



# Modernizing compliance risk assessments



# Making the case: Benefits of modernizing your compliance risk assessment

As the financial services industry continues to evolve, Financial Institutions (FIs) are exposed to more risks than ever before. The changing regulatory landscape and FI's increasingly complex operational structures introduce new compliance risks that must be assessed and mitigated. Simultaneously, as regulators have increased their expectations for more robust risk frameworks, FIs must continue to evaluate whether they adequately capture and assess the risks their organization faces to align with regulatory expectations.

As organizations expand product and service offerings and incorporate new technologies into their operations, managing new and more complex compliance risks becomes increasingly challenging, resource-intensive, and more difficult to achieve the necessary level of risk mitigation.

## Drivers for change:

1

### Lack of technology

FIs often rely on dated technologies and manual processes that could be enhanced by implementing modern technology architecture and utilizing artificial intelligence and other automation solutions.

2

### Organizational size and complexity

As FIs and their product offerings grow in size and complexity, their compliance profiles have become more challenging to assess.

3

### Regulatory impacts

As FIs expand their products, services operations and the jurisdictions they serve, they are subject to additional state, federal, and international regulatory requirements.

Compliance risk assessments (CRAs) are a critical component of a risk management framework intended to help organizations capture and assess their risk exposure. However, many organizations use outdated methods to conduct their CRAs and often rely on manual processes and antiquated tools that have not kept pace with the expanded scale and complexity of their risk profiles. FIs have the opportunity to enhance and modernize their CRA process to control for and address these inefficiencies.



# Revisiting the CRA framework and methodology

Effective CRA frameworks allow FIs to capture the appropriate compliance risk(s) posed by their products, processes, and services while aligning with their organizational goals. While framework architecture may differ among institutions, similar elements are typically

deployed across complex FIs and risk management program maturity levels. FIs should consider the following practices to modernize their CRA frameworks across each of these components

1

## Align and refresh foundational data elements

FIs must have confidence that the foundational data elements of their CRA framework are comprehensive and accurate. To facilitate an effective assessment process, FIs must design processes to review and refresh their foundational data elements. To do so, FIs should:

- **Review and refresh regulatory inventories.** Regulatory inventories must comprehensively capture the applicable laws, regulations and requirements that the organization must comply with. As organizational complexity, products, services and regulatory requirements evolve, the regulatory inventory must evolve accordingly. FIs should not only perform a comprehensive review of their inventories to gain comfortability that they are accurately capturing all areas of regulatory exposure but must also design sustainable processes for ongoing accuracy and comprehensiveness.
- **Evaluate and update product mappings.** FIs should review their product mappings to confirm they correctly mapped and categorized according to their associated compliance risks and regulatory requirements. As product offerings and features expand, product mappings must be continuously evaluated and updated as needed.
- **Accurately capture the control environment.** FIs should create and maintain a comprehensive inventory wherein controls are accurately mapped to the applicable products, services and regulatory requirements. The control inventory must be continuously assessed and updated to reflect changes to allow for accurate assessment results. As the organization evolves through implementing new core platforms or other tech architecture, the underlying foundational data elements of these transformational programs must also be continuously assessed.



3

# Enable agile risk assessments

An agile CRA framework not only empowers adaptability and prioritization capabilities but also can eliminate resource drag while enabling more real-time assessment activities.

To enable more agile CRAs, FIs should focus on the following:

- **Design and implement triggers to prompt assessment activities.** Effective triggers must capture events or circumstances that indicate a change in risk exposure for a particular assessment unit within a broader structure. In practice, FIs should review the trigger and risk impact of the assessment unit at time of risk change and can review the entirety of the structural unit data on a less frequent basis. FIs should design triggers based on changes in regulations, internal policies or business operations, as well as findings from regulatory exams or audits, customer complaints, enforcement actions or other market developments. Triggers should also capture operational changes such as mergers, acquisitions, product expansion or technology implementation.. As the effectiveness of triggers is dependent on the data inputs, FIs must also establish ongoing processes to review the underlying data quality and accuracy.
- **Define risk-rankings to drive risk-based assessments.** Criteria for risk-based assessments should differentiate between high, medium and low-risk areas based on likelihood and severity of regulatory violations, the effectiveness of existing controls and the overall organizational risk appetite. CRAs should be prioritized based on the potential impact and likelihood of non-compliance to allow effective resource allocation, prioritize high-risk areas and tailor compliance actions to address the MOST significant organizational risks



# Use technology to your advantage

A crucial component of modernizing a CRA framework is implementing technology solutions in place of outdated tools and manual processes to drive efficiency and effectiveness. To integrate solutions, FIs should:

- **Determine and leverage the right tools.**  
Understand the specific needs and objectives of risk assessment processes and evaluate against the features and functionality of available solutions. Tools should enable automation of repetitive tasks, collect and analyze data from various sources and centralize data management. FIs should prioritize advanced analytics tools to identify patterns, trends and anomalies in current and historical data. To gain a comprehensive and holistic view of organizational risk, tools should promote connectivity to other programs by facilitating efficient data sharing, collaboration and reporting across departments in support of an integrated risk framework.
- **Enhance monitoring with data visualization tools.**  
Data visualization tools should transform complex data into easily comprehensible visual representations, enabling stakeholders to quickly analyze and identify potential impacts for timely and informed decision-making. FIs should incorporate tools to aid in monitoring activities and support the early identification of emerging risks and changes in risk levels to support proactive risk management.
- **Use reporting to drive consistency and clarity.**  
FIs should create standard reporting templates tailored to stakeholders, such as board and management, and design ad hoc reporting criteria to address emerging risks or other specific areas of concern. FIs should also define, review and establish aggregation methodologies to provide a comprehensive view of the organizational risk profile, capturing the various business units, products, and regulatory focus areas.



# Conclusion

Modernizing the CRA framework can offer significant benefits across the organization. First and foremost, modernization leads to improved risk management that can reduce the cost of compliance. Risk and compliance professionals should clearly articulate the need to invest in modernizing the CRA process, noting the return on investment achieved through reducing compliance costs such as regulatory penalties and potential third-party fees as well as nonmeasurable costs like reputational damage, brand erosion, and negative community perception. An enhanced CRA process also empowers employee morale by allowing risk management personnel to focus on strategic growth-oriented activities and support the organization's efforts to protect customers.

Applying the discussed elements and principles to modernize the CRA process can result in a more sustainable and interconnected program that can better respond to regulatory changes, new products and services, new technologies, and digital delivery channels that change the organizational risk profile.

From an efficiency and resourcing standpoint, modernizing the CRA framework allows for better optimization and further cost efficiencies. By streamlining processes, better utilizing employee resources, and refining strategies, FIs can achieve greater operational efficiency. This optimization reduces costs and further enhances the overall effectiveness of organizational risk management.

Modernizing the CRA framework improves risk management, increased program sustainability and flexibility, and cost optimization. Through proactively addressing deficiencies, FIs can position themselves for long-term success in a rapidly evolving regulatory and risk landscape.



# How KPMG can help

KPMG LLP (KPMG) has helped organizations improve their CRA framework and methodologies by modernizing their historical approaches to be more dynamic and identify risks in a constantly changing regulatory environment.

To help, KPMG provides various services and tools, including:

- Current state CRA assessment
- Design CRA framework and target operating model
- Implement CRA framework and tech/GRC capabilities
- Build foundational data elements
- Perform control mapping and rationalization
- Facilitate CRA execution



## Contact us



**Todd Semanco**

Partner, Financial Services Risk,  
Regulatory & Compliance  
T: 412-232-1601  
E: tsemanco@kpmg.com



**Mike Lamberth**

Partner, Financial Services Risk,  
Regulatory & Compliance  
T: 804-241-2795  
E: mlamberth@kpmg.com



**Chad Polen**

Partner, Financial Services Risk,  
Regulatory & Compliance  
T: 412-491-6006  
E: cpolen@kpmg.com



**Hernando Garcia**

Director, Financial Services Risk,  
Regulatory & Compliance  
T: 212-954-3287  
E: hernandogarcia@kpmg.com

Authored by Scott Page, Andrew England, Avery Moore, and Arianna Haynes

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

Learn about us:



[kpmg.com](https://kpmg.com)