DFSNY Rule 504 – Gathering the Evidence

The evidence required to support certification under DFSNY Rule 504 is extensive. This paper highlights some of the considerations involved in collecting and documenting the evidence to confirm the institution's programs comply with the requirements of the rule. Given that the latest date for submission of the first certification is **April** 15, 2018**, this note** is a timely reminder to Boards of Directors and Compliance Officers of affected institutions to address the issue without delay if they have not already done so.

Certification consists of a compliance finding by either the entire Board or by one or more senior officers that:

- the signatories have reviewed the evidence relevant to the finding.
- the signatories have taken all steps necessary to confirm that the Institution's transaction monitoring and filtering programs comply with the provisions of Section 504.3; and
- to the best of the knowledge of the signatories, the transaction monitoring and filtering program of the Institution, as of the date of the finding for the relevant year, complies with rule 504.3.

This paper focuses on assessing the design of the program, not the detailed testing required to substantiate that the program is operating as intended. Nonetheless, it is essential that the program is tested and reported on as part of the evidence gathering process. Records, schedules and data supporting the certification must be retained for five years. To the extent that any areas, systems or processes require material improvement, updating or redesign, records detailing their identification and any remedial efforts planned and underway to address them must be available for inspection.

Evidence Gathering Process

The evidence gathering process is time-consuming and extensive and requires significant inputs from staff and external vendors.

Transaction Monitoring Risk Assessments 504.3 (a) 1 -3

The institution's AML risk assessments must be reviewed to ensure they have been carried out to the exacting specifications set out in the Regulation. Pre-existing risk assessments should be updated to address changes to AML laws, OFAC regulations and regulatory warnings, recent consent orders and other relevant institutional information, such as acquisitions, new product lines etc. The assessed risks must be specific to the institution's businesses, products, services, and customers/counterparties and must include the identification of potentially suspicious or illegal activities. The resultant schedule of inherent risk must provide the basis for mitigating controls to ensure residual risk is consistent with the institution's risk appetite.

This whitepaper does not provide legal advice. For legal advice, please contact an attorney directly.

Transaction Monitoring Detection Scenarios 504.3 (a) 4

Supporting evidence must be obtained to confirm that:

- detection scenarios mitigate specific risks identified in the risk assessment, including:
  - transaction patterns or activities that require mandatory reporting (e.g., individual, aggregated and structured transactions more than defined limits, unusually high or complex transactions carried out by PEPs etc.)
  - transactions or transaction patterns that are out of alignment with expected volumes or amounts for that customer or the business's overall transaction patterns, volumes and amounts
- new or amended scenarios have undergone testing to ensure their suitability
- existing scenarios have been reviewed to ensure their continued suitability
- the frequency of scenario execution is proportionate to the risks monitored, and
- scenario parameters, thresholds and values applied are reviewed and tested to confirm they remain appropriate.

Transaction Monitoring Program Testing 504.3 (a) 5

End-to-end pre- and post-implementation testing are designed to ensure that the monitoring program is well designed and resourced and that its outputs continue to meet program objectives. Pre-implementation activities are those that are designed to make sure the program operates as intended. Post-implementation testing focuses on ensuring business and regulatory requirements have been met, that controls have been implemented as planned, that any changes to the program have gone through the necessary change management processes and that the outputs of the program continue to meet business expectations and regulatory requirements.

In both instances, tests need to be performed to confirm the required activities are complete and that the supporting programs around coding, data, scenarios, and model validation are operating properly. Reports detailing the results of these tests and any related remediation plan form part of the evidence and supporting documentation required to facilitate certification.

Transaction Monitoring Model Documentation 504.3 (a) 6

Documentation that articulates the intent and scope of the transaction monitoring model as well as describing the governance processes around its maintenance should be reviewed for completeness. The documentation should identify all source systems, including manual monitoring and any related controls, provide a validated map of all data flows, describe and confirm the results of a review of any ETL processes, identify the rationale behind any parameters and thresholds and should include a schedule of detection scenarios mapped back to the risk assessment. This evidence should be available for review by the signatories if so required.

This whitepaper does not provide legal advice. For legal advice, please contact an attorney directly.

Transaction Monitoring Alert Investigation and Disposition 504.3 (a) 7

The alert investigation and disposition process must be reviewed for completeness.

- Firstly, it must be capable of capturing multiple sources of alerts, whether they are in the form of automated alerts, employee observations, manual monitoring, national security letters etc., and a clear reporting pathway must be defined for all sources.
- Secondly, there needs to be a defined set of protocols surrounding the investigation process consisting of detailed guidance on procedures for prioritization, investigation, documentation, decision making and reporting.
- Thirdly, the process should be reviewed to ensure that it is adequately funded, that employees involved receive appropriate training and that investigation backlogs are minimized.

Transaction Monitoring Model Validation 504.3 (a) 8

The requirement to validate the model as part of the evidence gathering process arises from the obligation to ensure the transaction monitoring system is assessed for the continued relevance of the detection scenarios, the underlying rules, threshold values, parameters, and assumptions.

To a large extent, some of the required evidence will be gathered by the tasks above. The requirement under this part is primarily concerned with the overall governance processes and is more like a model validation exercise as defined in SR11-7. The existence of strong governance ensures that regulatory obligations are complied with, that roles, responsibilities, and accountabilities are clearly defined, that relevant risks are identified, that all source systems are subject to testing, that monitoring criteria are kept under review, that there is a clearly defined change management process in place and that the outputs of the program meet the design objectives.

OFAC Risk Assessment 504.3 (b) 1

The approach to evidence gathering for assessing the adequacy of the institution's OFAC risk assessment is similar to that required for transaction monitoring. The evidence collected needs to be sufficient to confirm that all relevant products, customers, geographies, etc. have been identified, and that potential risk scenarios have been identified and mitigated. As with the transaction monitoring risk assessment, the OFAC risk assessment should have been reviewed and updated in line with changes to the underlying regulations as well as taking account of both quantitative and qualitative factors within the business.

Filtering Program Name and Account Matching 504.3 (b) 2

The requirements of the rule only apply to OFAC obligations. However, it is appropriate that the same standards apply to any filtering lists used within the institution.

Supporting evidence is required to confirm that lists are kept up to date, that customers and ultimate beneficial owners are screened against current lists at on-boarding and up-dated lists as soon as practicable after updating and that appropriate procedures are in place to screen parties to transactions before execution of those transactions. While manual screening is acceptable where there the number of transactions is low, interdiction software should be deployed for large volumes of transactions. Where automated screening is applied, evidence needs to be obtained to confirm that the name matching technology complies with the requirements of the rule.

Filtering Program Testing 504.3 (b) 3

As with the Transaction Monitoring program, the Filtering program needs to be subject to end-to-end pre- and post-implementation testing to ensure good design and resourcing of the filtering program as well as ensuring that its outputs continue to meet program objectives.

Reports detailing the results of these tests and any related remediation plan form part of the evidence and supporting documentation required to facilitate certification.

Filtering Program Model Validation 504.3 (b) 4

The requirement to validate the model as part of the evidence gathering process arises from the obligation to ensure OFAC filters are performing as designed and that the thresholds and limits are applied as intended.

To a large extent, some of the required evidence is gathered in the tasks above, as is also the case with the transaction monitoring program. The requirement under this part is primarily concerned with the overall governance processes and is more like a model validation exercise as defined in SR11-7. What is required is to confirm that strong governance processes are in place for the program to ensure that all regulatory obligations are complied with, that roles, responsibilities, and accountabilities are defined, that relevant risks are identified, that all source systems are subject to testing. Test evidence should be available to confirm that the matching filter, any risk-based filters, and fuzzy matching filters are all performing as designed.

Filtering Program Model Documentation 504.3 (b) 5

Documentation that articulates the intent and scope of the filtering program as well as describing the governance processes around its maintenance should be reviewed for completeness and be reported on. Source systems, data flows, and ETL processes should be documented and tested to ensure data flows properly through the filtering system, and the results of such testing should be available for review by the signatories if so required.

Transaction Monitoring and Filtering Program

The following additional evidence is required with respect to each of the programs:

• Identification of all Data Sources 504.3 (c) 1

Confirm that all data sources have been identified and mapped to both the monitoring and filtering programs, as appropriate.

• Validation of Data 504.3 (c) 2

Confirm by reference to independent testing that data has been tested for integrity, accuracy and quality

• ETL Processes for Automated Systems 504.3 (c) 3

Confirm by reference to independent testing that data sourced from the system is complete, that transformations are performed correctly and that the transformed data is fully absorbed into the relevant program.

• Governance and Oversight 504.3 (c) 4

Confirm by reference to organizational charts, HR policies and procedures, compliance and internal audit reports, board meetings and other such documentation as is available that effective governance processes are in place for both programs and that the Board exercises an appropriate degree of oversight of the programs.

• Vendor Selection 504.3 (c) 5

The appointment of new vendors for the acquisition, installation or testing of either the monitoring or filtering program should include requirements documentation, requests for proposals and a vendor scoring and selection process, including ensuring the vendor has the necessary experience to carry out the specified tasks.

• Appropriate Funding 504.3 (c) 6

Evidence of appropriate funding is subjective and involves consideration of the tools, technologies, and staffing available to both programs. Nonetheless, a degree of objectivity can be brought to bear on gathering the requisite evidence. In particular, the following tasks are likely to be indicative of the adequacy of funding:

- Number of alerts processed by investigators
- Number of training programs run during the year
- Number of staff with professional certifications
- Size and frequency of alert backlogs
- Budgetary approval rate for compliance funding applications.

• Qualified Personnel 504.3 (c) 7

Execution of the programs requires competent personnel. Consequently, it is essential to obtain evidence to confirm that employees have the requisite skills, knowledge and experience required to carry out the tasks they are required to perform. Evidence obtained should, at a minimum, include:

- consideration of the skills, knowledge, certifications and experience of MLRO
- a review of the training records of key staff
- assessment of alert re-work rates
- identification of alert escalation rates for individual employees.

• Periodic Training 504.3 (c) 8

The institution's training records should be reviewed to confirm that all employees receive general AML/Sanctions training at least annually, that employees receive targeted training directly related to their roles, that employees are tested at the end of each training session and that the results are recorded and retained on file as part of their HR records.

This whitepaper does not provide legal advice. For legal advice, please contact an attorney directly.

Identification of Remedial Effort

A remediation plan is required where the institution has identified areas, systems or processes requiring material improvement, updating or design. While the term "material" is not defined, it is intended to cover any aspect of the program that could have a significantly negative impact on program outcomes, i.e., that significant and recurring acts of money laundering could potentially go undetected or that recurring breaches of OFAC regulations could go undetected.

The proposed remediation plan should be submitted to the Board along with other documents, reports, and certifications so that the Board can satisfy itself that it addresses the deficiencies identified in the supporting documentation.

The remediation plan should, at minimum:

- identify the deficiency
- describe its potential impact
- assess its urgency
- define the plan
- identify budgetary implications
- estimate completion date.

The remediation plan should be kept under review and should be the subject of an updated report at each meeting of the Board or any sub-committee appointed to oversee its implementation.

Conclusion

The requirements of this rule have significantly raised the bar by implementing highly prescriptive requirements that exceed current guidance from the FFIEC and OFAC as well as obligations specified in the BSA.

The Rule implements three significant challenges that need to be addressed as a matter of urgency by affected institutions. Firstly, programs need to be reviewed to ensure they meet the highly prescriptive requirements of the rule. Secondly, evidence needs to be collected to confirm the programs are operating as intended. Finally, a detailed remediation plan needs to be put in place to address any material deficiencies identified in the current programs.

About The Mizen Group

The Mizen Group is a dedicated/boutique/niche RegTech consultancy and advisory firm specializing in end-to-end regulatory and technology solutions and services for the Financial Services Sector. Our portfolio of tools includes diagnostics that address compliance programs, compliance culture, data governance. data quality, scenario testing and transaction look-backs. We also provide tools and technologies required to satisfactorily implement AML/Sanctions programs, including risk assessments, data mapping services, KYC tools for UBOs and transaction monitoring and watch list filtering capabilities.

We have considerable experience in assisting institutions with the design and implementation of processes that comply with rule 504, as well as addressing the evidence-gathering and testing challenges of the rule Whether you are a small or large, domestic or international institution facing challenges with implementation of the rule, or indeed any AML/Sanctions related issue, feel free to contact us and we will be happy to have a preliminary discussion to identify if we can assist or point you in the right direction.

For further information, please contact: learningcenter@mizengrp.com.

This whitepaper does not provide legal advice. For legal advice, please contact an attorney directly.