Compliance's Expanding Coverage

Current and future roles

May 2024

Contents

> *"Compliance is at a turning point as it moves from enforcer and overseer to an enabler and guardian. The time is now for giving it the voice, skills and investment to realize the returns this pivot creates for the business - not only to lessening issues, breaches, and violations but to increasing brand satisfaction and productivity."*

Amy Matsuo

Principal, U.S. Regulatory Insights Leader
KPMG LLP

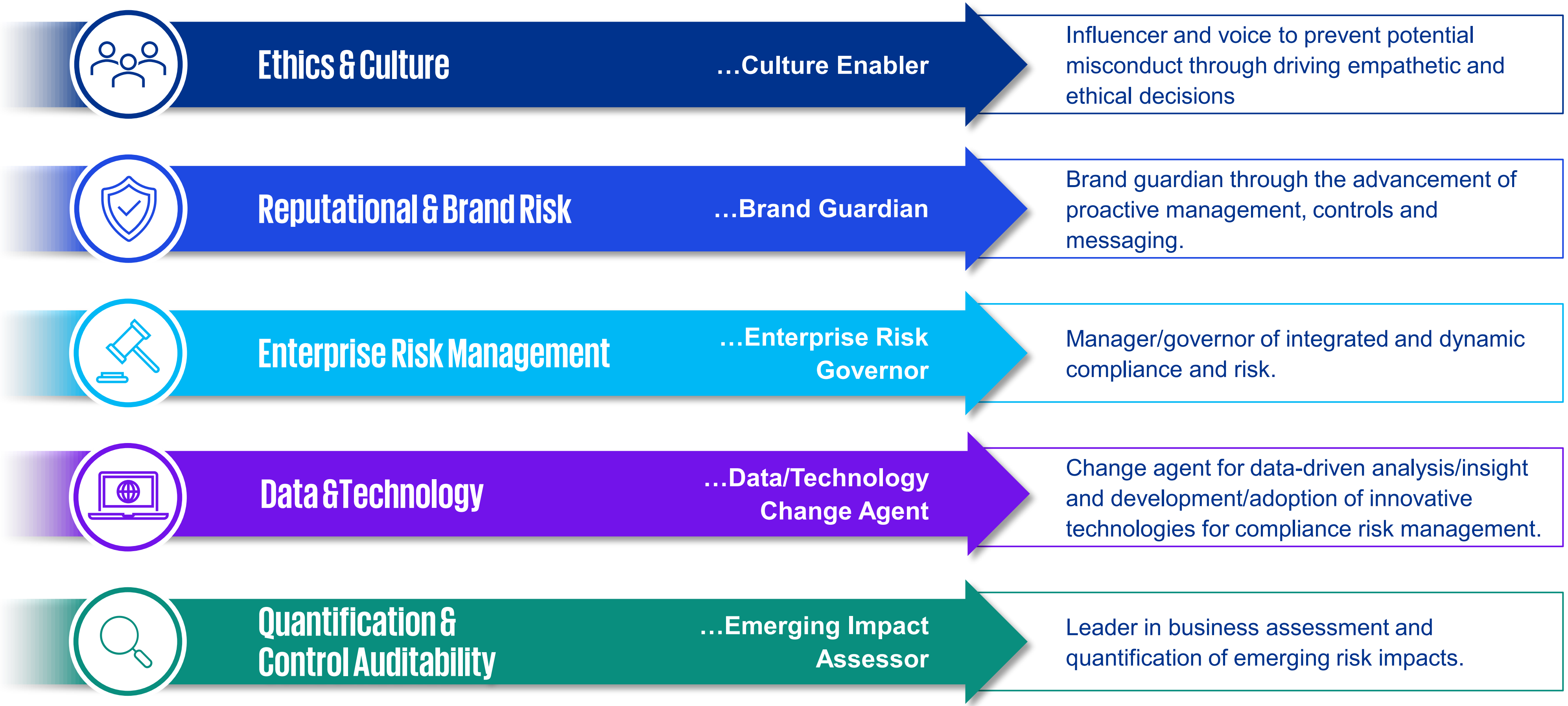
> *"With rising expectations from regulators such as the DOJ and PCAOB, the evolving role of compliance has and will continue to expand into previously siloed pillars of risk management including but not limited to fraud, investigations and disputes."*

Matthew McFillin

Partner, *Forensic Services*
KPMG LLP

Key Takeaways

Compliance has an undisputed critical function as not only an enforcer but increasingly as a trusted advisor to assist the business in the prevention of non-compliance. Compliance's value is not only in identifying and ensuring resolution of issues, but in preventing and mitigating such issues – in helping to drive effective controls and alignment with business processes across the organization. As such, the areas of coverage for which Compliance takes direct and/or indirect responsibility are ever increasing. Five areas that Compliance should anticipate expansion in the next several years include:



Standard Setter and Enforcer…	Ethics & Culture	…Culture Enabler	Influencer and voice to prevent potential misconduct through driving empathetic and ethical decisions
Reputational Risk Overseer…	Reputational & Brand Risk	…Brand Guardian	Brand guardian through the advancement of proactive management, controls and messaging.
Compliance Risk Monitor…	Enterprise Risk Management	…Enterprise Risk Governor	Manager/governor of integrated and dynamic compliance and risk.
Data Reporter…	Data & Technology	…Data/Technology Change Agent	Change agent for data-driven analysis/insight and development/adoption of innovative technologies for compliance risk management.
Control Inspector…	Quantification & Control Auditability	…Emerging Impact Assessor	Leader in business assessment and quantification of emerging risk impacts.

Ethics & Culture

In order to drive an effective compliance program and help prevent potential compliance-related occurrences, Compliance will be looked on as an influencer and voice for driving ethical business decisions – helping to set an environment that fosters and facilitates empathy, civility and “doing the right thing”. This dynamic is underscored by regulatory guidance such as the DOJ’s policies relating to corporate conduct and investments in Compliance and the SEC’s compensation clawback policies.

Standard Setter and Enforcer

Compliance sits at the forefront of fostering a strong ethical environment that looks to enhance integrity and earn/maintain trust. Compliance departments currently function as Standard Setters and Enforcers, including:

- Setting and/or reviewing company policies and procedures against regulatory requirements
- Implementing a “speak up” culture across the organization
- Assessing the culture of compliance through ongoing reviews against compliance requirements and employee surveys
- Training employees on regulatory obligations and company codes of ethics and conduct (including personal device usage, “speak up” programs, compliance forums, etc.).
- Identifying and assisting in resolution of firmwide compliance violations and investigating potential misconduct
- Enforcing company disciplinary policies (e.g., compensation clawbacks, financial sanctions, etc.)

Drivers

- Heightened regulatory focus on culture of compliance, corporate misconduct, board diversity, and employee inclusion
- Increased productivity linked to diversity & inclusion in the workplace
- Geopolitical disparity
- Market structure changes

Culture Enabler

Compliance departments are shifting to a role as Culture Enabler by adapting and enhancing their oversight and enforcement of ethics & culture as businesses adjust to complex workplace structures/environments and integrate advanced technological tools such as AI/GenAI into their operations. Responsibilities can include:

- Serving as a partner to the business to increase awareness and understanding of organization standards, enhance employee confidence/trust, and build consistent experiences
- Establishing shared goals among board and senior leadership to strengthen techniques for driving performance
- Responding to feedback from the business, stakeholders, and customers and updating compliance training and messaging as a result
- Embedding the results of compliance assessments within broader risk management practices and enterprise risk assessment activities
- Defining and aligning target behaviors and transformation tactics to achieve desired organizational outcomes
- Ensuring the business understands its role in maintaining compliance and promoting accountability throughout all business units and employee levels (including senior management)
- Embedding compliance controls into routine business processes
- Partnering with HR to help continuously define, drive and improve an ethics-based culture

Reputational & Brand Risk

In safeguarding brand reputation, the role of Compliance has evolved from enforcing adherence to regulations to having an active role in driving accountability and sustaining long term business success. Heightened regulatory and public expectations relating to sustainability, fairness, and ethical marketing necessitates Compliance's influence on risk management strategies, policies, reporting, and marketing content.

Reputational Risk Overseer

Compliance is now positioned with a seat at the table to coordinate and collaborate with the board and senior leadership on preserving the organization's reputation and maintaining stakeholder and public trust by:

- Enhancing compliance governance frameworks with defined goals
- Validating content messaging, reporting elements, and stakeholder responses prior to issuance
- Assessing regulatory change management processes and ensuring that they fully capture diverging global, federal, and state regulations
- Conducting on-going monitoring of consumer complaints and investigations
- Detecting and issuing timely responses to potential violations or misconduct

Brand Guardian

As stakeholder and regulatory expectations continue to expand, compliance departments will function more as Brand Guardians by taking a more proactive approach to preventing reputational and brand risk. Expanded coverage can include:

- Ensuring alignment between strategies, processes, and organizational messaging
- Collaborating with the business to embed compliance standards early in the product lifecycle
- Support in process design and alignment to corporate standards
- Integrating Compliance to ensure that products, services, regulatory reports, marketing materials, etc. are in line with business strategies and informed by regulatory, shareholder, and consumer expectations
- Enforcing business unit accountability throughout the enterprise
- Implementing a dynamic risk assessment that is inclusive of sizing for potential reputational/brand risks as part of both inherent and residual risks
- Bringing together owners and stakeholders that are responsible for related risks within the company

Drivers

- Disparate state, federal, and global regulations
- Heightened sensitivity of varying "social" issues
- Regulatory push for more transparency in reporting and disclosures
- Public/consumer expectations for companies to "do as they say"

KPMG

Enterprise Risk Management (ERM)

Historically, individual risk has been managed in siloed pillars and essentially managed by individual functions. Due to the interconnected nature of varying risks, there has been a shift to a more integrated approach that has led to cross function collaboration and coordination in conducting dynamic assessments, risk monitoring, and resolution. Across industries, there is a push for companies to invest in compliance risk management and innovation. In the KPMG 2023 Chief Risk Officer Survey, regulatory and compliance issues were ranked as the biggest expected risk management challenges in the next 2-5 years.

Compliance Risk Monitor

Compliance’s current role has expanded from monitoring compliance risks to more “governance” focused responsibilities such as:

- Identifying, escalating, and resolving issues
- Inventorying and mapping laws, rules, and regulations to controls
- Supporting the business lines in their processes to capture relevant risks
- Reviewing supervision and control testing coverage to determine any need to increase coverage
- Facilitating enterprise-wide review/application of identified risks to risk assessments/RCSAs
- Encouraging risk ownership of each business function/unit

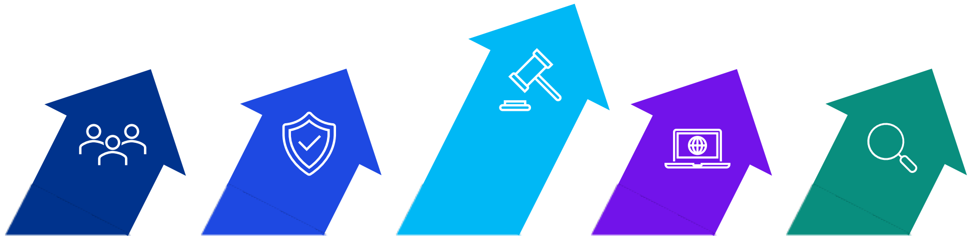
Drivers

- Increasing operational risk management expectations
- Intensifying regulatory scrutiny of management of risk and controls
- Ongoing supervision and rulemaking in areas of risk such as cybersecurity, privacy, fairness, sanctions, etc.
- Supervisory findings spanning across compliance and operational risk

Enterprise Risk Governor

Future expansion of roles and responsibilities will require the Compliance function to merge with that of Risk Management to:

- Assess the impact of compliance risks on the broader organizational risk profile, supported with a uniform and consistent risk rating methodology
- Support the development, implementation, and oversight of risk mitigation plans
- Define and implement assessment criteria for severity determinations
- Understand and assess “contagion” risk impacts
- Hedge against novel and emerging threats and vulnerabilities (e.g., virtual currencies, sanctions evasion, malware/ransomware, human rights/forced labor, organized crime).
- Integrate and operationalize risk and compliance into business processes and controls
- Ensure board approval of risk appetite including company risk culture and quantitative risk statements
- Develop comprehensive data strategies for producing and sharing risk insights with stakeholders
- Enhance scenario planning capabilities to prepare the business for high impact risks
- Drive consistency across risk and compliance by establishing commonality of risk taxonomy (e.g., tiering/severity levels/ratings) and operating protocols



Data & Technology

As companies develop and adopt new technologies, as well as generate/use large amounts of data, the role of Compliance is shifting from reporting data to serving as a change-agent for data-driven analysis and insight, as well as for the development and adoption of innovative technologies.

Data Reporter

Compliance departments are increasingly hiring tech and data specialists as they integrate analytics and automation into their processes. Today, their role as Data Reporters involves:

- Monitoring/inventorying regulatory developments and ensuring that business functions assess and implement requirements and/or controls appropriately.
- Utilizing analytics and existing technological infrastructure to identify, measure, and monitor risks across the business
- Collaborating with stakeholders, technology teams, and vendors to address compliance challenges
- Establishing and monitoring compliance key risk indicators (KRIs) and linking them to the organization's risk tolerance/appetite
- Creating policies and procedures to govern personal devices, communications platforms, and messaging applications
- Analyzing compliance data to identify historical trends and patterns to identify root causes and evaluate the effectiveness of controls.

Drivers

- Ongoing state, federal, and global AI regulations
- Enhanced cybersecurity threats
- Regulatory supervision and enforcement relating to :
  - Data use and privacy
  - Model risk management
  - Mitigating risks of bias and consumer harm resulting from automated decision making

Data/Technology Change Agent

Ongoing and expanding regulations related to the development, deployment, and use of advanced technology such as AI/GenAI and models will transform the Compliance department into a Data/Technology Change Agent within the business. Future expansion of Compliance coverage can entail:

- Ensuring balance and adherence to diverging federal, state, and global regulations on automated systems and innovative new technologies" (e.g., software; models; predictive analytics; and algorithmic processes, such as AI, ML, NLP, and LLMs) across the full lifecycle of design, development, and deployment
- Fostering a culture of transparency and accountability within the organization through clear communication of compliance-related goals, functionality, and potential impacts of automated systems to both internal and external stakeholders.
- Identifying and prioritizing AI and other technology/automation use cases to drive efficiencies in data analysis/insights and compliance programs
- Inventorying the varying AI applications and models being deployed across the organization and identifying and building mitigating controls to the downstream compliance risks related to each
- Serving as a trusted advisor to technology and data teams
- Incorporating new and evolving technologies in ongoing risk assessments, and facilitating ongoing monitoring of new tools and analyses
- Shifting from policy and regulatory change management of data/technology risks to ensuring real-time monitoring and surveillance of data/technology risks

KPMG

Quantification & Auditability

Heightened risk standards call for demonstrable agility and mitigation of risk and compliance “shocks”, as well as robust risk accountability and governance. In keeping with these standards, Compliance’s coverage is expanding to a more hands on approach in measuring, preventing, and detecting future risks.

Control Inspector

The current role of Compliance involves serving as a Control Inspector as it prepares the business to meet heightened data requirements, and more granular reporting by:

- Reviewing supervision and control testing coverage and increasing coverage as needed.
- Identifying compliance metrics that provide more insights on business operations and effectiveness of risk mitigation plans
- Assessing and measuring compliance effectiveness by triangulating data sources (e.g. third-party reviews, internal audit, transaction testing, culture surveys, stakeholder interviews for additional insights)
- Creating compliance metrics that factor in information about possible situations or scenarios, available resources, past/current performance, and suggest a course of action or strategy
- Measuring the performance of the compliance function and the business line by utilizing execution effectiveness metrics

Drivers

- Proposed amendments to auditing standards related to Noncompliance with Laws and Regulations (NOCLAR)
- Mounting pressure from boards and regulators to enhance Compliance
- Increased data reporting requirements

Emerging Impact Assessor

Future expansion of Compliance coverage will shift to the roles and responsibilities of an Emerging Impact Assessor as the Compliance department establishes itself as a key facilitator of company risk preparedness. Expanded coverage will encompass:

- Conducting full and dynamic inventories of applicable laws, rule, and regulations that are mapped to business processes/controls and utilized for ongoing compliance risk assessments (including inherent and residual risk)
- Integrating such inventories with ongoing risk assessing activities and strengthening the maturity of related inherent and residual risk calculations
- Expanding ongoing controls, control mapping, control accountability and control testing in line with SOX and/or SOX-like standards
- Facilitating program enhancements related to the overall control environment to mitigate fraud and abuse risks
- Understanding capacity planning to execute changes, specifically for data, analytics and modeling teams.
- Measuring the severity of potential compliance/ethics matters and determining the impact on operations, consumers, and investors
- Quantifying previously qualitative risks (e.g., potential consumer harm impact) and linking to risk monitoring practices including “outside-in” analyses (e.g., industry enforcement, negative news)

Relevant Thought Leadership

Regulatory Alert

Regulatory Insights

- Heightened Risk Standards: Focus on Risk Frameworks, Processes, and Controls
- Noncompliance with Laws and Regulations, Including Fraud: PCAOB Proposed Amendments
- AI Regulation: Cross-Agency Actions
- Enforcement/Supervision to “Automated Systems”

Compliance Insight

- Ethics and The Culture of Compliance
- Analytics & Automation

Ten Key Regulatory Challenges of 2024

Strengthen the cards you hold

Ten Key Regulatory Challenges of 2024

2023 Chief Risk Officer Survey

Reserve your copy now

2023 KPMG Chief Risk Officer Survey

Strengthening Compliance Effectiveness Metrics

Board Leadership Committee November 2021

Strengthening Compliance Effectiveness Metrics

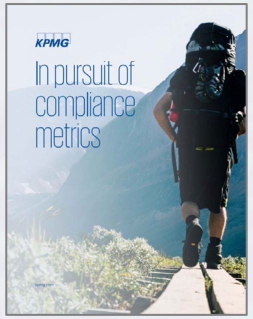
The “Empowerment” of State Law and Regulation

Reassessing risk and compliance

The ‘Empowerment’ of State Law and Regulation

Anticipating more scrutiny

2023 KPMG Chief Ethics & Compliance Officer Survey



In pursuit of compliance metrics

In pursuit of compliance metrics

Compliance Transformation (CT) Industry Leaders

Amy Matsuo
Principal and Leader
Compliance Transformation and Regulatory Insights
amatsuo@kpmg.com

Matthew McFillin
Partner
Forensic Services
mmcfillin@kpmg.com

Dan Click
Consumer/Industrial Manufacturing CT
dclick@kpmg.com

John Kemler
Technology, Media, and Telecommunications CT
jkemler@kpmg.com

Brent McDaniel
Retail/Energy CT
bmcdaniel@kpmg.com

Anthony Monaco
Government CT
amonaco@kpmg.com

Mike Lamberth
Insurance CT
mlamberth@kpmg.com

Jaime Pego
Healthcare CT
jpego@kpmg.com

Todd Semanco
Financial Services CT
tsemanco@kpmg.com

Jennifer Shimek
Healthcare & Life Sciences CT
jshimek@kpmg.com

KPMG

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.