KPMG

Compliance Transformation

Internal Audit Point of View

April 2017

Contents

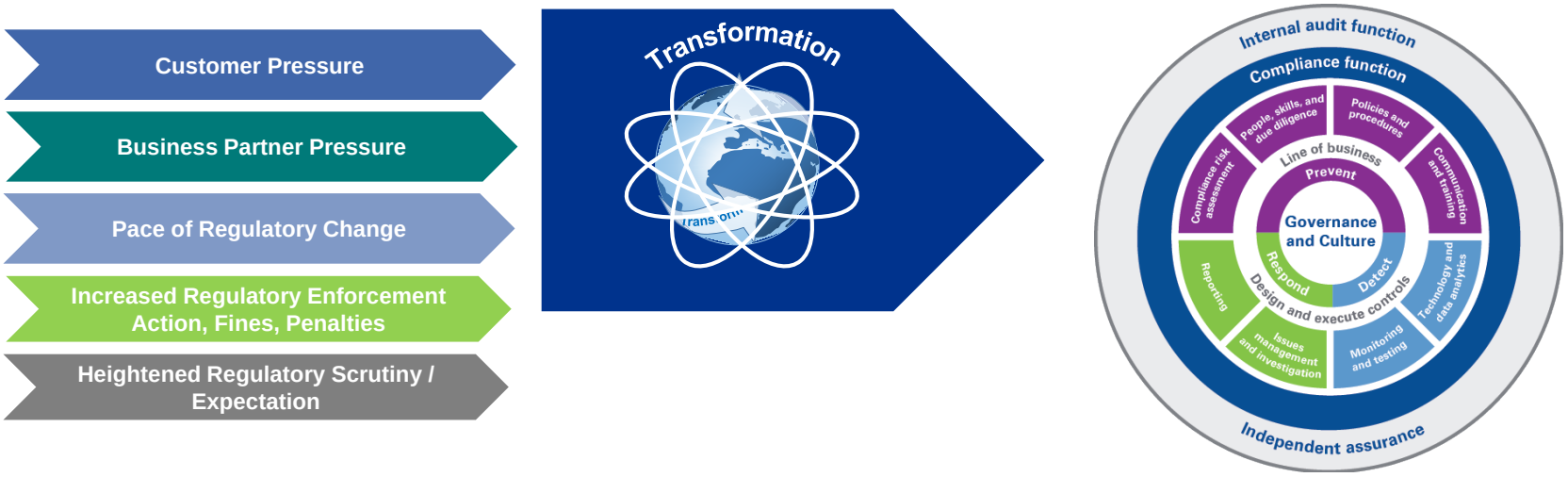
What is Compliance Transformation:

The continual evolution and alignment of an enterprises' compliance activities with their internal risk profile and tolerance, culture, strategic and financial objectives, business, operating, functional, and human capital models.

Organizations should deploy change and adapt their people, processes and technology in support of the compliance activities to address continually changing environments.

Transformation - Case for Change

Heightened customer and business partner demands, as well as the **evolving regulatory landscape** with fines, penalties, and reputational risk continuing to increase across all industries, are driving the case for organizations to change their approach to compliance.



The case for change demands a focus on **enhancements** to the current compliance management program and a new expectation of **expanded accountability** for compliance with the **integration** of compliance across all Three Lines of Defense.

Compliance is a Top Priority of Management and Board of Directors

The pace and complexity of regulatory change, coupled with the increase in regulatory scrutiny and enforcement action by relevant authorities, continues to make compliance a top concern for the Board

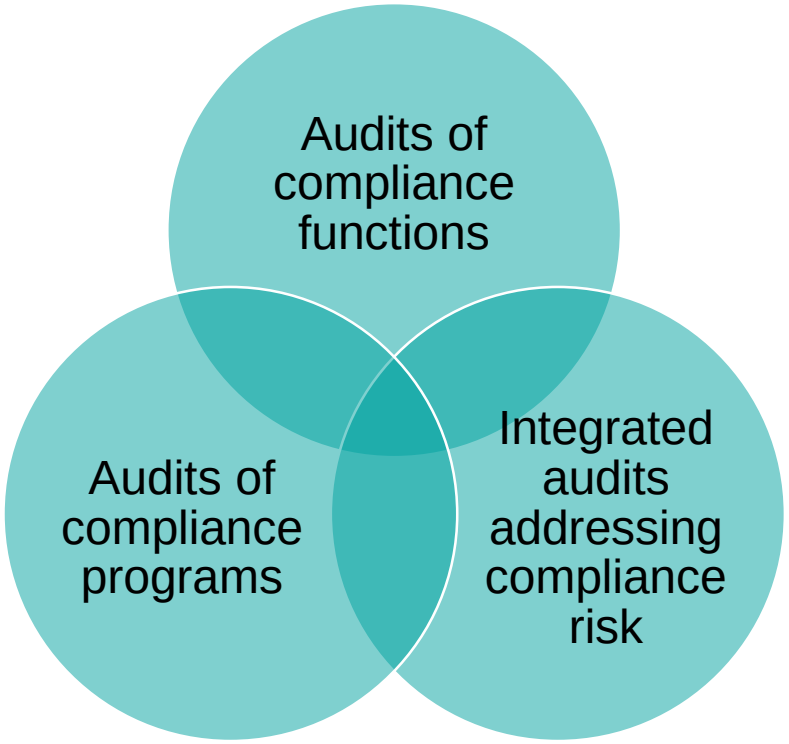
Boards of Directors are asking:

- How do we know we are complying with all the rules and regulations applicable to our company?
- How do we ensure we have a consistent compliance culture and framework across our enterprise?
- How can we better integrate compliance across our people, processes and technology in all three lines of defense?
- How effective are our internal systems in holistically supervising our business compliance efforts

What does this mean for Internal Audit?

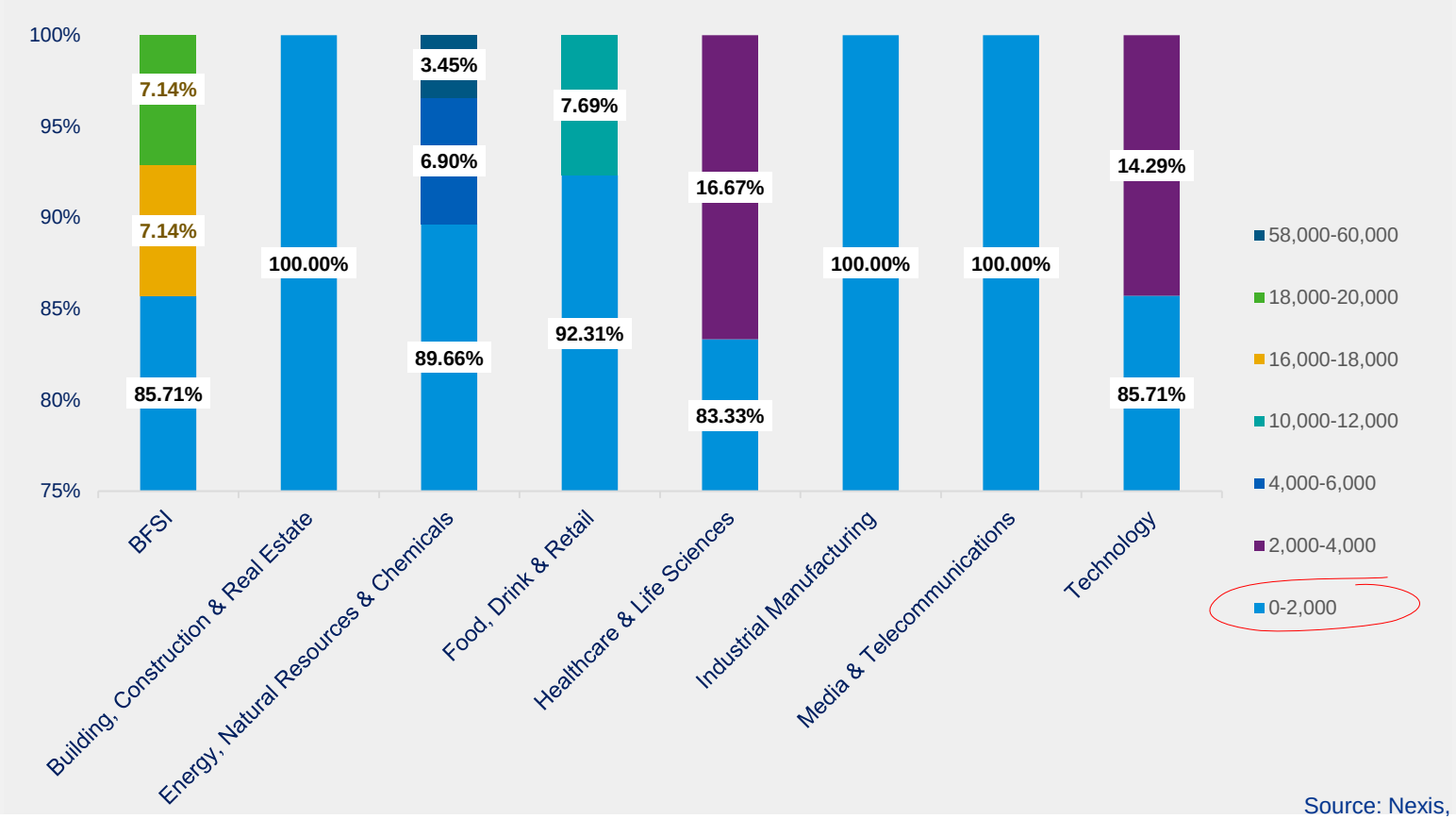
78% of CFOs and Audit Committee Chairs consider **providing compliance feedback** as an attribute that makes Internal Audit **insightful and valuable**.*

68% of CFOs and Audit Committee Chairs consider **Regulatory Expertise** among the **Top 10 Skills** necessary for Chief Audit Executives.*



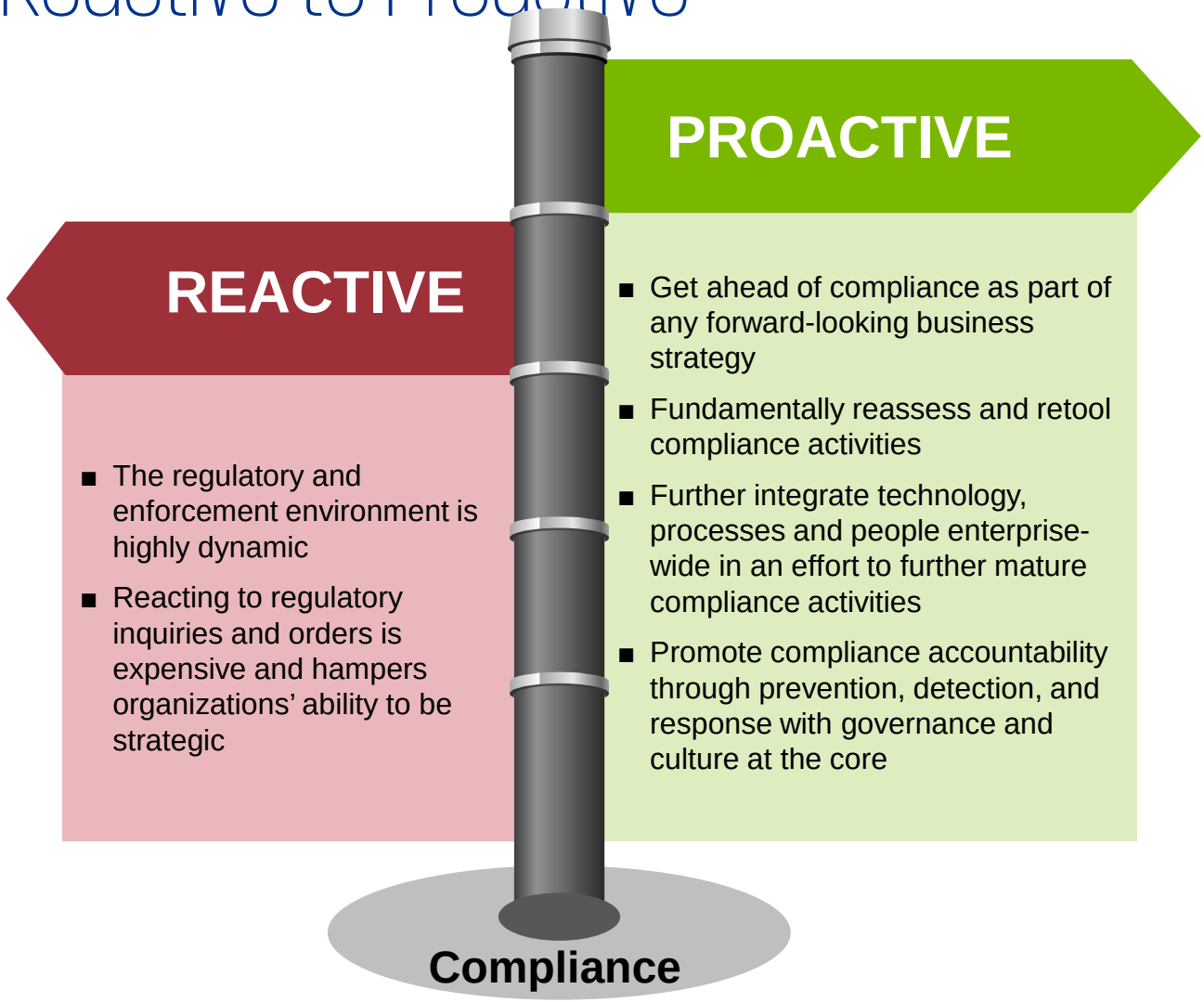
Forbes Research Insights on Internal Audit -2015

Count of Fines by Sector In US$ Million, 2012-2015



Source: Nexis, Factiva

From Reactive to Proactive



Internal Audit and Compliance: Face-to-face

Boards and Audit Committees are calling upon Internal Audit to review Compliance and assess controls and program effectiveness.

Key questions

— What are Compliance's expectations of Internal Audit?

— What are Internal Audit's expectations of Compliance?

— How do you measure compliance program effectiveness?

Three Lines of Defense Model

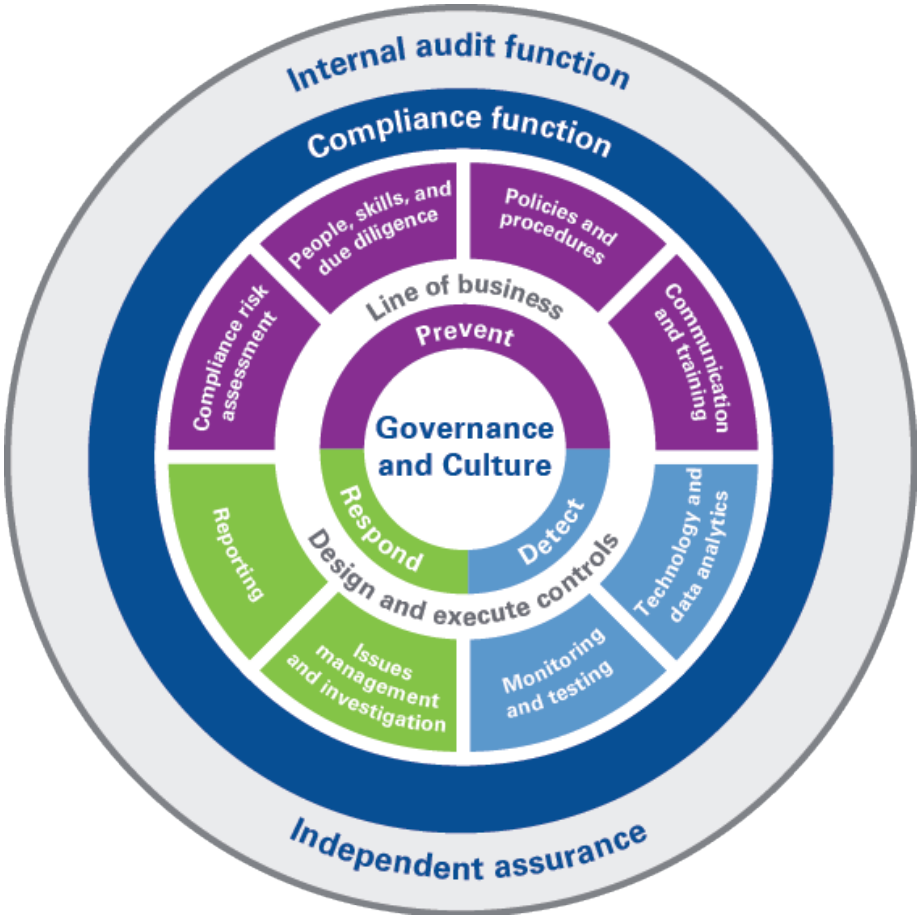
The "Three Lines of Defense" model is an enterprise-wide framework that serves as the basis for addressing risk, improving communication and achieving strategic business objectives. With clearly defined roles and responsibilities, each "line" of defense plays an important role within the organization's overall risk management governance framework.

The Three Lines of Defense Model

1st Line of Defense		2nd Line of Defense	3rd Line of Defense	External
Management Operations	**Business Monitoring (Ongoing)**	**Oversight Monitoring**	**Internal Audit**	**External Auditors and Regulators**
Ongoing management monitoring procedures conducted of their own processes, systems or products to ensure the are in compliance and controls are operating effectively. Examples include system testing, management review, approval and self inspections.	Ongoing monitoring against a defined standard such as regulations, guidelines, and policies and procedures to measure compliance. Such monitoring forms as essential control process for the business area and is performed by a group or individuals(s) independent of the operation or activity being monitored, e.g. Quality Assurance. This provides management with objective evidence that controls are operating effectively and complying with the requirements.	Reviews, audits or assessments facilitated or performed by oversight groups such as compliance or ERM to gain assurance that business is mitigating risks, implementing appropriate controls and maintaining compliance.	Independent audits of key risk areas by the Internal audit function to assess the adequacy of risk mitigation through established internal controls.	Inspections or audits conducted by external parties, including regulatory agencies, to assess compliance against regulatory or other external standards.

Compliance Transformation Framework

KPMG has developed a Compliance Transformation Framework rooted in governance and culture and aligned with eight key program elements. Our detailed and robust Compliance Transformation Framework may be used to build a comprehensive compliance audit plan for any organization.



Compliance Transformation Survey

Identified strengths

1. Governance and culture programs, including codes of conduct, are mostly in place with board participation
2. Policies and procedures support compliance programs and align with the organization's mission, vision, and values
3. Clear lines of communication exist within organizations, and employees generally receive training appropriate to their roles and responsibilities
4. Employees and third-party vendors are subject to onboarding due diligence and skills assessments

Identified areas for improvement

1. Monitoring and responding to regulatory change
2. Recognizing the competitive advantage provided by a strong compliance culture and good conduct
3. Conducting ongoing assessments of employee compliance skills and adherence to policies and procedures
4. Ongoing oversight of third-party contractors and vendors, including monitoring, testing, and training
5. Aligning technology infrastructures with compliance requirements, and leveraging technology to support compliance initiatives

Compliance Transformation Survey Key Results

Boards of directors provide active oversight. More than **90 percent** of CCOs report their board of directors or a committee of the board is adequately informed of compliance risks and mitigation efforts. The group meets annually to review and approve the compliance program.

More involvement needed from lines of business. Only **65 percent** of CCOs say that management in the lines of business take ownership of the compliance culture and agenda. Only **15 percent** strongly agree with this statement.

Communicating to employees the importance of compliance. Four in 10 CCOs (**39 percent**) do not consider adherence to compliance policies and procedures as a factor in performance ratings and compensation decisions, and **32 percent** do not agree that their employees understand the competitive importance of a strong compliance culture.

Engaging the organization in compliance Risk Assessment. While **84 percent** of CCOs report having a compliance risk assessment process, **31 percent** do not agree that business unit, operations, and IT management are involved in assessing compliance risk within their units.

More focus required on third parties. Only **half** of organizations have a process to confirm that third-party vendors adhere to compliance due diligence processes, and just **31 percent** manage third-party risk and issue tracking through an enterprise-wide tool capable of monitoring KPIs and KRIs.

Opportunities to leverage technology. While **69 percent** of CCOs say their organization leverages technology to support its compliance initiatives, only **47 percent** say they use data analytics and other technology processes to conduct root cause and trending analysis.

2017 Compliance Transformation Survey

Compliance Transformation Survey Key Results

Compliance policies and procedures. **94 percent** of organizations report having appropriate policies and procedures in place, while **95 percent** have compliance requirements including the code of conduct accessible to all employees.

Many organizations require more robust compliance testing. Less than **two-thirds** of CCOs report having a compliance testing program and plan under which the organization performs transactional, process, and controls testing.

Keeping pace with regulatory changes. Only **27 percent** of CCOs strongly agree that the compliance department has a change management process in place to identify and incorporate changes in laws and regulations.

Widespread use of enterprise-wide compliance reporting. **84 percent** of organizations provide reports on the enterprise-wide state of compliance including culture, conduct, governance, and key issues. In contrast, only **47 percent** of CCOs say their company has an enterprise-wide reporting system that is integrated across functions and business units and with compliance monitoring.

Compliance Transformation - Governance

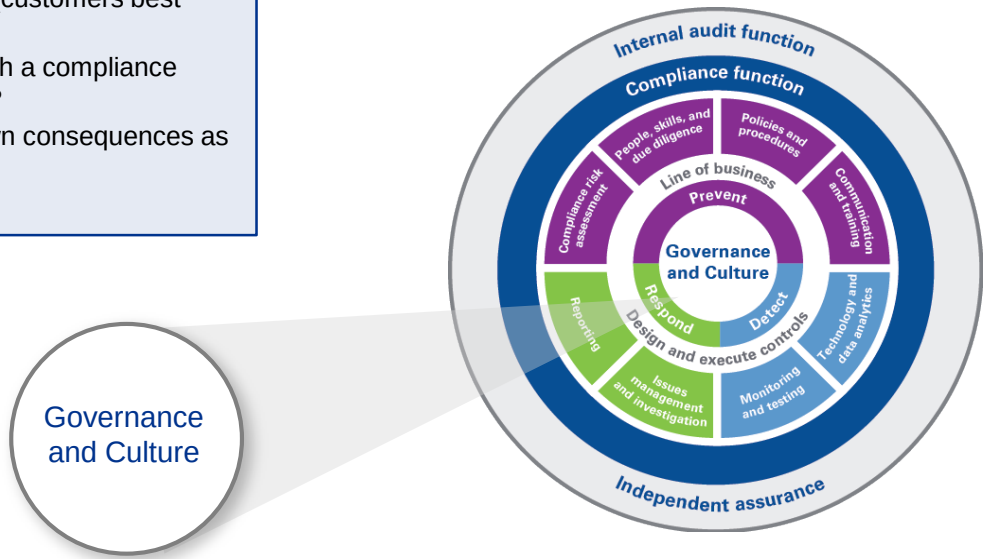
The organization's governance and culture will serve as the launching point for developing a customized compliance audit framework. Interviews with key individuals and review of key corporate documents (risk appetite statement) will set the stage for the compliance audit approach.

Questions for Internal Audit to Consider:

- How do you move your compliance program beyond what is required to what is expected for an organization of your size and complexity?
- What should the target state be for your compliance program across people, process and technology?
- How can you help ensure that the changes made will be demonstrated and sustainable?
- Does the organization/business focus on the "customer" (customers best interest at the heart of the business model)?
- Do the Board, executive and middle management set forth a compliance culture, consistent with actions, values and expectations?
- Are all employees accountable for compliance, with known consequences as well as associated incentives?

Governance and Culture

- Focus on the "customer"
- Tone at the top
- Accountability
- Effective Challenge
- Incentives



Compliance Transformation - Prevent

Does the organization's compliance efforts address the prevention of compliance issues? This will be a multi-element approach ranging from people and communication to policies and risk assessments.

Questions for Internal Audit to Consider:

- Do you have a centralized inventory of compliance obligations mapped to your policies and procedures, compliance testing and compliance training?
- How do you track regulatory and operational or business changes and the impact to your compliance controls and activities?
- Do you have the right talent and compliance operational metrics to take help ensure compliance effectiveness?

Prevent

Compliance Risk Assessment

- Inventory regulations
- Categorize inherent compliance risk
- Assess residual risk

People, Skills & Due Diligence

- Roles & responsibilities
- Due diligence (including background checks and on-going skills assessment)
- Performance management and compensation/Incentives
- Disciplinary enforcement and accountability

Policies & Procedures

- Mission/vision/values statements
- Entity-wide policies and procedures (e.g., code of conduct)
- Policies and procedures with embedded compliance requirements
- Policy management
- Regulatory change management

Communication & Training

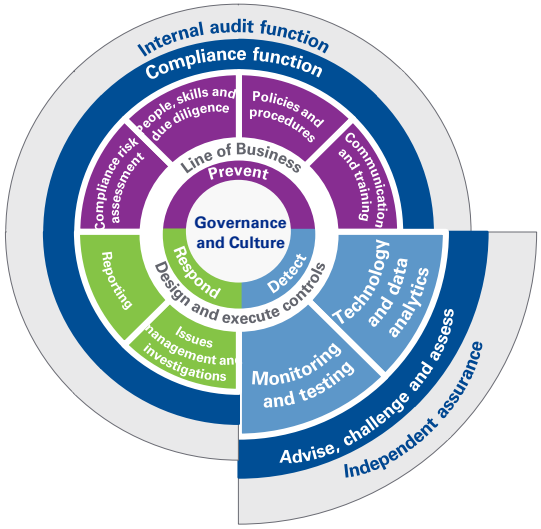
- Regular and frequent communications
- Culture / tone of compliance and regulatory change
- Regular and frequent training
- Third party participation in training programs

Compliance Transformation - Detect

What does the organization do once it has detected a potential compliance issue? Incorporating audit steps to measure what the organization has in place as it relates to compliance issue detection techniques may help to determine the strength of detective controls.

Questions for Internal Audit to Consider:

- Do you have both the data quality and the technology infrastructure to identify, measure, and monitor compliance risks across business lines and legal entities?
- Are compliance thresholds and metrics well-defined with ongoing monitoring and testing?
- How are third-party relationships monitored for regulatory and compliance risk?
- How do you assess the effectiveness of your compliance program?



Detect

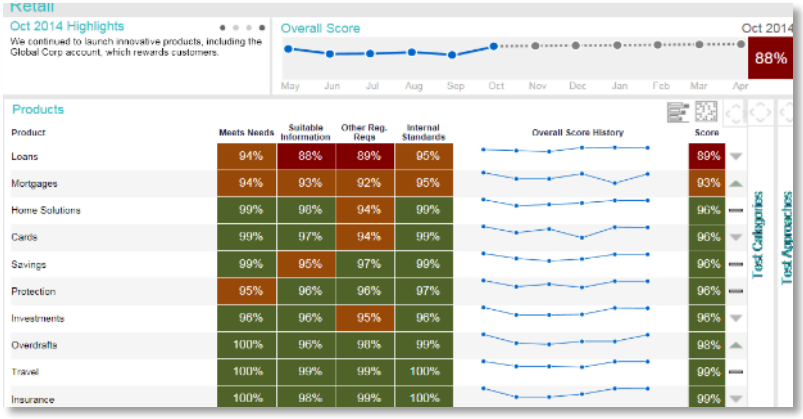
Technology & Data Analytics

- Technology to support compliance program (testing, training records, etc.)
- Predictive measures: key risk indicators (KRIs) / key performance indicators (KPIs)
- Root cause analysis and trending

Monitoring & Testing

- Monitoring and tracking of regulatory change
- Transactional, process and control testing
- Third-party compliance due diligence and management
- Licensing
- Periodic compliance program evaluation

Dashboard Reporting

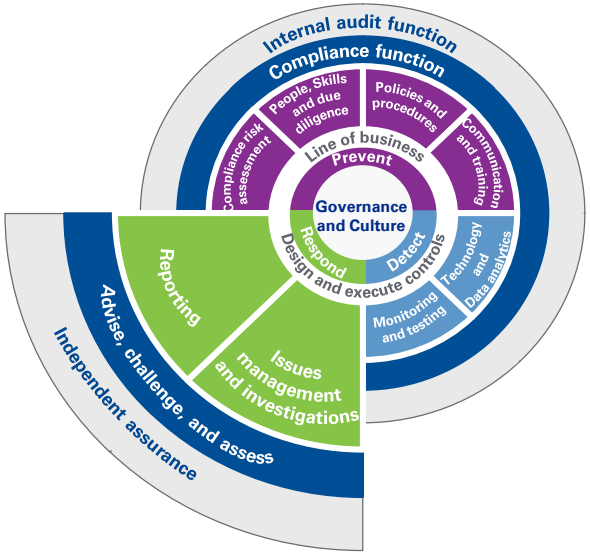


Compliance Transformation - Respond

Stakeholders will most certainly place significant importance on how the organization responds when incidents arise. Incorporating the framework elements into audit activities may help to assess the strength of the organization's response to compliance issues.

Questions for Internal Audit to Consider:

- Is the current "State of Compliance" reporting robust with key compliance themes, compliance program assessment and emerging risks metrics?
- How are your compliance issues inventoried, prioritized, remediated and reported?
- Do you have clear management standards for investigations, examinations and inspections?



Respond

Issues Management & Investigations

- Issues management and remediation
- Voluntary disclosure protocols/self-reporting
- Responding to government investigations/exams/ inspections
- Response plan and process for investigating alleged non-compliance

Reporting

- Periodic reporting to management and the Board
- Required regulatory reporting

Compliance Transformation - Alignment

In order to achieve a more mature Compliance Program, consideration must be given to connections between each of the components of the Compliance Transformation Framework.

Prevent

Compliance Risk Assessment, People/Skills, Policies & Procedures, Communication & Training

- Updated enterprise-wide risk assessment to include new/amended regulation(s) and/or necessary control enhancements identified through testing; completion drives testing scope/frequency
- Updated skills assessment for compliance testing staff to address new/amended regulation(s) (risk/controls) as well as ability to execute corresponding testing and/or associated controls
- Performance metrics updated to address and prevent manual control outcomes, issues and/or failures identified through testing
- Updated Policies and Procedures to address new/amended regulation, controls, processes and/or identified risks
- Updated training and regular communication to address new/amended regulation, controls, processes and to address failures identified through testing

Respond

Issue Management / Reporting

- Outcomes, issues and failures identified are formally documented on a centralized issues management repository and include, key stakeholders, action plan/steps, timeline
- For remediation action planning, consider spirit and intent of regulation, root cause analysis and control enhancement opportunities
- Reporting includes new/emerging risk areas, regulatory change and trending of testing results
- Reporting addresses enterprise-wide state of compliance, including an impact analysis of control outcomes, issues and failures

Compliance Transformation Framework

Detect

Technology & Data Analytics

- System coding / business rules built to map updates upon regulatory change, including, regulatory inventory, process flows, and testing
- Automated metrics (to help produce red flags, exception reporting, etc.) and data analytics models updated to reflect enhanced controls / processes based on control outcomes, issues and failures identified through testing

KPMG

Thank you

kpmg.com/socialmedia

Lucie Wuescher
Managing Director
Advisory Services
Phone:713-319-2103
lwuescher@kpmg.com

Chris McDonald
Managing Director
Advisory Services
Phone: 713-319-2586
crmcdonald@kpmg.com