps evaluate your CRA performance, identify weaknesses, and devise strategies to address them. Additionally, it assess the target institution's BSA/AML program for any existing gaps or issues.

Enables Active Involvement with Product Leaders

- Modern 3LD Model encourages engaging in discussions surrounding product changes, new products, and innovation within your organization. During times of economic strain, financial institutions often seek new revenue streams through innovative means. However, it is important for Compliance and Risk management professionals to participate in these discussions actively.

Ensures Effective Risk Assessment Process by

- Conducting a thorough and up-to-date risk assessment and utilizing it effectively.
- Ensuring the risk assessment covers areas such as Fair Lending, Third Party Risk, UDAAP, the entire product life cycle, BSA/AML, and cybersecurity.
- Accurately evaluating the inherent risk considering business conditions and economic factors; avoiding downplaying the inherent risk.
- Determining your institution's risk appetite in the current environment.

Outcome of Implementing Modern 3LD Model

Continued...

Enhanced Compliance Program Management

- Increases the utilization of automation for monitoring, analyzing, and implementing regulatory changes to reduce errors and inconsistencies inherent in manual processes.
- Helps in analyzing consumer complaint activity, including internal records and the CFPB database, to identify emerging risks.
- Assists in customizing monitoring and testing efforts to focus on areas with the highest risk as identified in the risk assessment.
- Establishes a precise mapping of the regulatory inventory to related elements of the compliance program, such as products, services, policies, procedures, risks, controls, and training.
- Evaluates program effectiveness using the DOJ Sentencing Guidelines: Evaluation of Corporate Compliance Programs.

Effective Management of Regulatory Change

- Helps in utilizing the provided regulatory implementation periods fully. Organizations often delay taking action immediately, so it is crucial not to waste valuable time.
- Establishes clear accountability and responsibility throughout the organization for effectively implementing upcoming significant regulatory changes, particularly the 1071 regulations.
- Determines who will take ownership of the implementation process and identifies the ultimate accountable party.
- Develops a comprehensive action plan and ensures its progress is actively tracked.
- Helps in documenting the entire implementation process from start to finish.
- Engages relevant stakeholders, including IT and Operations, to ensure their involvement and collaboration.
- Helps in defining the testing procedures required to control risks effectively.
- Promotes providing monitoring reports to the Executive team and Board of Directors regularly to keep them informed.

Key to successful implementation of 3LD Model

Optimizing Collaboration Between the Three Lines

There are different routes audit, governance, risk, and compliance functions can take to begin addressing the collaboration challenges. To initiate a fruitful alliance, the first crucial step involves the teams mutually committing to enhancing methods of cross-collaboration. All stakeholders should agree and understand that optimizing collaboration is a business imperative to add more value to the organization ultimately.

Transforming this shared aspiration into tangible outcomes can effectively trigger the process of augmenting collaboration. Of course, being able to quantify the impact on the overall cost of compliance will always help in fostering additional buy-in. Through collaborative efforts, audit, governance, risk, and compliance teams come together to develop shared resources, such as a universal risk library and risk methodology. To foster collaboration among risk, compliance, and audit teams, the following activities can be undertaken:

- Implementing a universal catalogue for risks and controls to ensure consistency of information, minimize confusion, and eliminate redundant data.
- Adopting a standard methodology for assessing and addressing issues and risks, enabling streamlined reporting and analysis.
- Transitioning risks, controls, and issues data from fragmented systems and outdated tools to a centralized record-keeping system. This should include an integrated mechanism for tracking open issues across the organization.
- Creating an assurance map to identify gaps and overlaps in assurance activities.
- Developing a unified strategy for assurance to streamline risk management processes across all three lines.
- Establishing a standardized risk taxonomy, along with clear definitions and criteria for ranking risks.

Conclusion

Augment the 3LD Model with Technology to Overcome Compliance Challenges

The pandemic has exposed the risk and vulnerabilities of providing quick online access to services. As the world embraces the "new normal," these vulnerabilities will be further exploited. In response, new and stringent compliance rules would be issued by regulatory authorities, especially for financial services organizations. While businesses can deal with each of these fresh regulations individually and on a case-to-case basis, the best practice is to implement the 3LD model that provides the framework to deal with any current and future risk and compliance obligations.

However, to successfully implement the 3LD model, there is a mandate for the three lines to collaborate so that a single, standard, comprehensive library of risk definitions can be formed. Building such a centralized library of risk data by cutting across organizational silos is only possible by deploying integrated risk management software like IBM OpenPages with Watson. It helps organizations establish a centralized risk and compliance data library and enables leaders to make informed decisions for their risk and compliance initiatives.

For more information on how implementing IBM OpenPages can help you manage compliance challenges, write an email at **reachout@iTechGRC.com** or submit your contact details **here**.

References

- https://www2.deloitte.com/us/en/pages/regulatory/articles/banking-regulatory-outlook.html
- https://www2.deloitte.com/us/en/pages/advisory/articles/modernizing-the-three-lines-of-defense-model.html
- https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/a-best-practice-model-for-bank-compliance
- https://www.wolterskluwer.com/en/expert-insights/the-10-cs-revisited-what-to-expect-and-what-you-need-to-do
- https://www.v-comply.com/blog/what-are-the-banking-regulatory-trends-of-2023/
- https://assets.contenthub.wolterskluwer.com/api/public/content/a816db29a88a4bce9e340b0409ed4dfb?v=bc4d46d1&_gl=1*1w3tkpf*_ga*MTU4OTcwMjI4MS4xNjg1NjQwODky*_ga_7DJGBC7BG3*MTY4NjEzOTEwMy4xLjEuMTY4NjEzOTEwNy4wLjAuMA..
- https://nycscouting.org/yptstandards/#:~:text=Adult%20Registration%20Requirement%20to%20Take%20Effect%20September%201%2C%202023&text=(Effective%20September%201%2C%202023),in%20every%20unit%20serving%20females.
- https://buckleyfirm.com/blog/2023-03-31/cfpb-finalizes-section-1071-rule-small-business-lending-data
- https://www.wolterskluwer.com/en/know/regulation-1071
- https://buckleyfirm.com/sites/default/files/InfoBytes%20-%20CFPB%20SBREFA%20Report%20re%20Section%201033%20Proposals%202023.03.30.pdf
- https://www.lexology.com/library/detail.aspx?g=b141ad3c-dd94-4322-98c8-4d1aa80c9af2
- https://www.reuters.com/legal/legalindustry/sec-is-inching-closer-clarity-cybersecurity-requirements-2023-04-19/#:~:text=2023%20new%20rule%20proposals&text=Under%20Rule%2010%2C%20%22market%20entities,to%20address%20their%20cybersecurity%20risks.
- https://www.occ.treas.gov/topics/supervision-and-examination/climate/index-climate.html
- https://www.dfs.ny.gov/industry_guidance/climate_change#public-feedback
- https://www.globalfinregblog.com/2023/01/nydfs-proposes-guidance-on-climate-change-risk-management/
- https://www.apra.gov.au/sites/default/files/2021-11/Final%20Prudential%20Practice%20Guide%20CPG%20229%20Climate%20Change%20Financial%20Risks.pdf
- https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/sec-climate-disclosure-rule-delayed-until-fall-former-commissioner-says-75479173
- https://www.icas.com/professional-resources/audit-and-assurance/internal-audit/internal-audit-three-lines-of-defence-model-explained
- https://www.bdo.co.uk/en-gb/insights/advisory/risk-and-advisory-services/the-three-lines-of-defence-model-has-been-updated-what-does-this-mean-for-heads-of-internal
- https://www.iansresearch.com/resources/all-blogs/post/security-blog/2022/01/13/how-to-apply-the-three-lines-of-defence
- https://guidehouse.com/insights/financial-services/2021/public-sector/garp-three-lines-of-defence
- https://www.erm-academy.org/publication/risk-management-article/three-lines-defence/
- https://internalaudit.olemiss.edu/the-three-lines-of-defence/