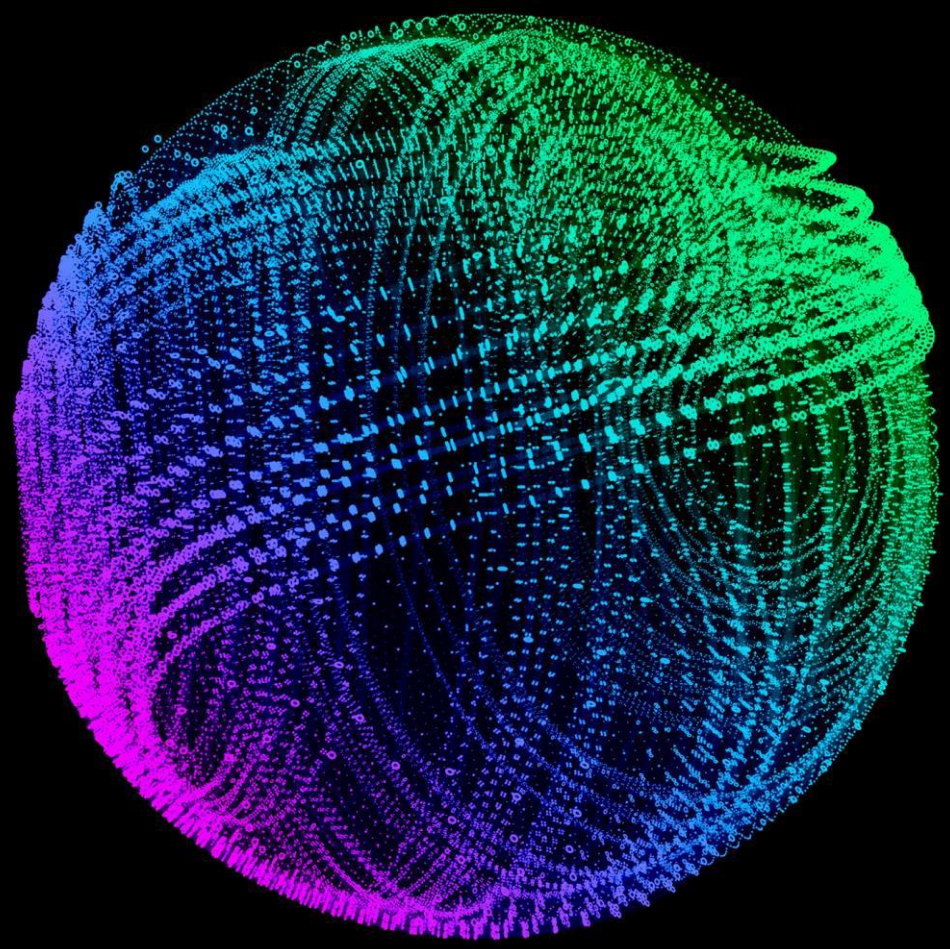
Deloitte.



Back to Basics - Lessons learned from recent governance, risk, and control failures

Deloitte Point of View

October 2021

Executive summary - Back to basics

Global and local financial regulators have reinforced their requirements for robust governance, risk management, and controls since the financial crisis in 2008 through new regulations, supervisory guidance, and focused examinations and inspections.

Several recent governance, risk management, and control failures in the financial services industry have made headline news, resulting in nearly $14 billion[1] in financial impact and public enforcement action. These events signal that organizations have not done enough to protect themselves from risks arising from cross-border businesses and legal entities, as well as to operationalize core risk management frameworks, principles and requirements within the operating model and culture of their organizations.

This point of view synthesizes the most impactful themes from the recent incidents and regulatory actions, and offers practical recommendations on what the Board, Senior Management, including business and risk functions, can do to immediately evaluate and address the types of vulnerabilities that led to these incidents.

It's time for an industry call to action to ensure foundational risk management and governance expectations are implemented and operational. In many respects, this is "back to basics". Urgency of actions should be calibrated to the size and complexity of the organization.

[1]Estimated regulatory settlements and operational losses (including implicit costs such as cost of remediation, business interruption, loss of customer confidence, and others) incurred by G-SIBs and other select risk incidents occurring from January 2020 to August 2021. This point of view has intentionally omitted reference to specific events or company names.

Thematic pain points:

- **Ownership and accountability are unclear** due to poorly defined roles and responsibilities, resulting in mismanagement of risk
- Management and staff are **under-resourced** and face unrealistic 'dual-hatting' of responsibilities; 3LoD operating models aren't providing the first line adequate resourcing to own and manage risk
- Governance structures and processes are ineffective and lack end-to- end enterprise connectivity including **lack of alignment between business strategy, risk and capital management**
- **Risk appetite and risk breaches** are not credibly governed
- Extent of risk is not always evident, notably amongst complex **cross-border and intra-business transactions** and relationships
- **Risk reporting and processes fail to 'connect dots'** across multiple business relationships at the enterprise-level
- **Incentives to manage risk safely are not credibly embedded in organizations' performance management processes**; reporting and escalation challenges limit the Board's ability to hold front office units accountable

Practical levers for change:

- Facilitate **credible and periodic testing of stress points/conflicts** amongst Senior Management against **realistic 'dual-hatting' guidelines**
- Incorporate front office **staffing/management composition trends in risk governance reporting**
- Redefine risk appetite and breach governance processes including **bright-line boundaries and decision-making protocols**
- **Re-engineer the incentive structure by embedding risk allocation metrics in compensation** and performance decisions
- Evaluate tactical and longer-term adjustments to **risk architecture, processes, and controls to ensure business risk reporting is prepared, monitored, and used for decision making/challenge**
- Balance global versus **regional and legal entity governance processes** and ensure transparency of cross-border risk, for global institutions
- **Enhance infrastructure and invest in improved processes, controls** to allow management to focus on managing risk, driving revenue

Regulatory guidance and trajectory

US regulators' expectations for **governance, risk and compliance management** have been clear since before 2008 and are included in key regulations. The regulators expect by now, that these requirements are **fully business as usual** and **effective** for consideration to be ***"well-managed"***

Start: 2008-2012

Financial crisis aftermath paves the way for legislation - *Dodd-Frank Wall Street Reform and Consumer Act* (July 2010) mandated regulators to issue "enhanced prudential standards" (EPS) regulation

FRB *proposes EPS rule-making* for US BHCs (12/2011) and FBOs (12/2012)

FRB issues supervisory guidance, (SR 12-17 – Consolidated Supervision Framework for Large Financial Institutions)

2012-2016

FRB finalizes EPS for US BHCs and FBOs (February 2014) with *implementation* (July 2015 and July 2016) respectively

OCC proposes Formal Guidelines for Heightened Standards for Large Banks (January 2014); OCC finalizes into *Part 30, Heightened Standards,* solidifying risk regulations

2016-2019

FRB proposes Board/corporate governance and a new Large Financial Institution Rating (August 2017), including a *Governance and Controls rating*

FRB proposes *risk management expectations* - Board, senior management, business lines, independent risk management, internal audit (January 2018)

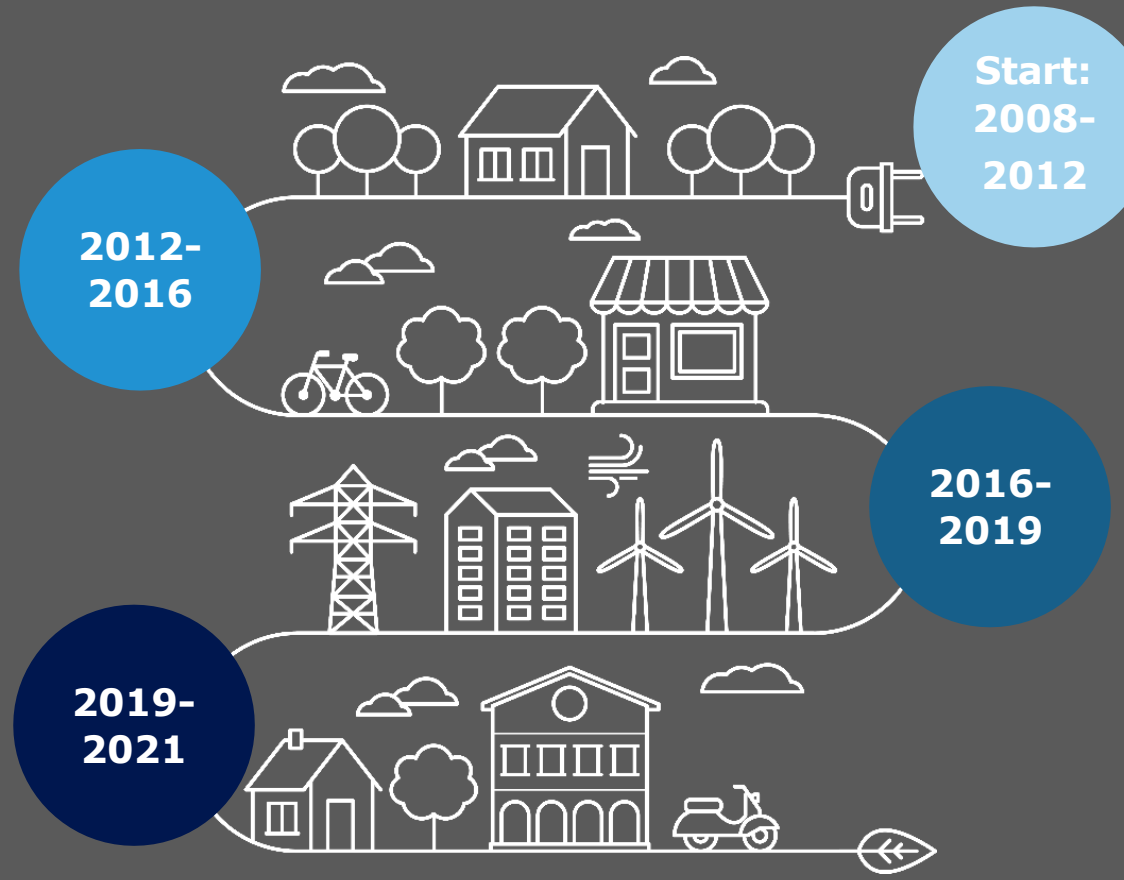
FRB finalizes Large Financial Institution Rating for 2019 ratings cycle (November 2018)

2019-2021

Post 2017, Congress passes *Economic Growth, Regulatory Relief, and Consumer Protection Act; revising Dodd Frank;* "tailoring of EPS requirements" based upon size, scale, risk profile

FRB, OCC, and FDIC finalize *tailoring* (October 2019) *prudential standards* (no impact to US GSIBs)

FRB Supervisory SR 21-3 / CA 21-1 guidance on Board Effectiveness (February 2021)



Were these requirements operationalized? Can you demonstrate traceability and effectiveness of governance, risk and compliance management over business operations?

Industry pain points (1/2)

Despite years of effort and investment by many institutions, several pain points remain issues for organizations. Pain points are both top-down given **overall lack of effective risk governance, accountability, and ownership** from the Board to Senior Management and across independent risk/compliance and internal audit; as well as **horizontal** across the enterprise, due to a **lack of meaningful risk culture and effective risk processes, staffing models, infrastructure and frameworks that incentivize sound risk decisions and provide the full risk picture.**

Unclear accountability & ownership

- **Lack of escalation and awareness of risk-related issues** to and from the Board and Senior Management
- Lack of resource planning along with **expense management pressures have resulted in loss of staffing/skillsets, de-leveling and "over-extended managers"**
- **Management and risk staff typically have many roles** (e.g., C-suite members are **'multi-hatted'** across entities or regions), leading to conflicts of interest
- **Business management and front office staff have an insufficient understanding of how to effectively carry out necessary risk responsibilities**
- Organizations fail to maintain an **effective three lines of defense operating model** and a **formal accountability framework**

Lack of enforcement of risk appetite, limit breaches, escalations

- **Formal risk appetites** defining risk limits and thresholds metrics **are not appropriately established** to holistically assess risks across businesses and legal entities
- **Organizations take accommodative approaches to risk** often with first line influence leading to **inadequate responses to risk limit breaches** (e.g., breaches are dismissed, overridden and/or not escalated)
- **Client trading strategies, counterparty risks, and conflicts of interest are not holistically monitored**, leading to persistent limit breaches
- Organizations **fail to operationalize risk management standards and limit frameworks** across **siloed business functions and legal entities**

Inconsequential risk culture, performance management

- Incentives to safely manage risk are **not embedded in the culture of the firm** (e.g., performance metrics are not prioritized for risk-related responsibilities)
- There are significant **deficiencies in risk culture**, including a **lack of self-improvement and self-awareness,** top-down and bottoms-up
- Personnel have **casual attitudes** towards risk discipline, **lack accountability** for risk failures, and **fail to escalate** risk-related matters often out of fear that they may not be supported

Industry pain points (2/2)

Under-investment in risk data & architecture

- **Lack of alignment between their technology and data strategies; strategies are silo'd and lack a front-to-back approach.** Tech strategy for risk and control aren't fully incorporated into first line risk and operational systems and/or are misaligned with second line risk systems. Data strategy must be formalized across products and global functions and consider consumption data requirements
- **Risk reporting and processes lack adequate controls (with potential for supervision failures)** related to interaction and coordination in remote environments. More broadly, data operating models need to be clearly defined with roles in business and functional units
- **Challenges in risk reporting, processes and infrastructure** (e.g., data quality, complex architecture) lead to **delayed and ineffective management of risks,** particularly in scenarios where they are **not effectively integrated and operationalized into core business operations** and allow straight-through processing. Lack of commitment to digitizing risk, control processes that could alleviate pain points
- **Basic data tagging** to legal entity, jurisdiction, business, customer, product that is necessary for reporting and metrics has not been enabled within key systems; **metrics demonstrating data quality are not being measured**
- Investment in control infrastructure is de-prioritized due to **budget constraints, approvals, limited resources**
- **Ineffective controls that are largely detective, manual and do not mitigate risk appropriately**

Unclear ownership of cross-border & enterprise risk

- **Firms do not always fully understand how legal entities are utilized,** particularly in **cross-border** (e.g., exposure from remote booking), **cross-business** (e.g., counterparty risk across multiple relationships within the firm) and **cross-entity** (e.g., risk from booking to other legal entities in the same parent firm) **scenarios**
- Risk and control teams across different regions and businesses have **inconsistent or conflicting responsibilities or hand-off processes**
- **New or complex products are booked in entities or regions that are not trained to manage or understand the risks posed**
- Similar risk-related **weaknesses are seen across large, international banks as well as smaller, local institutions**, per US regulatory feedback

Practical levers for change

Governance & accountability

- Instill an organizational commitment to an enterprise-wide **risk/compliance culture that is reinforced through risk-reward processes and governance**
- Establish effective **reporting and escalation channels** from the business, to Senior Management and the Board
- **Define 'multi-hatting' requirements** and conflict of interest guidelines
- Conduct **staffing assessments** to ensure **resources are sufficient and skillsets are adequately allocated**
- Facilitate trainings **to reinforce responsibility and accountability** from the top-down
- Define **RACI and accountability** across the first, second and third lines for risk management activities
- Ensure **policies and standards** designed by the second line are operationalized and tied to **regulatory and internal requirements**

Risk appetite / limits & controls

- **Articulate a formal risk appetite with Board approval** that aligns to all legal entities, businesses, and jurisdictions
- **Implement and maintain risk appetite, monitoring and reporting systems** and ensure breach escalation and remediation processes are in place for escalating and remediating breaches
- Ensure the risk appetite is integrated into core business operations **to monitor interaction and coordination in remote/hybrid working environments**
- Ensure **risk appetite is efficient and scalable across business operations** to accommodate changes in methodologies and logic (e.g., ensure risk framework enables the organization to 'connect the dots' across all businesses)
- **Understand processes and controls** on a front-to-back basis with emphasis on implementing preventative, automated controls
- Anchor processes and controls to **enterprise risk and product-level risk taxonomies (e.g., using common risk language across regions and businesses)**

Data, analytics & technology

- Utilize **advanced data collection** measures (e.g., predictive/forward looking KRIs based on enterprise data pools) to identify and flag risks
- Develop **key risk indicators/metrics** to evaluate control effectiveness and increase **predictive analysis**
- Develop **client management processes** and controls (e.g., BSA/AML, KYC requirements)
- **Prioritize investment in modernized technology** to maximize **straight-through processing** and simplify applications
- **Enhance technology to ensure risk data can be produced at a holistic level,** across functions, businesses and entities, that consider inter-company and intra-function bookings
- **Establish effective, enterprise-wide escalation processes that clearly coordinate** with leaders across all regions, businesses and entities
- Enhance **cross-border, cross-business and cross-entity technology and communication channels**

Risk culture & transformation

- Ensure **performance measurement and incentives** align with risk management objectives and **risk-reward trade-offs are overseen** by the Board and Senior Management
- **Implement a risk culture which emphasizes the importance of understanding operational risks and supports open communication** (e.g., empower personnel to take ownership and escalate issues)
- Instill a **culture of self-improvement and self-awareness** through both a top-down and bottom-up approach (e.g., circulate reoccurring communications from Senior Management reinforcing sound risk practices)
- Maintain awareness of other risk management programs and their relevance to **reduce siloed efforts** (e.g., complete regular reviews of risk related initiatives across the enterprise)
- **Implement risk transformation efforts** which clarify the risk management approach of the organization

The scale and public nature of the recent enterprise risk management and control failures along with regulator feedback to institutions regarding weaknesses in risk processes puts the industry on notice in a way that should not be ignored or responded to without looking at differences between global, local/regional and business/legal entity dimensions.

Identifying and meaningfully responding to cross-border, cross-entity and intra-business risk vulnerabilities across an entire organization requires self-awareness and top-down buy-in across the three lines.

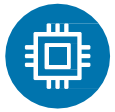
In our experience in supporting financial institutions and engaging regulators, there are practical ways to address these vulnerabilities which can yield immediate results.

Getting started…

To demonstrate effective and sustainable risk management processes, it is fundamental to **understand relevant risks, enhance infrastructure, implement a robust risk framework and ensure firm culture promotes sound risk practices**—we urge organizations to immediately take the steps listed below to achieve this.

Proactively perform **risk assessments** against relevant **'pain points'** to confirm which pose the greatest risks, and once complete, **evaluate controls** to determine which will most effectively mitigate applicable risks. **Analyze root causes and lessons learned** in earnest, and not as a 'check the box' exercise

Review risk management and control frameworks across businesses, legal entities and cross-border operations with a clear view towards global/enterprise and regional/local tensions. Consider ownership of risk, roles and responsibilities, communication channels, and escalation protocols with effective **monitoring and reporting processes to support**



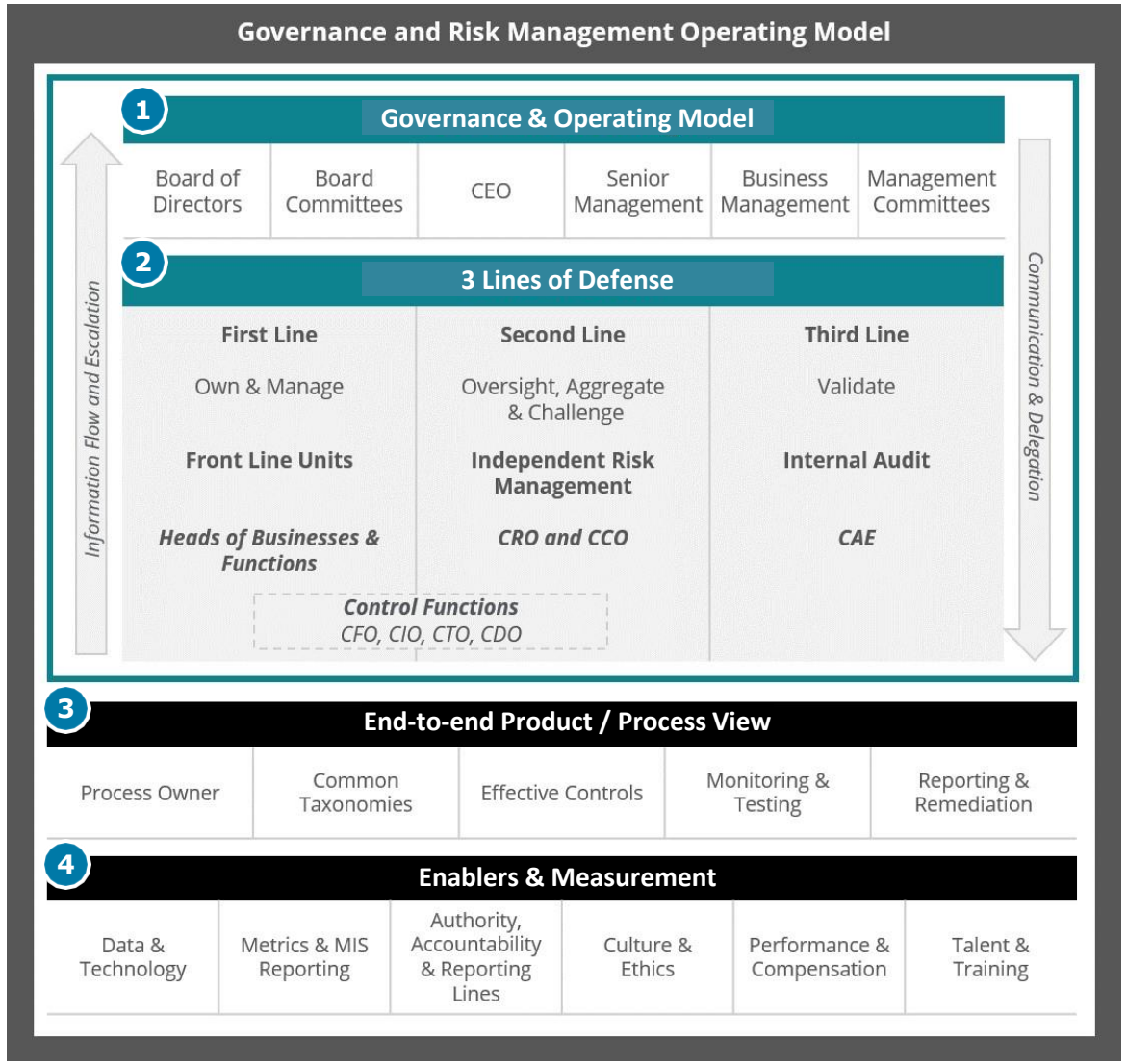
Identify immediate changes to monitoring and MIS/reporting protocols to ensure all relationships and related risks posed by the customer are captured. In the longer-term, invest as needed in new/improved technology to eliminate disparate and complex architecture; focus on intercompany/intra-function activities

Host challenge workshops that examine the firm's risk appetite and breach protocol including bright light boundaries and clearer escalation guidance and protocols which support independent decision-making accounting for business, legal entity, and product lenses

Define **incentive structure and staffing levels** in a way that ensures **roles and responsibilities around risk** are adequately performed, '**dual-hatting requirements'** are adhered to, and employees are encouraged to proactively **manage, escalate and remediate risks**

Start with an effective framework: Are the three lines really working?

The **call to action starts with this question – Are the three lines operating effectively?** Arguably, most organizations would say we have this; however, key components may be missing or not operating as intended, which has led to governance, risk management, and internal control challenges. Banks need to **pause and self-evaluate their ability to govern** and manage themselves **horizontally and vertically** across businesses, legal entities, products and jurisdictions.



Key questions

1. Is the ***Board*** receiving timely ***escalation*** and providing adequate ***oversight***?

   Is ***Senior Management*** being held ***accountable*** and achieving ***result-oriented outcomes***?

2. Are ***roles and responsibilities*** clearly defined and enabled across each line?

   Are sufficient ***resources*** with the appropriate ***risk and challenge mindset*** embedded across all lines?

3. Are ***common taxonomies*** and ***end-to-end process and control maps*** reflective of current practices?

   Are controls being adequately ***re-engineered, rationalized, automated, and tested*** to measure effectiveness? Has control digitization been accounted for in enterprise planning?

   Can controls be ***traced to*** regulatory requirements?

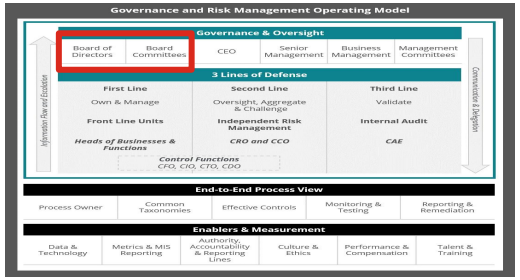
4. Have necessary investments been made to achieve ***accurate data and MIS reporting***?

   Do the ***right enablers*** exist to demonstrate accountability, effectiveness, and a robust risk and compliance culture?

   Are firms adequately considering where they can get value from strategies like managed service for risk infrastructure?

Appendix - Role specific call to action

Diagnostic assessment and call to action
Board



Key self-assessment questions to ask

- Are we doing enough to **enforce accountability** and a **culture of transparency and integrity**?
- Are we receiving the **information** needed to **effectively exercise our oversight responsibilities** on a timely and effective basis?
- Does management have a **robust process around escalation** and are the right things making their way to us for resolution?
- Are we confident that **key regulatory expectations** are appropriately implemented in the organization?
- Are **risks being self-identified** and are **internal audit, regulatory and other corrective actions being resolved** to fundamentally address the root cause of the issues noted? How is **management holding itself accountable**?
- Is the **three lines framework designed and implemented** appropriately?
- Is **Senior Management appropriately incentivized** with appropriate linkage of outcomes to performance management and incentive compensation?

Immediate actions to consider

- ✓ **Review reporting packages** received, and **self assess any gaps in information** by looking at agenda, reporting packages, timelines/quality of information
- ✓ **Ensure reporting is comprehensive** and covers the entire risk management framework from multiple dimensions. Ensure Board receives an **'independent, objective view'** of day-to-day operations
- ✓ Set up appropriate **process around regulatory remediation and corrective actions** ensuring accountability related to actions proposed, management accountability, how actions address regulatory requirement etc.
- ✓ **Review trends of issues, complaints and risk reporting** and ensure management has a **robust process around escalation**
- ✓ Ensure the risk appetite is approved by the Board and the **risk appetite and limits reporting is meaningful**
- ✓ Focus on **risk linkage across performance management and compensation structures with risk-rewards trade-off being overseen** by the Board
- ✓ **Self-assess the organization regularly against regulatory standards** and further evolving regulatory expectations

Diagnostic assessment and call to action
Business heads

Key self-assessment questions to ask

- Is the business **'too big and too complex'** to manage? If so, what actions can be taken to **simplify infrastructure**, legal entities, products?
- How do you know that **regulations and risks are being effectively managed in the first line**? What **reporting and MIS** do you receive to demonstrate this? Does your **governance structure** enable meeting the various demands of regulators in multiple jurisdictions?
- Do **business heads take accountability for risks and controls**? Is first line **empowered to self-identify** and report risks?
- What **types of issues, risks and business matters** arise that you are surprised about? Are these **communicated** to you timely? Are **root causes of issues** further explored with lessons learned documented and consequences/accountability impacted as a result of issues?
- How well does the **organizational structure and culture foster transparency, escalation, accountability**, and effective challenge?
- Do you have **effective controls** and are you confident that they mitigate your business risk appropriately? Do you have the right transparency and balance between **preventive and smart detective controls and manual/automated controls**? Are these **controls linked to enterprise risk and product risk taxonomies?**
- Are you investing appropriately in **rationalizing, re-engineering and automating** business processes and controls to optimize effectiveness?
- Is there **appropriate coordination and communication** between business and operations and technology/control functions?
- What **resources and investments** do the **risk, compliance and internal audit functions** need to effectively implement and sustain the **three lines** and to **meet regulatory requirements** and expectations for the organization?
- Is the **risk appetite integrated into the core business operations** for efficient identification and monitoring of risks?

Immediate actions to consider

- ✓ Ensure the business has a **documented business/operating model.** Determine **proactivity of business** in identifying issues relative to new /modified products. Ensure the business **understands the regulatory requirements** facing them
- ✓ **Document roles, responsibilities and accountabilities**. Ensure there is **appropriate monitoring** against the roles. **Develop clear escalation protocols** through the business
- ✓ **Manage and monitor risk appetite metrics/limits** to alert business management if there are issues
- ✓ Ensure business has a **risk and control function** that assists in operationalizing impact of controls in business processes
- ✓ Ensure **controls are rationalized** across first and second lines and investments are being made to **re-engineer and automate** as appropriate. **Document end-to-end processes and controls**. **Evaluate and test controls** on a frequent enough basis to highlight issues

Diagnostic assessment and call to action
Front office

Key self-assessment questions to ask

- Is the **front office risk and controls infrastructure scalable, reliable, periodically reviewed and adequately detailed** to sufficiently capture and address risks?
- **Is accountability and governance clear between the first and second line?** Including Business unit control functions?
- What **heightened controls and communications processes** are in place to ensure adequate transfer of information and collaboration across businesses?
- Have you **defined a 'dual hatting' guideline** to appropriately assess whether personnel has the time, skillset and expertise to perform assigned capabilities? Have you **considered conflict of interests** in such situations?
- Are you **reinforcing, supporting, and enabling the independence of the risk management and internal audit** functions?
- Is all personnel **aware of the roles and responsibilities across business and functions**, to avoid duplicative efforts and ensure accurate risk assessments?
- What **mechanism does your firm have to incentivize and hold the business accountable to carry-out their risk management responsibilities**?
- Are **employees encouraged to speak up and report issues** as and when they occur? Have you defined **clear escalation paths**?

Immediate actions to consider

- ✓ Clearly **define roles and responsibilities** for all front office employees
- ✓ **Evaluate existing policies, procedures, and frameworks** to ensure that they convey the business' responsibilities clearly
- ✓ **Reexamine risk appetite and controls** on a periodic basis
- ✓ **Impose clarity and controls over acceptable risk appetite including establishing limits on risk exposure** and policies governing exceptions to and **escalations of breaches** of such limits
- ✓ Employ **accurate processes and controls for coordination and interaction for efficient information dissemination**, especially in remote-working environments
- ✓ **Integrate risk infrastructure with core business operations** and **modernize technology** to assess and escalate risks in a timely manner
- ✓ Instill a **culture of responsibility, accountability and respect for controls** where each employee is held responsible for identifying and managing risks
- ✓ **Employ monitoring and reporting tools** that provide accurate information about risk exposures for timely escalation

Diagnostic assessment and call to action
Chief risk officer

Key self-assessment questions to ask

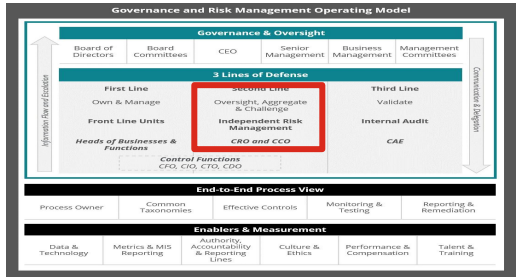
- How effective is the first line in **owning/managing risk and implementing the risk management framework**? How does the first line demonstrate implementation of the risk management framework?
- Are **roles and responsibilities across the three lines** clear (across countries, legal entities and risk types)? Is the risk function **independent with sufficient** access to Board, CEO, to **drive risk governance** with appropriate challenge to the first line?
- What **key risk processes and controls are the second line** currently performing on behalf of the first line?
- What **types of issues/risks arise** that you are surprised about? Are clear **escalation paths** developed and are these **communicated timely**? Does a **culture of transparency** exist in the first line, where information is shared, issues escalated and discussed on how best to partner/move forward? How effective are your monitoring, testing and surveillance routines?
- Are the **risk management frameworks operationalized effectively** across the organization? How would you **assess the effectiveness and sustainability** of the risk management framework across the organization? Does a common **risk and control taxonomy** exist that is understood and used throughout the organization? Does a **risk appetite/limits structure** provide **meaningful limits/thresholds across risk types** that cascades to all risk /legal entity types across the first and second line? How are **emerging/idiosyncratic risks**, risks arising from new/modified products/services, business model changes, digital platforms identified?
- What is the **vision for risk data /supporting architecture to provide** relevant, timely, accurate, predictive information for decisioning?

Immediate actions to consider

- ✓ **Clarify roles and responsibilities** between the first and second line. Establish ability to **hold first line accountable** e.g. report to Board, assign a risk score
- ✓ Ensure **CRO has requisite standing** within the organization and the right experience to lead the function. Ensure CRO is empowered to make **sufficient investment** in people, technology in both number of resources and skill sets
- ✓ Re-assess operationalization, **effectiveness and sustainability of ERM program** across the organization
- ✓ **Re-engineer risk identification and risk assessment**; ensure **clarity in risk measurement**
- ✓ Enable an **end-to-end view of risk assessment** (annual with quarterly reviews) and **encourage use of predictive analytics** to make decisions
- ✓ Build **robust analytics and stress testing infrastructure** to understand potential impact of change/scenarios
- ✓ **Upscale monitoring and control** enabling an end-to-end process view and owner with **less reliance on manual activities** and controls
- ✓ **Accelerate risk data and reporting initiatives** ensuring accurate and quality data

Diagnostic assessment and call to action

Chief compliance officer



Key self-assessment questions to ask

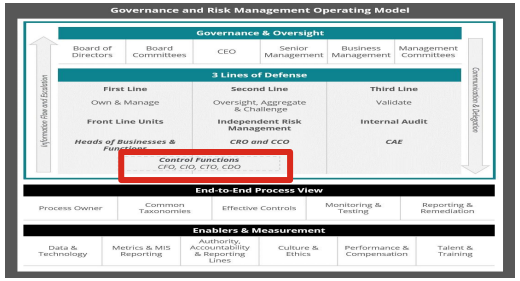
- To what extent has **compliance conducted a self-assessment of the compliance program** against written regulatory expectations and industry leading practices? Are **MRAs and MRIAs received by the organization effectively addressed**? Are your **BSA/AML and KYC requirements aligned to regulatory expectations** and current industry practices?
- How do you demonstrate compliance and ensure traceability with regulatory expectations across business lines?
- How would you describe the **stature of the compliance program** within your organization?
- How effective are the **issue identification and escalation protocols for compliance issues**? Do you have a defined interaction model with all compliance partners (e.g., risk, finance, business)? To what extent has compliance established a **set of standards by which issues are identified, ranked, managed, and resolved**?
- Is your **GRC platform agile and nimble and does it leverage** common taxonomies? How is the **requirements inventory managed** dynamically?
- Are **corrective actions and remediation plans regularly monitored for sustainability**, in addition to completion and overall 'status'?
- How effective is **compliance reporting (proactive/reactive) in providing a current snapshot**? Have **baseline performance metrics** been established in partnership with the business? Is it **forward looking**, including predictive risk indicators?
- How effective are your **monitoring, testing and surveillance routines**? How are they **refreshed** and at what frequency? Is your regulatory inventory current, accurate and effective?

Immediate actions to consider

- ✓ Ensure CCO has **requisite standing within the organization** and the right experience to lead the function
- ✓ Liaise with **compliance partners** to **identify compliance issues**
- ✓ Define **formalized standards to identify, track, rank, manage and resolve issues and MRAs/MRIAs**
- ✓ Regularly **measure and monitor corrective actions and remediation plans** to track status. Review **process around issues and regulatory remediation and corrective actions**; ensure **ownership and accountability** are in place
- ✓ Develop **effective monitoring, testing and surveillance routines** along with established frequency to refresh such routines
- ✓ Continuously **self-assess the compliance program** against regulatory expectations. Perform **comprehensive self-assessment and retrospective review** of compliance program. **Identify limitations and weaknesses** and solutions to enhance methodologies, tools and techniques

Diagnostic assessment and call to action

Chief financial officer



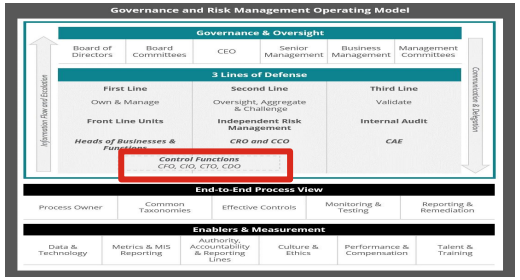
Key self-assessment questions to ask

- How comfortable are you with the **accuracy of reported data and process/control environment** for your **key reports**? Are there inconsistencies in reporting that are utilized in decision-making?
- Do you fully **understand the root causes of persistent or growing volumes of issues** impacting regulatory or financial reporting?
- To what extent are there **report assurance processes including data and control testing to identify data quality issues and their impact** across reporting processes? Across key internal MIS and regulatory reporting?
- Do **business finance leads understand applicable risks and controls within the end-to-end financial processes**?
- Do you have a **front to back data program** encompassing business through to finance/risk? Is **data quality measured** and embedded into process and controls?
- Is there **sufficient accountability for data and data quality** end-to-end for existing processes within a defined model?
- Is there an **integrated architecture across business and finance** where data quality is measured end-to-end?
- Do you have an **efficient budgeting and financial planning process** developed?

Immediate actions to consider

- ✓ **Understand the full inventory of applicable risks and controls** and how they **align with regulatory expectations**
- ✓ **Create a robust change management and governance framework** that can adjust to rapidly evolving **reporting processes** and enterprise level requirement changes
- ✓ **Document roles, responsibilities and accountabilities** across first and second lines and ensure there is **appropriate monitoring** against roles
- ✓ **Rationalize finance processes and systems** and identify areas where processes can be enhanced through technology or automation
- ✓ **Accelerate finance data and reporting initiatives** ensuring accurate and quality data, providing ability to business/functions to pull data on a timely basis, as needed
- ✓ **Enforce the budgeting and planning process** and develop **robust analytics platform** to support control environment and financial analyses
- ✓ Support the identification of **critical data requirements for regulatory, risk and management reporting**
- ✓ Ensure **processes** are in place to **identify data issues and material weaknesses impacting reporting processes**
- ✓ **Examine the controls** throughout the report production process for sufficiency and effectiveness and ensure **controls are rationalized** across the first and second lines

Diagnostic assessment and call to action
Chief data officer



Key self-assessment questions to ask

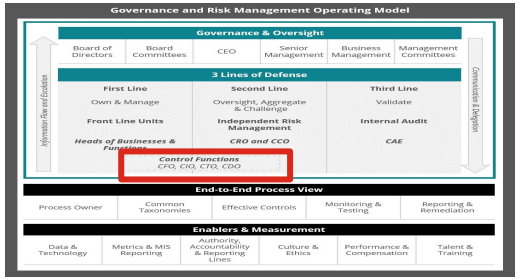
- To what extent are the **business and functions aware of their accountability** and **role for data** across the organization's data lifecycle?
- Are the **formalized policies clear** and do they **drive data quality standards** and expectations? How effectively have these expectations been implemented?
- How effective are the **mechanisms to monitor the implementation of** data standards? Are **data issues being proactively identified** vs. downstream? Are **advanced data collection measures utilized** appropriately to identify and flag risks?
- To what extent are **critical data requirements for regulatory and management / business reporting** understood and associated with clearly **defined and controlled golden sources** for data needs?
- Are you aware of your **end-to-end data flow** – from origination through to regulatory and critical management reporting, and the **effectiveness of controls** throughout the data flow?
- Have you **designed and documented data and systems architecture** across the organization enabling a common, consistent taxonomy?
- What **testing is being conducted** to assure proper level of data quality? How confident are you in your risk and regulatory reporting?

Immediate actions to consider

- ✓ Understand the **end-to-end data flow** – from origination through to regulatory and critical management reporting
- ✓ **Formalize clear and robust data quality standards** in policy, highlighting the expectations from the businesses and control functions
  - Business and control functions should ensure that the **policies related to data standards/expectations are implemented**
  - **Implement measurement mechanisms** to monitor adherence to data standards
- ✓ Ensure businesses and control functions are aware of their **accountability** and **role regarding data governance and management** across the organization's data lifecycle
- ✓ Identify **critical data requirements for regulatory and management reporting** along with golden sources of data – ensue that there is an understanding of the data flows to address reporting requirements
- ✓ **Examine the controls** throughout the data flow for both design, appropriateness aligned to measurement points, and effectiveness
- ✓ Ensure **processes** are in place to **identify data issues and concerns**
- ✓ **Ensure adequacy of testing for data and report quality**

Diagnostic assessment and call to action

Chief information officer/Chief technology officer



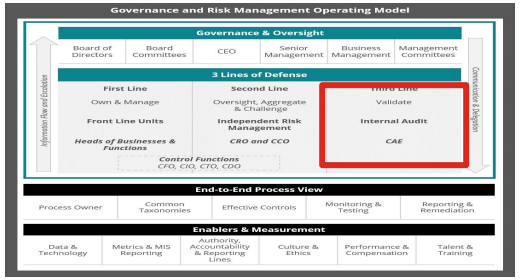
Key self-assessment questions to ask

- What steps are being undertaken to **design and implement a target state system infrastructure** aligned with your organization's overall business strategy? To what extent is the organization **aware of the role and scope of technology**, and is technology enabling the role of the businesses and functions?
- Do you have a defined system architecture governance standard that enforces accountability across the organization? How effective are **governance and oversight mechanisms over technology and the systems infrastructure**, and are critical challenges and issues being identified and addressed? Does your **technology and systems architecture produce risk data at a holistic level**?
- Are **data definitions and standards** established and consistent across the firm?
- To what extent are you aware of the **critical systems and applications** supporting product / asset classes, regions and functions in your organization, and those considered essential to the **aggregation and reporting of data**?
- How pervasive is **use of EUCs and manual adjustments**, and to what extent are they effectively governed and controlled?
- Do you conduct **regular assessments to identify new/advanced/improved technology to modernize your systems/architecture**?
- Are you appropriately **taking advantage of the latest technology** for improved automation and increased efficiency, including cloud technology, big data, and artificial intelligence?

Immediate actions to consider

- ✓ **Redesign and invest** as needed, in your systems and data architecture – maximizing straight-through processing, rationalizing applications, and modernize technology
  - Consider alignment to the organization's overall **business strategy**
  - **Develop a buy/hold/sell strategy with concrete migration dates towards target state**
  - Evaluate the **pervasiveness of the use of EUCs and manual adjustments**, and the effectiveness of their governance
  - Ensure linkage between business, systems and data architecture
  - Leverage the **latest technologies** in infrastructure
- ✓ Ensure there is clarity and **awareness related to role and scope of technology** across the organization
- ✓ Leverage consistent **modernization of implementation methods** – using agile techniques to improve execution of outcomes
- ✓ Focus on **critical systems/application enabling enterprise-wide aggregation and reporting** of data

Diagnostic assessment and call to action
Chief audit executive



Key self-assessment questions to ask

- Do we have the **right stature and brand** to drive change?
- Are we **calling strikes and truly holding management accountable for remediation** of all identified enhancement areas?
- Are we effectively **partnering and aligning** with the other **lines**?
- Are we effectively **conducting root cause analyses** and identifying thematic and/or **systemic risks**?
- Where is our **issue management process** potentially falling down?
- Are **regulators continuously identifying issues** that were not identified by internal audit?
- Are we providing the **right level of effective challenge** throughout the organization?
- Do we have the **right data information available and metrics** (e.g., KRIs, KPIs) to proactively identify and monitor all risks, including new and emerging risks?
- Are we proactively **monitoring and assessing the impact of transformation and change** within the organization, including the pace of change and its impact?

Immediate actions to consider

- ✓ **Hold yourself accountable about how to be more effective**. Perform **comprehensive self-assessments and retrospective reviews** of internal audit processes. **Identify limitations and weaknesses** and identify solutions to enhance methodologies, tools and techniques
- ✓ Review **methodology and approach to assessing and opining on the effectiveness of risk management**; ensure it is **comprehensive** enough across all elements of a risk management function (e.g., risk appetite, risk management functions, effective challenge frameworks, etc)
- ✓ Review **process around issue and regulatory remediation and corrective actions**; ensure **ownership and accountability** across the three lines
- ✓ Review the **maturity and sufficiency of end-to-end process and control documentation** within the organization. Assist and advise on how to **enhance risk and control self assessments** and **internal control documentation**
- ✓ Assess **Senior Management and audit committee reporting** to ensure **appropriate escalation and prioritization of significant issues**, including identification of thematic and systemic issues
- ✓ Perform **robust skills assessment** to ensure you have the right skillset and talent across all risk domains and regulatory compliance areas

Contacts

Irena Gecas-McCarthy

FSI Director, Deloitte Center for Regulatory Strategy, Americas

Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Colin Campbell

Senior Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Monica Lalani

Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Arpita Mukherjee

Manager | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Richard Rosenthal

Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Gabrielle Lombardi

Senior Consultant | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Michele Crish

Principal | Deloitte Risk & Financial Advisory
Deloitte & Touche LLP

Additional contributors to this publication include subject matter advisors: Adam Regelbrugge, Paul Lindow, Shruti Sinha, Bala Balachander, Dilip Krishna, Courtney Davis, Oz Karan, Joanna Connor, Ken Lamar (Independent Senior Advisor) and support from Kyle Cooke and Meghan Burns.

Deloitte.

This presentation contains general information only, and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.