Compliance priorities for digital transformation in consumer & retail

Delivering on customer experience
Digital technologies are reshaping both consumer demand and competitive dynamics in the consumer products marketplace, as well as restructuring how consumers shop for and buy products.

For consumer and retail organizations, the evolving digital technologies offer the ability to transform consumer data into real customer insights, enabling them to better understand consumer behavior and potentially foster new and differentiated products and experiences to promote brand and product loyalty.

However, the volume of available data and the fast pace with which digital transformation and marketplace changes are evolving combine to create an increasingly complex and interconnected business environment that is challenging consumer protections and regulatory frameworks. This evolution can, and will, shift products and services outside of traditional industry boundaries and into new regulatory jurisdictions. By extension, organizations will be faced with new regulatory requirements and potentially new regulators.

To date, U.S. regulators have indicated they do not want to impede innovation and have taken a cautious approach toward implementing policies to address emerging technologies. In large part, they have looked to existing laws and rules to set the guardrails for evaluating organizations’ new digital applications and related products and services, keeping consumer protection and fair markets as their primary measure. This is now changing. Vast and growing data networks have begun to blur the lines between consumer/retail, financial services, payment systems, and technology companies; lawmakers and regulators are increasingly focused on data privacy, data security, competition policy, and fairness as well as how to revamp their regulations to ensure all parties with data touchpoints, including consumers, are adequately covered.

This paper highlights ten areas of potential regulatory compliance challenge that consumer and retail organizations may face as they push toward a customer-centric digital transformation. It outlines market drivers and actions organizations can take to keep digital innovations consistent with current and developing regulatory expectations.
Data privacy
The collection and use of consumer data is the focus of heightened consumer awareness and public policy. Companies must establish and maintain robust data governance and consider the consumer protection components to their data privacy strategy and controls.

Cybersecurity
The risk of cyber threats to the resiliency of the organization and to the protection of consumer data is tied to the interconnectedness of markets and systems, third-party technologies, and increased digital use.

Consumer protection
The distribution of goods and services to consumers brings forth expectations for the accessibility, usability, fairness, and transparency from advertising and marketing through to delivery and fulfillment.

Ethics and compliance
Companies are expected to effectively set forth controls and a risk culture that drives ethics and integrity, mitigating and monitoring for potential fraud, waste, abuse, and/or misconduct.

Third-party providers
Companies must conduct appropriate diligence and monitoring of their suppliers, distributors, and other third parties to ensure regulatory and compliance standards. Third parties also include consumer digital services providers such as software and cloud providers as well as distribution firms, clearing houses, and inventory firms.

Customer-centric compliance
Compliance processes and controls must be put forward that allow for the voice of the customer across strategic design and change and include the ability to appropriately reach and serve customers and effectively respond to customer complaints as well as product recalls and refunds.

Payments
Consumer payment processing must be transparent and safe.

Financial crimes
Consumer digital transactions are subject to the potential for financial crime, fraud, waste, and/or abuse in the areas of shipping and sales restrictions, sanctions, and tariffs as well as anti-money laundering risk.

Environmental, social, and governance policies
Investor and reputational demands for social and environmental sustainability are driving enhanced risk awareness, standards, and controls in the manufacturing and distribution of goods.

Divergent regulation
Current and evolving divergent regulatory activity at the local/state, federal, and global levels may impact such risks as taxes, data privacy, and licensing.
Drivers
— Proliferation of available digital data, spread across disparate systems and vendors
— Heightened regulatory awareness/expectations around consumer data protection
— Transforming the customer and digital experience through privacy-enhancing technologies to increase customer trust

Actions
— Be transparent with your data collection and use:
  Identify your personal information collection and usage purposes and give proper notice to users to enable them to make informed decisions
— Unlock privacy to demonstrate business value:
  Proactively enable privacy into your customer journeys to provide a differentiated user experience
— Empower users to take control of their data:
  Establish a platform for users to exercise their individual rights to access, correct, and delete their personal information
— Embed privacy into your design processes:
  Implement privacy-by-design (PbD) principles to minimize personal information collection without compromising functionality

Representative regulatory coverage areas
Data privacy including privacy impact assessments; individual rights of access, correction, deletion; third-party risk; incident response and breach management; and cross-border transfer agreements.
CA Consumer Privacy Act (CCPA), Other State Consumer Privacy bills/laws (WA, TX, HI, NY, etc.), EU GDPR, Brazil LGPD, India PDP (Draft), FCRA, FTC Act, US/EU Privacy Shield, China Cyber Security Law, Russian Federal Law on Personal Data, U.S. Chamber of Commerce framework, industry-specific regulations such as those implementing the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA)

Regulatory perspective
“By 2020, digitized data is forecasted to be generated at a level that is more than 40 times the level produced in 2009.”
— U.S. Treasury Report, A Financial System That Creates Economic Opportunities, Nonbank Financials, Fintech and Innovation, July 2018

“Privacy done right—putting the customer at the core of your privacy strategy—is a game changer. Regulations like CCPA, GDPR, and other similar global regulations provide incentive but compliance should be a by-product, not the end goal of a well-designed privacy program.”
— Driving Change: The time is now to prepare for changes to California’s privacy law, KPMG, August 2018
Drivers
— Gaining a 360-degree view of the customer to enable secure and personalized interactions
— Customer demand for access through multiple innovative technology channels
— Heavy focus on digital security and identity as a driver for business enablement
— A convergence of data collection, fraud prevention, and cybersecurity

Actions
— Implement cybersecurity across development:
   Include cybersecurity considerations in the development lifecycle, including secure and rapid design, testing, and implementation, and through to ongoing monitoring, testing, and reporting
— Design a frictionless registration and authentication customer experience: Measure the usability and experience across your customer identity experience
— Evaluate opportunities to adopt advanced authentication: Consider adopting advanced authentication methods such as touch or face ID or voice recognition in place of weak password authentication
— Focus on fraud reduction to enhance secure and personalized customer interactions: Understand your customer’s typical behavior to recognize anomalies and prevent fraudulent activity

Representative regulatory coverage areas
Cybersecurity, resiliency (adaptable tools); third-party data security; access management (enterprise, privileged, and consumer); encryption
NIST Cybersecurity Framework, NYDFS Cybersecurity Rule, CCPA, EU GDPR

Regulatory perspective
“Digital Identity Management is designed to support enterprise digital transformation initiatives, such as enabling digital commerce, personalizing omnichannel interactions, and building trust through respecting preferences and providing secure and seamless experiences for employees, business partners, and customers.

Driving customer engagement is a top priority for business leaders, and these experiences must be secure and consistent across all channels.”

“Traditional certification regimes are built around static risk. Cybersecurity risks constantly evolve; things that were certified as secure in the yesterday may well be insecure tomorrow. We need new mechanisms of governance and new market mechanisms to capture this evolving risk.”

— Diane Rinaldo, Deputy Assistant Secretary of Commerce for Communications and Information, National Telecommunications and Information Administration, OECD Global Forum Digital Security for Prosperity, December 13, 2018
Drivers
— Consumer demand for integrated, personalized products and services
— Public policy and regulatory attention on sharing and use of consumer data
— Demographic shifts and accessibility expectations of digital products
— Heightened attention to product safety and public safety/responsibility
— Class action and litigation cases

Actions
— **Upfront controls:** Build upfront controls in product digital design to allow for fair, unbiased access and treatment. Ensure disclosures, contracts, and online terms and conditions permit consumers to provide honest reviews. Establish an organizational policy and procedures to identify violative products and implement a recall plan, including reporting and notification requirements.
— **User testing:** Build user testing for consumer accessibility, usability, and transparency
— **Data protection:** Strengthen customer data protection program
— **Fraud protection:** Conduct consumer/investor and fraud protection assessments
— **Behavior analysis:** Invest in tools/capabilities to better analyze consumer-impacting employee and consumer behaviors, trends, and patterns. Evaluate and enhance surveillance and monitoring and testing. Consider AI applications that impact consumers - directly or indirectly - to be higher risk that should be subject to increased scrutiny and more frequent review

Representative regulatory coverage areas
- Accessibility, usability, fairness and transparency from advertising and marketing through delivery and fulfillment
- Data privacy; Unfair and Deceptive Acts and Practices, Fair advertising, Fair debt collections, Fair credit reporting, American’s with Disability Act, Telemarketing Sales Rule, Children’s Online Privacy Protection Act, Customer Review Fairness Act, Consumer Product Safety Act

Regulatory perspective

“The FTC’s Bureau of Consumer Protection stops unfair, deceptive and fraudulent business practices by collecting complaints and conducting investigations, suing companies and people that break the law, developing rules to maintain a fair marketplace, and educating consumers and businesses about their rights and responsibilities.”

— FTC Bureau of Consumer Protection

“Because the CPSC and firms have a common interest in consumer safety, CPSC staff and firms often work closely to agree on, implement, and communicate appropriate corrective actions. The degree of a firm’s cooperation is a factor taken into account in evaluating potential additional enforcement actions or penalties... The CPSC Office of Communications must review and agree upon press releases and social media-based communications that a company intends to use in a product recall before publication or dissemination... Firms should notify its customers using all available social media and mobile platforms.”

— CPSC Regulated Products Handbook
Drivers
— Risk to reputation/brand and liability as a result of platform economy negative assessment or comments
— Board and supervisory focus on effective monitoring and management of misconduct by employees, third parties, and partners/affiliates
— High-profile regulatory enforcement actions

Actions
— **Assess “soft controls”:** Continuously analyze your company’s overall and digital environment for clarity, role modeling, commitment, achievability, transparency, discussability, ability to call someone to account, and enforceability

— **Perform diligence risk analysis:** Perform diligence and monitoring checks for board, executives, and third parties; make brand and reputational risk management part of your business continuity/crisis response plan as well as scenario testing

— **Recognize the voice of the customer/employee:** Ensure employee hotlines are monitored and employee/customer complaints addressed

— **Uplift investigations processes:** Ensure appropriate investigation triaging, resolution, and reporting; provide appropriate governance, escalation, and transparency to findings and trends

**Representative regulatory coverage areas**
- Ethics and integrity, mitigation of fraud, waste, abuse and/or misconduct
- Ethics and Culture, Reputation, Sales practices, FTC UDAP, DOJ compliance program guidance, DOJ compliance program guidance, Foreign Corrupt Practices Act

**Regulatory perspective**

“Beyond compliance structures, policies, and procedures, it is important for a company to create and foster a culture of ethics and compliance with the law. The effectiveness of a compliance program requires high-level commitment by company leadership to implement a culture of compliance from the top…Prosecutors should examine the extent to which senior management have clearly articulated the company’s ethical standards, conveyed and disseminated them in clear and unambiguous terms, and demonstrated rigorous adherence by example.”

— U.S. Department of Justice, Criminal Division, Evaluation of Corporate Compliance Programs, updated April 2019

**The top compliance activities that CCOs are looking to enhance and improve:**

- Ethics 66%
- Investigations 65%
- Monitoring and testing 65%

**Source:** KPMG CCO Survey, April 2019

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International. NDPPS 982062
Drivers
— Increased reliance on third-party distributors and others representing an organization’s brand as consumer product companies and retailers try to solve for the last mile
— Risk to reputation/brand and liability from third-party supplier and distributor activities
— Board and supervisory focus on effective diligence and monitoring of third-party risk management, including conflicts of interest, anti-bribery and corruption, and misconduct by partners/affiliates
— High-profile consumer data and control lapses by third parties

Actions
— Perform enhanced due diligence: Expand and enhance diligence reviews of third and fourth-party providers, as appropriate, inclusive of those in the digital channel such as distribution firms, clearing houses, inventory firms, and software and cloud providers
— Ensure adherence to regulatory and compliance standards (inclusive of vendor code of conduct, SOC1 control requirements, etc): Conduct regular monitoring and testing of third parties to ensure compliance and appropriateness of ethics and compliance controls and activities
— Integrate third-party risk management across performance-based areas, jurisdictions, risk functions, and disciplines
— Automate and streamline third-party diligence and reviews through use of integrated workflow and cognitive learning technologies

Representative regulatory coverage areas
Supplier, distributor, and provider diligence and monitoring
Ethics and culture, reputation, Foreign Corrupt Practices Act, FTC UDAP, DOJ compliance program guidance

Regulatory perspective
“A company’s third-party due diligence practices are a factor that prosecutors should assess to determine whether a compliance program is in fact able to ‘detect the particular types of misconduct most likely to occur in a particular corporation’s line of business.’ ”

— U.S. Department of Justice, Criminal Division, Evaluation of Corporate Compliance Programs, updated April 2019
Drivers
— Historically siloed and narrow view of compliance now expanding to role in ethics and culture as well as recognition of compliance as a “trusted adviser”
— Recognized customer-centric business strategy with recognized obstacles without compliance in design/build ("security by design")
— Expectations by leadership for more “real-time” compliance risk management and insights
— Emerging technologies with applications for enhanced and/or customized customer experience (e.g., AI, machine learning, advanced analytics, bots) are changing the technology landscape
— Ongoing pressure to cut operating costs and improve productivity

Actions
— **Redefine the stature and mission of compliance:** Dispel the “checklist” or the “enforcer” perception of compliance and elevate the mission, the skills/talent, and the executive presence to make compliance a valued and trusted risk adviser with the business and to executive management and the board
— **Expand compliance metrics and data analytics,** including adoption of advances in data and behavioral analytics; application of emerging technologies must be monitored for fair customer treatment, clear and transparent disclosure, and the “explainability” of results

— **Demonstrate fair, unbiased treatment:** Demonstrate adequate review, examination, and investigation of customer complaints and platform reviews; demonstrate adequate review, examination, and investigation of AI decisions and outcomes for inherent biases
— **Evaluate regulatory change management,** including the capturing of regulatory changes and the maintaining of current inventories of regulatory obligations
— **Integrate compliance risk management activities,** including an agile interaction model and inclusion/alignment of compliance with business strategy
— **Automate/Achieve more “real-time” compliance** via investment in integrated case and workflow management and advanced technology functionality and analytics; focus on areas that reach and serve customers, inclusive of customer complaints, product recalls, and refunds; deploy tooling to better digitize governance within the organization

### Representative regulatory coverage areas
- Ethics and compliance program, consumer protection regulations
- Ethics & Culture, Truth in advertising, fair debt collections, consumer product safety, DOJ compliance program guidance, unfair and deceptive acts and practices

### Top compliance automation challenges

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misunderstood and/or insufficiently managed dependencies</td>
<td>39%</td>
</tr>
<tr>
<td>Leadership and/or stakeholder attention</td>
<td>36%</td>
</tr>
<tr>
<td>Insufficient metrics for measuring progress</td>
<td>35%</td>
</tr>
<tr>
<td>Unavailable resources</td>
<td>32%</td>
</tr>
<tr>
<td>Unavailable data or data did not have the anticipated integrity</td>
<td>26%</td>
</tr>
</tbody>
</table>

**Source:** KPMG Innovating compliance through automation, October 2018, based on an unpublished KPMG survey of CIOs and CCO across multiple industries
Drivers
— Faster payments, including real-time payments, and ubiquitous system
— Demands for transparent and safe payment processing
— Customer demands for multi-payment optionality with digital ease and speed

Actions
— **Fraud prevention**: Understand potential for fraud risks across consumer and business segments and conduct fraud assessments
— **Data protection and security**: Implement privacy by design (PbD) principles to minimize personal information collection without compromising functionality
— **Disclosure and fee transparency**: Ensure that consumer disclosures of fees and other transaction terms are complete, clear, and easily accessed
— **Payment processing and transaction fulfillment**: Strengthen governance, escalation, and transparency across all payment channels and options
— **Cross-border payment efficiency**: Enhance cross-border payments through payment file type translation innovation, improved trade finance processing, simplified messaging formats, and understanding emerging technology providers

---

**Third parties**: Leverage third-party service providers to simplify and/or accelerate the development/integration of multiple/alternate customer-facing payment services

---

**Representative regulatory coverage areas**

Consumer payment processing must be transparent and safe across the payment lifecycle including the consumer, merchant, third-party payment providers, and financial institutions.

Example requirements: Financial crimes - Anti-Bribery and Corruption (ABC) compliance, OFAC sanctions compliance, BSA/AML/KYC; Consumer protections – UDAP, ECOA/Reg B, TILA/Reg Z, FCRA, FDCPA, ADA; Data privacy – GLBA, PCI compliance, EU GDPR, EU PSD2 (open banking), CCPA; Funds Availability – NACHA operating rules, EFTA/Reg E/Reg CC, currency conversion, fee disclosures; Third-party risk management

---

**Regulatory perspective**

“Today, our payment system is again at a crossroads. There is a growing gap between the transaction capabilities we need and expect in the digital economy – fast, convenient, and accessible to all – and the underlying settlement cap abilities.

Faster payment innovations are striving to keep up with this demand, but gaps in the underlying infrastructure pose challenges associated with safety, efficiency, and accessibility.”

— Federal Reserve Governor Lael Brainard, Supporting Fast Payments for All, October 3, 2018

“Online shopping has become the norm for millions of Americans, but its growth has been accompanied by a trend no merchant welcomes: increasing e-commerce fraud...Payment tokenization should be part of the solution...but implementation concerns and lack of understanding about the security benefits, particularly in the e-commerce space, are among the factors holding it back.”

— Boston Federal Reserve, Industry Perspectives on the Evolution of EMV Payment Tokenization, Susan M Pandy and Marianne Crow, September 2018, and blog post by Jay Lindsay, March 12, 2019
Drivers
— Availability of new technologies and ability of financial crime networks and individuals to perpetuate crimes on large scale
— Regulatory expectations for increased integration and improved risk management abilities for preventing and detecting potential financial crime activity
— Divergent regulations on sales restrictions, sanctions, and other prohibitive business activities

Actions
— Evaluate need for data analytics and emerging technologies to predict, detect, and respond to financial crimes risks
— Automate compliance processes
— Integrate processes for greater agility, cost savings, consistency, and refined risk evaluation
— Plan for potential regulatory changes—sanctions refinements, monitoring and reporting human trafficking, and shared platforms/arrangements

Representative regulatory coverage areas
Fraud, waste, and/or abuse; shipping and sales restrictions, sanctions; tariffs; anti-money laundering; crypto assets
ABC compliance, shipping restrictions, sales restrictions, Office of Foreign Assets Control (OFAC) sanctions compliance, tariffs, AML

“Many organizations conduct screening of their customers, supply chain, intermediaries, counter-parties, commercial and financial documents, and transactions in order to identify OFAC-prohibited locations, parties, or dealings. At times, organizations have failed to update their sanctions screening software to incorporate updates to the SDN List or SSI List, failed to include pertinent identifiers such as SWIFT Business Identifier Codes for designated, blocked, or sanctioned financial institutions, or did not account for alternative spellings of prohibited countries or parties.”

— Root Causes of OFAC Sanctions Compliance Program Breakdowns, Framework for OFAC Compliance Commitments, OFAC, Department of the Treasury, May 2019
Drivers
— Investor and reputational demands for corporate social responsibilities and ESG compliance and disclosures
— Enhanced risk awareness, standards, and controls in the manufacturing and distribution of goods
— Board and executive management focus on corporate ESG responsibilities, meeting regulatory requirements, and controls for ESG management

Actions
— **Level set:** Agree on material ESG topics that are important to the company and its stakeholders
— **Assessment:** Determine which ESG risks and opportunities (physical and transitional, including regulatory change management) are of strategic significance to the company
— **Integration:** Encourage integration of strategically significant ESG issues into the business strategy
— **Stakeholder communications:** Shape the company’s key ESG messages/disclosures to investors and other stakeholders in the context of strategy and long-term value creation
— **Board oversight:** Ensure that the board has the right composition, structure, and process to oversee ESG in the context of strategy and long-term value creation

Representative regulatory coverage areas
— Environmental – water and waste management, natural resource scarcity, climate change impacts; Social–human trafficking, child labor, diversity and inclusion, supply chain management; Governance–workplace and safety compliance, political contributions, ethics and compliance, board accountability
— Example requirements: environmental compliance (OSHA, EPA), workplace and safety compliance (OSHA), transportation safety (DOT, FAA), Equal Employment Opportunity, data privacy/cybersecurity, sanctions compliance (OFAC)

**Regulatory perspective**

“CEOs are also very mindful of creating values that there customers expect from today’s businesses. Eighty-one percent feel that it is their personal responsibility to ensure that their company’s ESG policies reflect the values of their customers.”
— KPMG, 2019 U.S. CEO Outlook

“S&P Global Ratings ESG Evaluation is a cross-sector, relative analysis of an entity’s capacity to operate successfully in the future and is grounded in how ESG factors could affect stakeholders and potentially lead to a material direct or indirect financial impact on the entity.”
— S&P Global Ratings, April 11, 2019 (webpage accessed July 8, 2019)
Drivers
— Rapid advances in technology are reshaping access to and delivery of consumer goods and services
— Public policies are lagging the deployment of new distribution channels and new technologies
— Federal, state, and foreign jurisdictions act independently; multiple regulators may have jurisdiction over data, technologies, or technology providers and regulations from different agencies may conflict

Actions
— Apply existing “pre-regulations”: Acknowledge existing laws and regulations as pre-regulatory applications
— Consider other regulations, policies, and principles: Review policies and regulations in other jurisdictions for examples of possible future technology/distribution
— Monitor regulatory change: Identify new legislation or other requirements applicable to the good, service, distribution channel, third party provider, etc.
— Participate in industry and standard-setters’ efforts to develop standards and work with regulators to develop guardrails, as appropriate

Representative regulatory coverage areas
Public policies are lagging technology development, and regulators are looking to existing requirements as “guardrails.” State, federal, and global regulatory requirements differ.
Example requirements: Licensing, taxes, cannabis regulation, CCPA, GDPR

“Regulatory perspective
“The United States does not have a comprehensive internet privacy law governing the collection, use, and sale or other disclosure of consumers’ personal information… Congress should consider developing comprehensive legislation on Internet privacy that would enhance consumer protections and provide flexibility to address a rapidly evolving Internet environment.”
— GAO, Internet Privacy, January 2019 (GAO-19-52)

“As part of the American AI Initiative, federal agencies will also work to build public trust by exploring regulatory and non-regulatory approaches to govern new AI applications. To this end, the White House…will work with regulatory agencies and other stakeholders to craft guidance for AI technologies that will promote innovation while respecting privacy, civil liberties, and American values.”
— Michael Kratsios, Deputy Assistant to the President, Op-Ed published on Wired.com, February 11, 2019 following Executive Order on Maintaining American Leadership in Artificial Intelligence, February 11, 2019
Conclusion

The availability of information has empowered consumers like never before. Today, consumers expect retail organizations to offer personalized products and services, an effortless experience across channels, reliable privacy protections, evidence of good corporate citizenship, and value for their money. They will remain loyal only if a brand meets these needs.

Digital technologies offer consumer and retail companies the ability to transform consumer data into real customer insights, enhance customer experience, and meet customer expectations. However, the transformation to digital data combined with the volume of available data and its application to predict consumer behavior creates a complex and interconnected business environment that crisscrosses industry and regulatory boundaries and raises questions of ethics and conduct around the use of consumer data.

Lawmakers and regulators in the U.S. and globally are increasingly focused on revamping regulatory frameworks to ensure the parties to all consumer data touchpoints are covered by data privacy, data security, competition policy, and fairness provisions. This patchwork of multiple and differing laws and regulations greatly increases the regulatory uncertainty, complexity, and risk that firms face. Further, as new protections are introduced at various levels, expectations for an overarching policy framework increase and likely extend the timeframe for debate.

In anticipation of future changes, consumer and retail companies need to assess their digital transformation and related data strategies with agile incorporation of controls to address technology, security, and compliance risks. They should also look to supplier and third-party procurement and vendor risk management from due diligence through to ongoing monitoring to assure they can address the same risks with similar agility.
Bringing it all together

Change is coming quickly. Ethics and compliance roles, responsibilities and expectations have evolved and progressive organizations will continue to look for opportunities to integrate ethics and compliance throughout their organization and use automation to facilitate an ethical and compliant organizational culture.

The ethics and compliance path

<table>
<thead>
<tr>
<th>Today, ethics and compliance is...</th>
<th>In the future, ethics and compliance will be...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Culture</strong></td>
<td>More formalized, integrated, and reinforced. Cultural expectations will be further embedded enterprise-wide in activities, addressing expectations for behavior, actions, and emphasis on &quot;moment that matter&quot;/ethical dilemmas.</td>
</tr>
<tr>
<td>A defined and communicated compliance culture, including expected behaviors and values.</td>
<td>Integrated through additional governance and/or communication channels, with the Board and additional functions—HR, finance, IT, and more—firmly engaged in ethics and compliance initiatives.</td>
</tr>
<tr>
<td><strong>Governance</strong></td>
<td>More fully automated processes across enterprise-wide operational activities, and increased focus on integration with GRC technology, data availability and accuracy, and tools that support advanced predictive analytics. Further integration of the 1st and 2nd lines of defense through process convergence and real time monitoring/testing.</td>
</tr>
<tr>
<td>A defined structure, either centralized, decentralized or a hybrid, with oversight from the Board.</td>
<td></td>
</tr>
<tr>
<td><strong>Process</strong></td>
<td>More formalized and automated risk assessment process, aggregating data enterprise-wide in a consistent standards and terminologies, capable of aggregation into a GRC/ERM assessment. Data and analytics are leveraged to enhance effectiveness and proactively identify control environment weaknesses.</td>
</tr>
<tr>
<td>Standardized processes to facilitate compliance and ethical behaviors, and which increasingly leverage data analytics (dependent upon data integrity).</td>
<td>More fully automated processes across enterprise-wide operational activities, and increased focus on integration with GRC technology, data availability and accuracy, and tools that support advanced predictive analytics. Further integration of the 1st and 2nd lines of defense through process convergence and real time monitoring/testing.</td>
</tr>
<tr>
<td><strong>Risk assessments</strong></td>
<td>Further integrated through policy management controls, testing and monitoring and automation of version control efforts; proactive identification and communication when violation occur as well as when updates are needed based on a robust regulatory inventor approach.</td>
</tr>
<tr>
<td>Standard, consistent and frequent compliance risk assessment efforts, based upon defined methodologies, tools and templates</td>
<td></td>
</tr>
<tr>
<td><strong>Policies, procedures and code of conduct</strong></td>
<td>More dynamic and pushed out to employees based upon real-time trigger events that spark need for training to reinforce ethics and compliance concepts.</td>
</tr>
<tr>
<td>Policies and procedures that align with implemented processes and are subject to policy management protocols; regulatory changes are integrated; and the code of conduct is regularly refreshed.</td>
<td>More dynamic and pushed out to employees based upon real-time trigger events that spark need for training to reinforce ethics and compliance concepts.</td>
</tr>
<tr>
<td><strong>Training and communications</strong></td>
<td>Leveraging automation to achieve greater monitoring and testing risk coverage, and supplementing work completed by the 1st line, in consideration of the organization’s annual risk-based plan (with detailed control testing linked to regulatory risks).</td>
</tr>
<tr>
<td>Organization-wide compliance trainings and communications, tailored to staff roles/responsibilities; reinforce culture, values and behavior.</td>
<td>Marked by greater investigative insights that are aggregated across the enterprise for a more reflective vision of risks, supported by KRIs/KPIs and data analytics that enable the organization to proactively address risks through more predictive assessments.</td>
</tr>
<tr>
<td><strong>Monitoring and testing</strong></td>
<td>Able to achieve more integrated reporting based upon further automation and a technology infrastructure that has greater connectivity and aggregation potential.</td>
</tr>
<tr>
<td>Dedicated resources and clear procedures for testing control design and operating effectiveness.</td>
<td></td>
</tr>
<tr>
<td><strong>Investigations</strong></td>
<td></td>
</tr>
<tr>
<td>Channels to raise concerns related to issues and investigations, which are then triaged based upon the content of the allegation for resolution; metrics may be based upon silo’ed data.</td>
<td></td>
</tr>
<tr>
<td><strong>Reporting</strong></td>
<td></td>
</tr>
<tr>
<td>Frequent and consistent reporting based upon robust organization-wide policies and procedures.</td>
<td></td>
</tr>
</tbody>
</table>

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International.
Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.