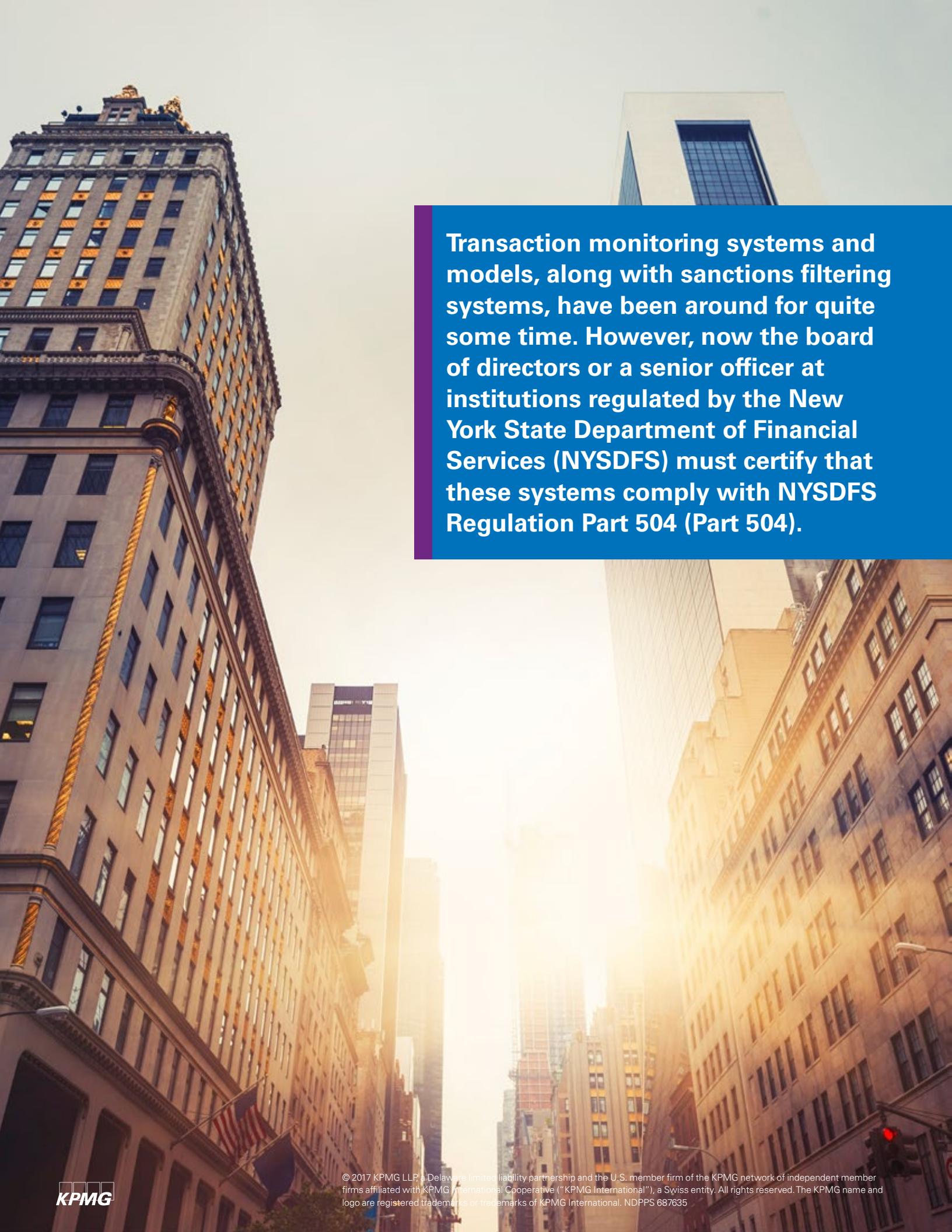




# The roadmap to certification

**Time is of the essence for complying with  
NYSDFS Regulation Part 504**



**Transaction monitoring systems and models, along with sanctions filtering systems, have been around for quite some time. However, now the board of directors or a senior officer at institutions regulated by the New York State Department of Financial Services (NYDFS) must certify that these systems comply with NYDFS Regulation Part 504 (Part 504).**

Institutions have shown various levels of sophistication in the development, implementation, maintenance, and testing of both transaction monitoring and sanction filtering systems—and in some cases, this is the genesis of the concerns raised by NYSDSFS.

Assessments of such systems—whether internal, third party, or regulatory—have shown varying degrees of weakness. A prime regulatory concern is that a failure in even one area may result in a significant number of potentially suspicious or prohibited transactions going undetected. This could result in the facilitation of money laundering or terrorist financing, or business being conducted with sanctioned individuals, entities, or countries.

Part 504 became effective on January 1, 2017, with the first annual certification due April 15, 2018.<sup>1</sup>

Now is the time for institutions to develop a plan around certification. Institutions must consider not only how robust their transaction monitoring and filtering programs are, but also how these programs are managed and tested over time. This regulation exposes the board or senior officer to significant risk if that certification is based upon incomplete or inaccurate data, a faulty system, or a faulty assessment of the system.

## Part 504: Summary

On June 30, 2016, the NYSDSFS published Part 504—Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications. The regulation requires regulated financial institutions (FIs), chartered pursuant to New York Banking Law and all branches and agencies of foreign banking corporations licensed pursuant to the Banking Law to conduct banking operations in New York, to maintain:

- A Bank Secrecy Act (BSA)/anti-money laundering (AML) transaction monitoring system
- A filtering program designed to restrict transactions prohibited by Office of Foreign Assets Control (OFAC)
- Minimum requirements governing the management and oversight over the transaction monitoring and OFAC filtering systems that are to be certified annually by the board of directors or a senior officer.

Specifically, Part 504 applies to all FIs regulated by NYSDSFS, including banks, branches/agencies of foreign banking organizations (FBOs), savings and loan associations, trust entities, private banking entities, and savings banks. The regulation also applies to NYSDSFS regulated non-FIs including check cashers and money transmitters.

Part 504 took effect on January 1, 2017, and will require a Board resolution or Senior Officer Compliance Finding (hereinafter also referred to as “certify,” “certification” or “certified”) to submit its first annual certification covering calendar year 2017 by April 15, 2018.

While Part 504 codifies, to some extent, existing regulatory expectations, the law also sets firm parameters and requirements that all regulated and non-regulated FIs must meet, not all of which are fully defined. For some FIs, this may require more investment in compliance resources and technology infrastructure changes than others.

<sup>1</sup> The Final Rule was issued after a series of record-setting fines and significant enforcement actions against financial institutions for violations of BSA/AML and OFAC laws and regulations. (See NYSDSFS Part § 504.1)

# Understanding Part 504

## What does Part 504 cover?

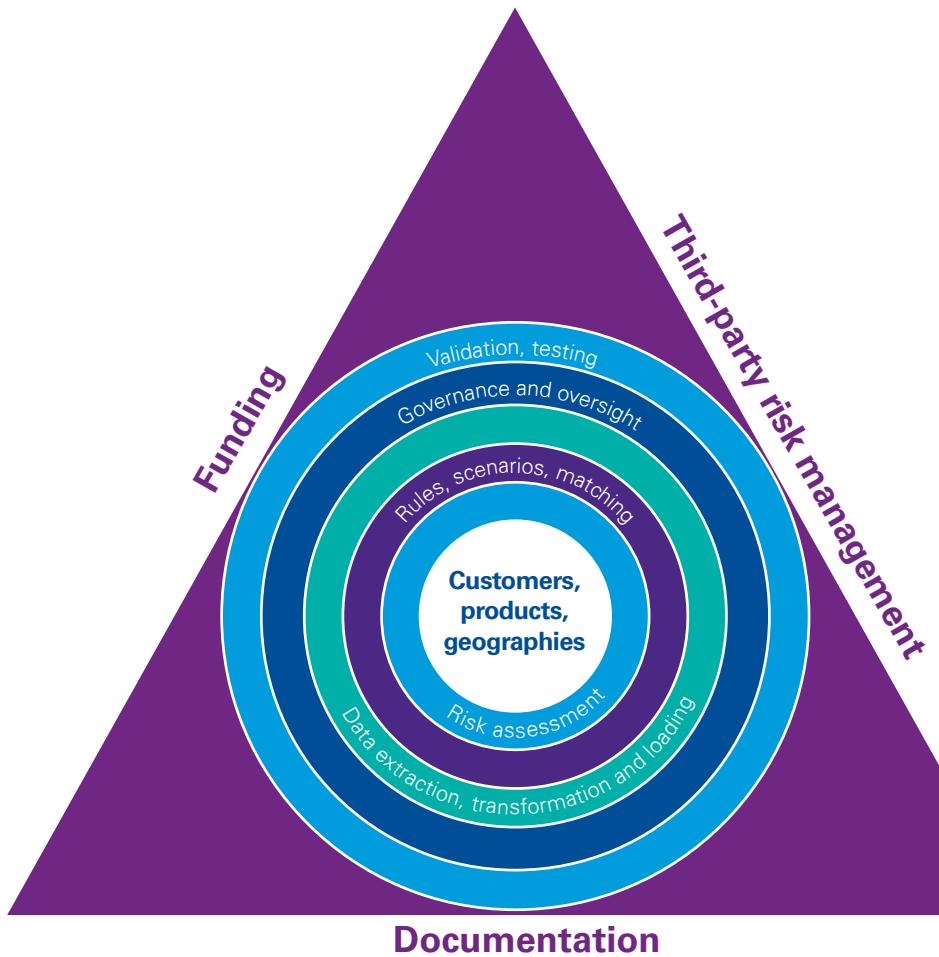
Part 504 covers both transaction monitoring systems designed to "monitor transactions after their execution for potential BSA/AML violations and suspicious activity reporting"<sup>2</sup> and filtering systems "interdicting transactions that are prohibited by OFAC."<sup>3</sup>

In each instance the programs must be "reasonably designed" to achieve their objectives. It is this reasonable

design that is the essence of the certification that must be submitted each year and sets forth two key areas of focus for the institution: program design and program testing.

## What should organizations be doing to prepare?

For both the transaction monitoring and the filtering programs, the foundation is the customer base, the products and services provided, and the geographies involved.



<sup>2</sup> See NYDFS Part § 504.3 (a).

<sup>3</sup> See NYDFS Part § 504.3 (b).

- **The institution must perform an enterprise-wide risk assessment to identify its BSA/AML or OFAC/sanctions risks.** Each of the BSA/AML risks should be tied to a rule or scenario designed to identify potentially high-risk transactions, and each customer and/or counterparty, as well as country, should be subject to appropriate OFAC/sanction name screening. This should result in data being extracted from relevant systems and analyzed, as necessary, to facilitate the execution of the rules or scenarios, as well as the name screening.
- **There must be a sustainable governance and oversight mechanism in place** to monitor the effectiveness of the program and manage changes to the program, including customer types, products and services, geographies, data, systems, rules and scenarios, and matching logic. Further, each component must be supported by policies and procedures as well as funding to ensure compliance and oversight of any third parties involved in the program.

#### **What are the risks?**

The regulation stipulates that it “**will be enforced pursuant to, and is not intended to limit, the Superintendent’s authority under any applicable law.**”<sup>4</sup> One can surmise from this that institutions will potentially find themselves facing increased scrutiny regarding the robustness of their programs. Further, one could reasonably expect increased and stronger enforcement actions, particularly when a board or senior officer has certified the programs and the program is later called into question by the Superintendent.

In particular, the specter of personal liability is once again raised when considering potential enforcement actions against individuals involved in the program and those who certify compliance. What’s more, if it is found that the certification submitted was knowingly false, there could be other consequences.

<sup>4</sup> See NYDFS Part § 504.5.

## Enterprise Risk Management

Enterprise Risk Management is a process, effected by an entity’s board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

—Enterprise Risk Management – Integrated Framework, Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004



## **What is the suggested approach to full compliance and certification?**

When determining how best to move forward, it is important to consider a framework in which to address the requirements of Part 504. A framework keenly suited to this is Enterprise Risk Management – Integrated Framework (ERM-IF) as published by COSO in 2004.

The ERM-IF is geared toward achieving an entity's objectives, set forth in four categories:

1. Strategic – High-level goals, aligned with and supporting its mission
2. Operations – Effective and efficient use of its resources
3. Reporting – Reliability of reporting
4. Compliance – Compliance with applicable laws and regulations.

While these categories may not be mutually exclusive, it is the last category that establishes the ERM-IF as a framework for compliance with Part 504.

### **Tone at the top**

Effective risk management and compliance starts with tone at the top. This can vary from strong, engaged, committed directors and senior officers, to ignorance of the risks and compliance requirements, to willfully ignoring requirements. Without a strong, committed tone at the top, the other components of ERM-IF (objectives setting; event identification, risk assessment, risk response, control activities, information and communication, and monitoring) will be adversely impacted.

Further, when examining the components of an ERM-IF, there is a clear linkage to the Part 504 framework:

**The internal environment encompasses the tone of an organization, and sets the bases for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and environment in which they operate.**

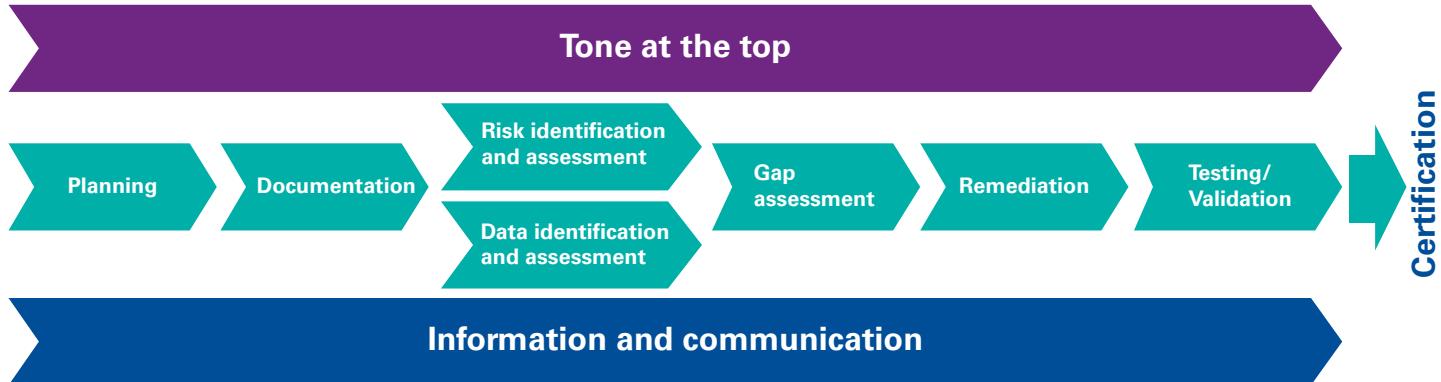
—Enterprise Risk Management – Integrated Framework,  
Committee of Sponsoring Organizations of the Treadway  
Commission (COSO), 2004

When examining the components of an ERM-IF, there is a clear linkage to the Part 504 framework.

#### Enterprise Risk Management – Integrated Framework



#### Part 504 framework



# Steps to certification

## Planning

Establishing a plan early on is key to positioning your organization, namely the board of directors or a senior officer, to be in a position to certify compliance with Part 504. Institutions need to either set up a governance structure or incorporate Part 504 compliance into an existing governance structure, as well as set forth the objectives and framework for compliance:

- What are your strategic goals?
- What various roles and responsibilities do resources have?
- How will progress and success be measured through reliable reporting?
- What is the definition and evidence of compliance for purposes of Part 504?

It is at this stage where communication of the plan, and the board and senior management commitment to compliance, i.e., tone at the top, is essential.

## Documentation

The entirety of the compliance efforts for Part 504 must be supported by comprehensive documentation. This includes:

- The objectives and plan established
- Governance structure
- Mission of any oversight committee(s)
- Risks and the assessment thereof
- Roles and responsibilities of individuals involved
- Data sources including extractions, transformations, and loading to downstream systems
- Models, rules, scenarios, and filtering routines
- Controls
- Policies and procedures
- Monitoring, testing, and/or validation exercises.

Your institution should identify what documentation is available in these areas and then evaluate the purpose and robustness of the documentation relative to the purpose.

## Risk identification assessment

One of the many areas of criticism from regulators, including NYSDFS, is the lack of connection between the actual BSA/AML and OFAC/sanctions risks faced by the institution and the transaction monitoring and sanctions filtering programs and systems. For example, issues arise when a firm deploys a generic risk assessment, not tailored to the risks associated with its client base, products or geographies, or when the firm pulls insufficient quantifiable data to substantiate the risks. Concerns were raised when an institution did not have a risk assessment or the risk assessment was insufficient. More to the point, however, is where the risk assessment identifies risks but the monitoring and filtering programs are not aligned to those risks.

So while the concept and process for BSA/AML and OFAC/sanctions risk assessments are not new, the quality of those risk assessments often needs to improve, and the linkage of those risk assessments to the monitoring and filtering program needs to be clear.

Today's risk assessment should incorporate both quantitative and qualitative factors. Historically, qualitative factors have played a significant if not the sole role. Now, with the ready availability of data, quantitative factors need to be included at least at a basic level—such as number of customers by type and risk levels; products and services offered and the number of customers using those; and geographic penetration of not only the customer base.

Moving forward, the bar is being raised as technology brings new innovation to data analytics as well as the ability to look at significantly more data in a shorter period of time.

## Data identification and assessment

No matter how well-documented, defined, or linked rules or scenarios are to the BSA/AML or OFAC/sanctions risks—any unavailable, poor-quality, improperly extracted, transformed, and loaded data will result in an ineffective transaction monitoring or sanctions filtering system. It's the old adage: "Garbage in, garbage out."

Data identification is the critical first step and must coincide with risk identification. The institution must answer the question: What data is necessary to measure the risks? Answering this question is just the beginning. There are many other questions that need to be asked as well, including:

- Is the data available? Where does it reside?
- Is the data complete? Is the data reliable?

There must be a clear understanding of the data lineage too. Where is and how is the data initially captured? How is it extracted, transformed, and loaded into various systems throughout the entire lifecycle? These questions must be asked and answered in order to have an effective risk assessment initially, aligned to effective transaction monitoring and filtering programs.

During the risk identification/assessment and data identification/assessment processes, the controls in place to ensure completeness and accuracy of the processes and data movement must be clearly identified. Whether the controls are systematic or manual, preventive or detective, these must be clearly documented, be the responsibility and accountability of specific persons, and be subject to monitoring, whether ongoing or periodic.

It is from this set of controls that effective independent testing can be formulated and conducted in support of the required annual certification.

## Financial Crimes Compliance Framework



In addressing the provisions of Part 504, many covered FIs may decide that they need to:

- Clarify sustainable roles and responsibilities across the three lines of defense, including the business lines and operational management (first line), the enterprise-wide or corporate risk management and compliance functions (second line), and internal audit (third line)
- Create strong linkage to existing compliance risk infrastructure and newly implemented testing, filtering and monitoring activities
- Establish clear senior roles and responsibilities between business and functions.



## Gap assessment

Once the assessment of the risks and data lineage is complete, a gap assessment is necessary to move forward. The question is, what is the target state to which the institution strives in order to identify gaps in its risk identification and assessment, and its data identification and assessment? The institution must establish a target state, one that satisfies its risk tolerance level and allows for the board of directors or senior officer to certify a compliance finding in accordance with the regulation.

The board or senior officer must set the standards under which the programs are “reasonably designed,” and those under which they will provide the certification—and these standards should be established with assistance from competent legal counsel. Generally, the programs should be designed and executed based upon the duty of care standard; namely, those responsible for designing and implementing the program “must act in the same manner as a reasonably prudent person in their position would”<sup>5</sup> and those executing must ensure that the program is “a reasonably informed, good faith, rational judgment without the presence of a conflict of interest.”<sup>6</sup> To the extent the programs or any component thereof do not meet this standard there is a gap that should be remediated prior to certification where possible.

## Remediation

The extent and speed of remediation is dependent upon the size and significance of the gap. Sufficient remediation must be completed in order to have programs that are “reasonably designed” to address the risk and a certification that is based on a reasonable and rational judgment. Part of the discussions around a remediation

plan need to include a determination of whether a lookback is necessary. While the certification is as of a specific date, it covers the prior calendar year.

If there were weaknesses identified in the transaction monitoring program or the filtering program over the course of the year, correction of those weaknesses at a point in time may not provide reasonable assurance that appropriate transactions were identified or filtered over the course of the year that is applicable to the certification. Action plans may be necessary where remediation cannot be completed prior to certification.

## Independent model validation and testing

There are two key but separate components necessary to effectively evaluate the transaction monitoring and filtering programs: independent model validation and independent control testing.

Independent transaction monitoring and sanctions filtering model validation have been and continue to be a regulatory expectation in the financial services industry. In many respects, this is one of the control functions that must be in place to assess the effectiveness of the systems and processes in place around the models.

KPMG’s approach to model validation follows accepted regulatory guidance and includes four pillars: conceptual soundness; data, system and process validation; ongoing and effective challenges; and outcomes analysis and reporting. These four pillars exist under an umbrella of model governance.

<sup>5</sup> Legal Information Institute, Cornell University Law School, [https://www.law.cornell.edu/wex/duty\\_of\\_care](https://www.law.cornell.edu/wex/duty_of_care)

<sup>6</sup> Ibid.

# Governance



## Conceptual soundness

### 1. Risk evaluation

- Review existing AML risk assessment
- Evaluate key risk factors (e.g., customer types, products and services, transaction volume, geography)
- Understand and assess specific recommendations brought by the internal and external auditors relevant to the Model validation program.

### 2. Rules

- Review current rules and thresholds (e.g. approach, frequency, documentation)
- Determine whether they are:
  - Commensurate with AML risk and designed to mitigate legal and regulatory risk
  - Aligned with industry trends
  - Adhered to OCC Model Governance Guidance

### 3. Developmental evidence

- Review documentation to support Model design and construction, including the following:
  - Inventory of transaction monitoring process (manual vs. automated)
  - Testing conducted by the institution, results, and supporting analysis
  - Inventory of Model limitations and assumptions



## Data, system, and process validation

### 1. Data validation

- Establish an inventory of data sources (customer and transactional based) and assess data quality
- Validate data sources and mapping documentation
- Validate data controls, reconciliation, and error reporting processes
- Sample test data feeds

### 2. System validation

- Review system functionality, settings, and any limitations
- Rules validation via:
  - Sample test transactions through each Rule/Threshold
  - Independently replicate model rules and compare results

### 3. Process validation

- Evaluate the existing Model workflow from the generation to the disposition of alerts
- Sample test alerts to evaluate the thresholds and parameter settings
- Evaluate the existing change control processes
- Evaluate consistency with the Model's original design



## Ongoing and effective challenges

### 1. Ongoing verification

- Review input monitoring process
- Review system set-up methodology for enhancements as changes occur in the business, regulatory environment, and overall AML risk
- Review the methodology to evaluate the sustainability of the process further to changes to data and/or system

### 2. Sensitivity and tuning

- Verify whether the model undergoes a periodic tuning process (e.g. rules, thresholds)
- Perform sensitivity testing above and below the line
- Recommend potential tuning opportunities

### 3. Benchmarking

- Using an alternative approach via KPMG's proprietary Case Management Tool (CMT) and Rules independently test the Model
- Review outputs
- Compare outputs against the existing Model



## Outcomes analysis and reporting

### 1. Outcomes analysis

- Conduct alert trend analysis (e.g. false positive ratios, case investigation yields, and SAR yields)
- Identify key red flags and the actual underlying SARs filing reasons and compare actual outcomes to Model estimates and forecasts
- Assess rules with highest and lowest Alert to SAR yields

### 2. Back-testing

- Run the Model logic over a historical dataset of transactions (e.g., six months back)
- Review outputs
- Back-test historically any proposed rule/threshold changes to assess the impacts to the Model in identifying potentially suspicious activity that led to SAR filings

### 3. Reporting

- Assess key performance indicators (KPIs) and key risk indicators (KRIs)
- Trending and analysis
- Evaluate reporting presented to the board and senior management

Independent<sup>7</sup> control testing needs to address two key components: testing of design and testing of operating effectiveness. Testing of design would be achieved by documenting end-to-end process flows and identifying key controls in place. As part of this documentation each control would be reviewed with an eye toward mitigating the risks identified to allow the institution to operate within its defined risk appetite. Testing of operating effectiveness would be achieved by selecting certain controls and performing sample testing to assess whether the control is performing as expected.

The independent model validation and the independent control testing work hand in hand. The independent control testing is foundational to the independent model validation. The independent control test, however, evaluates controls over the lifecycle of the data—from data capture through extraction, transformation, and loading. The model validation incorporates that into the data assessment as a key component of the overall validation effort.

The independent control testing however must also extend beyond the traditional capturing of a transaction or name for monitoring or filtering. It must include the capturing of due diligence data points which will likely be used in the alert resolution, case investigation, and potential reporting, blocking, or rejecting necessary under the transaction monitoring and filtering programs. It must also include an assessment of the controls around the actual resolution of alerts—namely, alert and case investigation protocols.

Thus, the independent testing plan must be laid out to include all of these areas, and the results pulled together into a comprehensive report for the board or senior officer.

### **Reaching the concluding step: Certification**

Certification comes at the conclusion of these various efforts. The board or senior officer needs to determine

whether they have executed a reasonably informed, good faith, rational judgment without the presence of a conflict of interest. A key component that must be considered when providing the certification is whether any identified issues have been fully remediated and re-tested, or are under way, on schedule, and assessed as to whether they will be effective if implemented as designed.

To reach this conclusion, the framework, for which the company is responsible, must be established early in the process and reflected by a clear “tone at the top.” Information and communication must continually flow to ensure there is always a clear plan and status to establishing and maintaining the framework. Failure to establish and maintain the framework will likely result in the inability to meet the duty of care standard necessary.

### **Next steps**

Although financial institutions need to complete compliance and certification by April 2018, the time to start is now, as the full year is subject to certification and will need to undergo the necessary evaluation and potential remediation.

We recommend that compliance professionals at institutions take stock of their current transaction monitoring and filtering program and where it stands relative to the NYDFS Part 504 compliance mandate.

From there, they should outline a roadmap to compliance as soon as possible to include a robust testing of design and operating effectiveness. Further, each institution must establish a robust certification framework, including sub-certifications by the business/system owners to allow the board or senior officer reliance that the mandate's requirements are being met, or deficiencies identified have been remediated or have well-defined remediation action plans.

<sup>7</sup> Independence in this context means the control testing must be performed by a person or group that is separate from those responsible for the design and implementation of the controls as well as those who perform the controls, for those that are manual, or those that maintain the automated controls.

# Conclusion

NYSDFS Part 504 levies substantial new mandates on covered FIs as described herein.

These new mandates will require a substantial investment of both time and budget to ensure compliance. Covered FIs must now ensure that their transaction monitoring and filtering programs comply with a comprehensive state regulation, in addition to complying with existing federal BSA/AML and OFAC mandates.

Moreover, FIs should expect NYDFS to enforce its new rule aggressively, as exhibited by its recent BSA/AML and OFAC enforcement actions. Part 504 explicitly requires the creation of a remediation plan for areas identified by the financial institution that merit material changes or updates.

Regulated FIs operating in New York will need to manage their oversight of monitoring and screening systems more closely, and will need to identify resources to effectively and efficiently evaluate the technology infrastructure they utilize in furtherance of these AML activities, while not over-engineering their validation processes. Therefore, it is important for AML officers to ask questions and develop a detailed understanding of their processes and controls as well as the accuracy and integrity of their data.

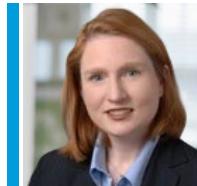
## How KPMG can help

1. Set up governance structure/framework for certification
2. Assist with control design testing
3. Assist with control operating effectiveness testing
4. Review of entity's protocols to achieve compliance with Part 504
5. Loan staff (to non-audit clients only)
6. Assist with standing up entire program to address Part 504 requirements

# Contact us



**Teresa Pesce**  
**Global AML and Financial Crimes and Enforcement Leader**  
**T:** 212-872-6272  
**E:** [tpesce@kpmg.com](mailto:tpesce@kpmg.com)



**Marikay Corcoran**  
**Principal, Financial Crimes and Enforcement**  
**T:** 781-901-1103  
**E:** [mahines@kpmg.com](mailto:mahines@kpmg.com)



**Thomas Keegan**  
**Principal, Forensic Technology**  
**T:** 212-954-7880  
**E:** [tkeegan@kpmg.com](mailto:tkeegan@kpmg.com)



**Stephen Marshall**  
**Principal, Financial Crimes and Enforcement**  
**T:** 212-954-3025  
**E:** [sdmarshall@kpmg.com](mailto:sdmmarshall@kpmg.com)

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

[kpmg.com/socialmedia](http://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.

© 2017 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 687635