Streamlining
to create value

The future of compliance
Organizations want to stay on the positive side of regulatory, compliance, and ethical risks while increasingly looking at how best to bridge business and compliance objectives. As such, the promise of artificial intelligence and automation gives rise to hopes of reducing and optimizing operational and compliance spend. While regulatory technology (RegTech) has great value across industries and is gradually being adopted, organizations must first reassess their core processes and controls in order to drive more streamlined governance while enhancing risk management and mitigation. Whether called convergence, integration, transformation, or optimization, all firms should look to three core elements in this process:

1. **Redesign skills and roles**

2. **Align risk and controls**

3. **Consolidate testing, surveillance, and investigations**
Redesign skills and roles

Often undervalued and yet critical to streamlining efforts are the buy-in, skills, and talent needed to set risk strategy and embrace changes in skills and roles. Compliance and ethics risk professionals must be change agents with great judgment as well as analytical and communication skills. This is even more critical in a time of advanced digital technology, agile business operations, and changing customer expectations. They also must be supported by skilled compliance and ethics professionals with the human and technology savvy to understand and apply information to human interactions in a fast-changing global business environment increasingly impacted by disruptive technologies. Likewise, business leaders must appreciate and prioritize the efficacy of compliance and ethics risk prevention, detection, and response above simply cutting costs.

As such, accountability for compliance and ethics is critical and should be both well understood and documented, with sufficient organizational stature and independent critical challenge. Compliance and ethics must also be an integral and respected partner with all areas, including its human resources and legal counterparts to drive forward ethics and culture programs; technology to drive automation, incident response, and privacy programs; and the front line to streamline onboarding, operational control effectiveness assessments, and employee, transactional, and vendor monitoring.

### Key skills

- Is cerebral and strategic
- Does not wait for authority to be given
- Aligns risks and program with the company’s vision
- Is comfortable with raising issues and asking for help
- Creates a culture of compliance
- Is thought provoking – Not reactive
- Must be fast and responsive in agile environment
- Acts as a change agent

### Leadership qualities

- Has the respect of senior leadership within the enterprise
- Protects the best interests of the company but not at the cost of the customer and doing what’s right
- Understands the organizational culture, including both strengths and gaps
- Understands the legal, regulatory, social, and economic factors impacting the company
- Quickly adapts to an ever-changing compliance environment

### Efforts to embrace streamlining and compliance automation are challenged by various factors including:

- Dependencies not understood in advance and/or not understood and managed sufficiently throughout (39%)
- Attention of leadership/stakeholders (36%)
- Insufficient metrics for measuring progress (35%)
- Lack of resources (32%)
- Lack of subject matter knowledge (29%)

Source: KPMG Compliance Automation Survey (2018), [unpublished].
Alignment of risk and controls

An alignment of risk and controls is needed to drive consistency around how to identify relevant compliance, ethics, and reputation risks; how to conduct assessments that are aligned to and informed by the realities of the company’s business operations; how to leverage output and quantify potential impact for business purposes; and what should be communicated to key stakeholders.

Most organizations do not have a central point to manage how new risk assessment requirements are implemented and how existing risks are mapped to the appropriate functional level of business controls. Meanwhile, their leadership is seeking to view risks and controls through a single lens for multiple purposes and communicate this information consistently in automated dashboards. Improving the content such that it clearly ties to business objectives and reduces redundancy can help encourage the appropriate level of focus on the part of the right senior resources.

Only 1 in 5 CCos and CIOs said they have an enterprise-wide strategy to better align risks and controls by automating compliance activities. Organizations have placed a priority on:

- **56%** Risk assessments
- **40%** Policy management
- **40%** Regulatory change management
- **39%** Due diligence
- **34%** Monitoring and testing

Source: KPMG Compliance Automation Survey (2018), [unpublished].
## Convergence continuum

<table>
<thead>
<tr>
<th>Category</th>
<th>Not converged</th>
<th>Partially converged</th>
<th>Fully converged</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Timing and assessment process</strong></td>
<td>Assessments take place at different times (e.g., quarterly, annually, as needed)</td>
<td>Some but not all assessments are aligned in implementation timing and reporting of results</td>
<td>The organization assesses once using the same process with aligned preparation, execution, and reporting time frames</td>
</tr>
<tr>
<td><strong>Governance</strong></td>
<td>Each assessment is governed by an independent body</td>
<td>Some degree of coordination among governing bodies but decisions are still made in silos</td>
<td>Centralized management of methodology, implementation, and sign-off</td>
</tr>
<tr>
<td><strong>Challenge/validation/control testing</strong></td>
<td>Challenge, validation, and controls testing occur in silos or are not performed</td>
<td>Partial integration of challenge, validation, and control testing activities into assessment program</td>
<td>Center of excellence for challenge, testing, and validation of assessment inputs and outputs</td>
</tr>
<tr>
<td><strong>Sign-off/attestation</strong></td>
<td>Assessment sign-off conducted independently</td>
<td>Some but not all assessments are aligned in sign-off timing; participants attest once for several assessments</td>
<td>Integrated sign-off structure</td>
</tr>
<tr>
<td><strong>Risk and control rating criteria</strong></td>
<td>Each assessment uses a unique rating methodology</td>
<td>Some but not all assessments are aligned in ratings definition and criteria</td>
<td>Single rating methodology used for all assessment types</td>
</tr>
<tr>
<td><strong>Assessment granularity</strong></td>
<td>Level of granularity varies greatly among assessments</td>
<td>Granularity of data is agreed within lines of business</td>
<td>Framework accommodates varying degrees of granularity across the organization and as needed by assessments</td>
</tr>
<tr>
<td><strong>Risk and control taxonomy</strong></td>
<td>Taxonomy is unique to assessments</td>
<td>Key assessments are aligned in risk and/or control taxonomy</td>
<td>A single risk and control taxonomy exists for all assessment purposes</td>
</tr>
<tr>
<td><strong>Library of risks and controls</strong></td>
<td>A standard library of risks and controls does not exist</td>
<td>Standardized libraries are leveraged by lines of business or assessments</td>
<td>Risk and control catalog is utilized for all assessments and across the firm</td>
</tr>
<tr>
<td><strong>Tools and technology</strong></td>
<td>Assessments are conducted in silos with desktop software or independent vendors</td>
<td>Tools exist for collecting and reporting on assessment data but are built for a single purpose</td>
<td>A common set of tools exists to facilitate all assessment types</td>
</tr>
<tr>
<td><strong>Reporting</strong></td>
<td>Reports are designed for a singular purpose</td>
<td>Reports exist and meet the needs of a single assessment or line of business with limited integration of other assessment activities</td>
<td>Centralized, standardized reporting exists that meets the needs of both the firm and regulators and integrates the outputs of other assessment activities</td>
</tr>
</tbody>
</table>

© 2018 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 790997
Consolidation of testing, surveillance, and investigations

Inefficiencies across the organization usually increase based on the number of disparate testing, surveillance, and investigation programs. This may lead to an inability to detect root cause and/or systemic issues. Increasingly, organizations are looking to both automate and consolidate testing, monitoring, and surveillance activities through constituent standards, plans, scripts, and reporting.

Likewise, prior disparate investigation units are increasingly sharing appropriate data and/or consolidating units in an effort to both gain greater efficiencies as well as to increase knowledge that may help to drive positive cultural and ethical change.

To get started, all organizations should:
1. Inventory risk and control source systems
2. Standardize naming conventions, definitions, and attributes
3. Rationalize risks and control inventories and align to common taxonomy
4. Inventory existing control testing, monitoring, and surveillance activities
5. Assess testing, monitoring, and surveillance objectives, scope, methodologies, and granularity
6. Identify technology platforms, including data sourcing agreements
7. Identify available key behavioral analytic and control metrics.

Six key pillars of an effective controls testing program:

1 KPMG Compliance Automation Survey (2018), [unpublished].

© 2018 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 790997
Measure the potential benefits and costs

Potential benefits:

**Enhanced effectiveness**
- Metrics/data analytics help to identify areas of greatest risk and uncover trending risks through forward looking analytics
- Greater consistency

**Greater efficiencies**
- Reduced operating and compliance costs
- Process optimization
- Streamlined and defined workflows

**Better management of compliance risks**
- A more tailored risk based approach
- Aggregated view of risks

**Improved regulatory management**
- Ability to lower regulatory exposure
- Improved readiness to support regulatory inquiries

**Expanded testing and monitoring coverage**
- Timely identification of risks and quick response

**Improved resource allocation**
- Deploy individuals to the most impactful activity (reallocation)
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.

© 2018 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.