ACAMS® Advancing Financial Crime Professionals Worldwide

Understanding the New DFS Part 504 Regulations and the Associated AML Program Testing Challenges

Chris Recor, CAMS

Executive Summary

Section 302 of the Sarbanes-Oxley Act ("SOX")[i] requires the principal executive and financial officers of a public company to certify in their company's annual and quarterly reports that such reports are accurate and complete and that they have established and maintained adequate internal controls for public disclosure. "The purpose is to ensure that a company's CEO and CFO take a proactive role in their company's public disclosure and to give shareholders confidence in the accuracy, quality and reliability of a company's SEC periodic reports."[ii]

The New York State Department of Financial Services ("NYDFS") now final part 504 Rule (the "Final Rule" or "Rule") is closely modeled on the SOX requirements (the "Rule") and is effective January 1, 2017. Essentially, the Final Rule requires a signature by each member of the Board of Directors or Senior Officer(s) supported by a remediation program for any deficient internal control areas and annually submitted to the Superintendent[iii] beginning April 15, 2018.

The Final Rule ***extends*** the signature attestations to cover BSA/AML and OFAC federal laws and regulations through the creation of ***binding control standards*** related to Transaction Monitoring and U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") related Filtering Programs that will be administered and enforced by New York State regulatory authorities. Under the Rule, New York state bank and non-bank Regulated [iv] are required to ***certify*** that their AML transaction monitoring and OFAC filtering program standards meet the ever more stringent compliance control expectations. The recently passed NYDFS Part 504 rule is prescriptive and granulized in that it goes further than previous regulations by spelling out the required program ***attributes*** in areas of transaction monitoring, OFAC sanctions filtering, governance, data, model validation, vendor selection, funding, use of qualified personnel and training.

The impact on regulated non-bank financial institutions ("NBFIs"), (e.g. money transmitters, check cashers and money services businesses) is more pronounced as these NBFIs may not have adequate resources in place to implement the Final Rule requirements by the effective date.[v] This paper assesses these requirements and provides insight into some of the operational implications in order to meet each Rule requirement along with control factors and testing considerations applicable to the third line of defense (e.g., Internal Audit) in determining an institution's compliance with the standards per the Final Rule.

Background

In a December 1, 2015 press release, Governor Mario Cuomo proposed anti-terrorism regulation requiring senior executives to certify effectiveness of their anti-money laundering control systems. The release noted that during the previous four years, the NYDFS had conducted numerous investigations into terrorist financing, sanctions violations, and anti-money laundering compliance at covered financial institutions. As a result, a number of deficiencies identified within transaction monitoring and filtering programs were identified including deficiencies in governance, oversight, and accountability at the senior levels of many institutions leading to the standards noted within the NYDFS Advance Notice of Proposed Rule Making ("ANPRM").

Conversely, many of the prescribed requirements noted were debated by Regulated Institutions and supported by the American Bankers Association's rebuttal letter of March 31, 2016 that strongly opposed implementation of the proposed Rule in its then current format. Although some public comments were considered, analysis reveals very little difference between the ANPRM and Final Rule which was formally adopted into law on June 30, 2016 and will be effective January 1, 2017.[vi]

The Part 504 Final Rule requires covered institutions to establish transaction monitoring and filtering programs designed to address shortcomings in their AML programs. Additionally, on an annual basis beginning April 15, 2018, either the Board of Directors as a governing body or a senior officer personally must certify[vii] that the AML program is compliant and that the governing body or individual certifying has undertaken the necessary steps to make such certification.

The Rule outlines the necessary steps that must be undertaken to address the *prescriptive* Transaction Monitoring and Filtering Program requirements including documentation of remedial efforts and an annual board resolution or senior officer compliance finding. The specific requirements put into law under Part 504 are listed below.

§504.3 Transaction Monitoring and Filtering Program Requirements[viii]

Transaction Monitoring Program

§504.3(a) Each Regulated Institution shall maintain a transaction monitoring program reasonably designed for the purpose of monitoring transactions after their execution for potential BSA/AML violations and Suspicious Activity Reporting, which system may be manual or automated, and which shall include the following attributes, to the extent they are applicable:

1. Be based on the risk assessment of the institution;
2. Be reviewed and periodically updated at risk-based intervals to take into account and reflect changes to applicable BSA/AML laws, regulations and regulatory warnings, as well as any other information determined by the institution to be relevant from the institution's related programs and initiatives
3. Appropriately match BSA/AML risks to the institution's businesses, products, services, and customers/counterparties;
4. BSA/AML detection scenarios with threshold values and amounts designed to detect potential money laundering or other suspicious or illegal activities;
5. End-to-end, pre-and post-implementation testing of the transaction monitoring program, including, as relevant, a review of governance, data mapping, transaction coding, detection scenario logic, model validation, data input and Program output;
6. Documentation that articulates the institution's current detection scenarios and the underlying assumptions, parameters, and thresholds;
7. Protocols setting forth how alerts generated by the transaction monitoring program will be investigated, the process for deciding which alerts will result in a filing or other

action, the operating areas and individuals responsible for making such a decision, and how the investigative and decision-making process will be documented; and

8. Be subject to an on-going analysis to assess the continued relevancy of the detection scenarios, the underlying rules, threshold values, parameters, and assumptions.

Filtering Program

§504.3(b) Each regulated institution shall maintain a filtering program, which may be manual or automated, reasonably designed for the purpose of interdicting transactions that are prohibited by OFAC, and which shall include the following attributes, to the extent applicable:

1. Be based on the risk assessment of the institution;
2. Be based on technology, processes or tools for matching names and accounts, in each case based on the institution's particular risks, transaction and product profiles;
3. End-to-end, pre- and post-implementation testing of the filtering program, including, as relevant, a review of data matching, an evaluation of whether the OFAC sanctions list and threshold settings map to the risks of the institution, the logic of matching technology or tools, model validation, and data input and Program output;
4. Be subject to on-going analysis to assess the logic and performance of the technology or tools for matching names and accounts, as well as the OFAC sanctions list and the threshold settings to see if they continue to map to the risks of the institution; and
5. Documentation that articulates the intent and design of the filtering program tools, processes or technology.

Both the Transaction Monitoring and Filtering Programs

§504.3(c) each transaction monitoring and filtering program shall require the following, to the extent applicable:

1. Identification of all data sources that contain relevant data;
2. Validation of the integrity, accuracy and quality of data to ensure that accurate and complete data flows through the transaction monitoring and filtering program;
3. Data extraction and loading processes to ensure a complete and accurate transfer of data from its source to automated monitoring and filtering systems, if automated systems are used;
4. Governance and management oversight, including policies and procedures governing changes to the transaction monitoring and filtering program to ensure that changes are defined, managed, controlled, reported, and audited;
5. Vendor selection process if a third-party vendor is used to acquire, install, implement, or test the transaction monitoring and filtering program or any aspect of it;
6. Funding to design, implement and maintain a transaction monitoring and filtering program that complies with the requirements of this part;

7. Qualified personnel or outside consultant responsible for the design, planning, implementation, operation, testing, validation, and on-going analysis, of the transaction monitoring and filtering program, including automated systems if applicable, as well as case management, review and decision making with respect to generated alerts and potential filings; and
8. Periodic training of all stakeholders with respect to the transaction monitoring and filtering program.

Documentation of Remedial Efforts

> §504.3(d) To the extent a regulated institution has identified areas, systems, or processes that require material improvement, updating or redesign, the regulated institution shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the Superintendent.

§504.4 Annual Board Resolution or Senior Officer(s) Compliance Finding

> §504.4 To ensure compliance with the requirements of this Part, each Regulated Institution shall adopt and submit to the Superintendent a Board Resolution or Senior Officer(s) Compliance Finding in the form set forth in Attachment A by April 15th of each year. Each regulated institution shall maintain for examination by the Department all records, schedules and data supporting adoption of the Board Resolution or Senior Officer(s) Compliance Finding for a period of five years.[ix]

This paper assesses each of the requirements under the Rule including examples of program risks, mitigating controls and testing measures that may be used to audit compliance with the Rule. Testing is the cornerstone of auditing the effectiveness of controls of the BSA/AML program. Controls are the system of internal controls (including policies, procedures, and systems) used to mitigate BSA/AML risks. To ensure that the BSA/AML controls are effective the following types of tests should be performed:[x]

1. *reperformance* using a "new transaction to see which controls are used by the client and the effectiveness of those controls;"
2. *observation* of "a business process in action, and in particular the control elements of the process;" and
3. *inspection* of "business documents for approval signatures," initials, signoffs or stamps confirming that a particular control has been performed.

TRANSACTION MONITORING PROGRAM (§504.3(a))

BSA/AML RISK ASSESSMENTS (§504.3(a) (1-3))

The Federal Financial Institutions Examination Council ("FFIEC") BSA/AML Examination Manual does *not* state that an institution is *required* to have a BSA/AML risk assessment. In fact, it states that "for the purposes of the examination, whenever the bank has not completed a risk assessment, or the risk assessment is inadequate, the examiner must complete a risk assessment based on available information."[xi] This ambiguity is clarified under the new Rule which requires linkage between the BSA/AML risk assessment and the Transaction Monitoring program.[xii] For example, the statement that the Transaction Monitoring program needs to "be based on a Risk Assessment" prescribes there actually be a BSA/AML risk assessment from which to use in identifying what detection scenarios best mitigate the inherent BSA/AML risks.[xiii]

There are numerous articles on BSA/AML risk assessments, and while the steps involved in developing one are beyond the scope of this paper, the core components of a BSA/AML risk assessment should include the identification of specific inherent risk categories (i.e. products, services, customers / counterparties, transactions and geographic locations) specific to the institution followed by a detailed assessment based upon both qualitative and quantitative information. Overall, the assessment then considers the inherent BSA/AML risks and the mitigating impact of controls (including policies, procedures and systems) toward residual risk assessments.

The institution's products and services may, by nature of their degree of anonymity or volume of currency, pose increased risk of money laundering or terrorist financing. Certain types of customers / counterparties may also subject the institution to increased risk based on the type of customer / counterparty (e.g. nonbank financial institutions, senior foreign political figures, nonresident aliens, etc.) or the geographic locations where the institution transacts business with the customer / counterparty (e.g. OFAC sanctioned countries, jurisdictions considered to be of primary money laundering concern, offshore financial centers, etc.).

Development of the qualitative and quantitative information for the risk assessment includes the collection and analysis of metrics around the customer / counterparty base, transactions processed and in which geographies customers / counterparties and transactions are processed. Existing controls are then identified and assessed against the inherent risks to determine the residual risks upon application of the effectiveness of controls and provides an overall risk profile of the institution.

The risk assessment must be periodically updated to reflect changes to BSA/AML laws, regulations and regulatory warnings and other relevant institutional information. The Rule does not specify what is meant by periodic updates but a review of recent BSA/AML Consent Orders indicates that documents, such as a risk assessment, in meeting this requirement should be reviewed and updated annually or when material changes have occurred in the institution's products and services, customers / counterparties and geographies (e.g. opening of a new branch in a high-risk geography, divestiture of a line of business, changes to the AML risk appetite, etc.) or when BSA/AML laws, regulations or regulatory warnings have been issued.

The risk assessment should be written to be easily understood by all appropriate parties in the institution and communicated to all business lines, the Board of Directors, management and appropriate staff.

There should be no mistake that the NYDFS now REQUIRES a comprehensive BSA/AML risk assessment that lays the foundation for the required AML program controls the institution must design and implement to mitigate its identified risks. In mitigating these risks, the institution, under the Rule, must select and implement the appropriate detection scenarios to identify potentially unusual and suspicious customer activity behavior to mitigate the identified inherent risks.

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine if the ***Transaction Monitoring BSA/AML risk assessment*** addresses the Transaction Monitoring regulatory requirements is illustrated in the table below:

BSA/AML Risk Assessment (§504.3(a) (1-3))				
Risk	Control Name	Control Objectives	Evidence of Control	Tests of Control
All products and services have not been identified in the risk assessment	Products / services	To ensure that all the relevant products and services have been identified	Cross-referenced list of the institution's products/services Job aid document Confirmation email from each line of business	Review the BSA/AML risk assessment and confirm that all of the institution's applicable products and services have been included and addressed in the risk assessment
All customer types have not been identified in the risk assessment	Customer types	To ensure that all the relevant customer types have been identified	Cross-referenced list of the institution's customer types Job aid document Confirmation email from each line of business	Review the BSA/AML risk assessment and confirm that all of the institution's different customer types have been included and addressed in the risk assessment
All relevant geographies served by the institution have not been identified in the risk assessment	Geographies	To ensure that all the geographies served by the institution have been identified	Cross-referenced list of the institution's geographies served Job aid document	Review the BSA/AML risk assessment and confirm that all of the geographies served by the institution have been included and addressed in the risk assessment
Risk assessment does not indicate what scenarios (models) should be implemented to	Scenarios	To ensure that each of the applicable inherent risks have been addressed by one or more	Coverage model assessment	Review the BSA/AML risk assessment and confirm there is a cross-reference of inherent risks to transaction monitoring scenarios

BSA/AML Risk Assessment (§504.3(a) (1-3))				
Risk	Control Name	Control Objectives	Evidence of Control	Tests of Control
mitigate the inherent risks		transaction monitoring scenarios		
Inherent risks have not been fully identified	Inherent risks	To ensure that all the relevant inherent risks have been identified	Inherent risk analysis	Review the BSA/AML risk assessment and confirm that the quantity of risk matrix identifies the inherent risks to the organization
Other qualitative risk factors have not been considered	Other qualitative risk factors	To ensure that other qualitative risk factors that may impact inherent risks have been considered in the risk assessment	Assessment of other qualitative risk factors and determination as to use in the risk assessment	Review the other qualitative risk factors assessment document and confirm that these have been considered in the overall inherent risks. Other qualitative risk factors include: • Client base stability • Integration of IT systems • Expected account/client growth • Expected revenue growth • Recent AML Compliance employee turnover • Reliance on third party providers • Recent/planned introductions of new products and/or services • Recent/planned acquisitions • Recent projects and initiatives related to AML Compliance matters (e.g. remediation, elimination of backlogs, off-shoring) • Recent relevant enforcement actions • National Risk Assessments

TRANSACTION MONITORING DETECTION SCENARIOS (§504.3(a)(4))

Transaction Monitoring detection scenarios (often also referred to as 'rules,' 'algorithms,' or 'models') include threshold values, amounts (dollar and volume values) or other specific criteria aligned with the institution's AML risk appetite and risk profile, as developed in the risk assessment, for certain types of customers / counterparties, transactional activity and geographies served. Models are then designed to compare these criteria against transactional information, such as comparing the total cash deposits made to an account in a single banking business day to specified limits. Models are also designed to compare the customer's profile against transactional information to determine if they are out of profile, such as if the customer's profile did not include high volumes of wire activity yet a transaction review shows several hundred funds transfers processed month over month. When the established thresholds are exceeded by the dollar values, volume or other criteria values expressed in the model an alert is created indicating that the customer's behavior warrants further review to determine if the activity is in fact suspicious thereby requiring the filing of a regulatory report (e.g. SAR, CTR, etc.)

The Rule also specifies that the models must be designed to detect "other suspicious or illegal activities"[xiv] which by definition include predicate offenses.[xv] These are referred to as specified unlawful activities ("SUA") and includes those either "committed or attempted (1) with the intent to promote further predicate offenses; (2) with the intent to evade taxation; (3) knowing the transaction is designed to conceal laundering of the proceeds; or (4) knowing the transaction is designed to avoid anti-laundering reporting requirements." [xvi]

An example of a simplified BSA/AML and OFAC audit program including the risks, controls and tests that can be performed by internal audit to determine if the ***Transaction Monitoring detection scenarios*** meet the regulatory requirements is illustrated in the table below:

Transaction Monitoring Detection Scenarios (§504.3(a) (4)				
Risk	Control Name	Control Objectives	Evidence of Control	Tests of Control
Models do not cover all risks in risk assessment	Risk coverage	To ensure that the models mitigate the inherent risks identified in the risk assessment	Coverage model assessment	Obtain and review the most recent coverage model assessment and confirm that the inherent risks identified in the risk assessment have been addressed by one or more models
Model thresholds are too high or too low	Settings	To ensure that the model's thresholds are set at appropriate levels	Tuning report	Obtain and review the most recent model tuning report and confirm that the testing results indicated the appropriateness of the current settings
Models not run on correct schedule	Schedule	To ensure that the models are being run on the correct schedule	Model run schedule	Obtain and review the current model run schedule and confirm that models run on daily, weekly, monthly or other schedules are correct

END-TO-END PRE AND POST IMPLEMENTATION TESTING (§504.3(a) (5))

This subsection of the Rule prescribes a comprehensive set of so called 'end-to-end' control tests of the Transaction Monitoring system covering the areas of governance, data mapping, transaction coding, detection scenario logic, model validation, data input and program output.

Pre-implementation activities are those required management actions that must occur prior to a new or materially changed Transaction Monitoring system going live. The purpose of these activities is to ensure, to the extent possible, that once the system goes live it will produce the required results, operate as intended protecting the institution from the threats of money laundering and terrorist financing, and will provide the means for the institution to adhere to all the relevant laws, regulations and best practices.

Post-implementation activities are those required management actions that must occur after a new or materially changed Transaction Monitoring system has gone live. The purpose of these activities is to ensure, to the extent possible, that the system has met the design objectives, that it is appropriately managed and staffed with qualified personnel, and that it is protecting the institution from the threats of money laundering and terrorist financing.

The pre and post implementation testing steps should be performed to ensure that the required activities were successfully completed and that the supporting programs around data, coding, scenarios, model validation and data input/output are operating effectively and regularly maintained.

As previously noted, testing is the cornerstone of auditing the effectiveness of the system of controls used to mitigate BSA/AML risks of the Transaction Monitoring program. To ensure that the BSA/AML controls are effective the following types of tests should be performed: (1) reperformance using a "new transaction to see which controls are used and the effectiveness of those controls;" (2) observation of "a business process in action and the control elements of the process;" and (3) inspection of "business documents for approval signatures," initials, signoffs or stamps confirming that a particular control has been performed.[xvii]

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine if the ***Transaction Monitoring end-to-end pre and post implementation testing*** meets the regulatory requirements is illustrated in the table below:

Transaction Monitoring End-to-End Pre and Post Implementation Testing (§504.3(a)(5))				
Risk	Control Name	Control Objectives	Evidence of Control	Tests of Control
Pre-implementation project risks not mitigated	Implementation project risks	To ensure that project scope and related implementation risks are mitigated	Periodic reviews of: • project risks • "to be" design • data conversion • integration testing • readiness / go live	Obtain and review: • Adequate budgets and funding have been approved • Steering committee charter • PMO and milestone plans • QA/QC plans and results • Requirements documentation • Implementation staffing • Design model • System interfaces • Integration test plan and results • Training plan and attendance schedule • User acceptance testing plan • Level of vendor involvement • User and business sign-offs • Go live plan • Post implementation plan
Failure to perform post-implementation activities	Post-implementation activities	To ensure that the post-implementation plan is properly executed	Post-implementation results documentation	Obtain, review and confirm: • Business, regulatory, IT and security requirements were met • Controls were implemented as planned • Key controls were tested • Customers, accounts and transactions were successfully processed through integration tests

Transaction Monitoring End-to-End Pre and Post Implementation Testing (§504.3(a)(5))				
Risk	Control Name	Control Objectives	Evidence of Control	Tests of Control
				• Approved changes were tested • Users and business have accepted the system • System results map back to requirements • System has appropriate levels of internal and external (vendor) support • Service level agreements are in place • Appropriate BCP tiering (e.g. level 1, 2 or 3) has been assigned to the applications

MODEL DOCUMENTATION (§504.3(a) (6))

This subsection of the Rule prescribes that models are supported by written documentation including "the underlying assumptions, parameters and thresholds" of each model.[xviii] Documentation should be formal (e.g. written, dated with approval signatures) and supplemented using the institution's change management process whenever changes to the model(s) has been determined to be required.

Transaction Monitoring solutions from 3rd parties include, at a minimum, an inventory of detection scenarios available for the institution to utilize, detection scenario logic documentation explaining the business and or regulatory purpose of the model, run schedule (e.g. daily, weekly, monthly, on-demand), reference period, and default thresholds and parameters. The documentation around the underlying assumptions and operational parameters and thresholds that are implemented in each model remain the institution's responsibility as these vary from one institution to the next. Additionally, the underlying assumptions, parameters and thresholds established in each model need to be directly linked back to the BSA/AML risk assessment and include supporting rationale as to what assumptions are being made and why the particular parameters and thresholds have been set to their current values.

Certain model changes will need to be made over time, such as the addition, deletion, deactivation, or change to the model's run schedule, reference period, parameters or thresholds. These changes may be required due to changes in the BSA/AML risk assessment, regulatory changes, industry standards or simply due to the fact that the model is producing alerts of minimal suspicious activity value. When changes are required it is critical to adhere to strict change management processes to document all of the changes made and appropriate approvals provided. In addition to the necessary governance functions around this process there are several key activities that should be performed. The Information Technology Service Management[xix] ("ITSM") organization defines the core activities of a change management process[xx] as:

- "Receiving change requests from appropriate parties

- Determining whether or not the change is appropriate
- Assigning the change to resources for solution identification, sizing and risk analysis
- Accepting or rejecting the requested change
- Assigning the change to solution development resources
- Reviewing the solution prior to implementation
- Scheduling the change
- Communicating change status as required to all interested parties
- Closing the change request order."

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine if the ***Transaction Monitoring model documentation*** meets the regulatory requirements is illustrated in the table below:

Transaction Monitoring Model Documentation (§504.3(a) (6))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
Source systems not documented	Source systems documentation	To ensure that all the systems of record applicable to the BSA/AML and OFAC program have been documented	Source systems diagram	Review the source systems diagram to understand and confirm the feeds to the BSA/AML and OFAC platforms have been documented
Data from source systems not documented	Source systems data documentation	To ensure that all the required data from all the applicable source systems has been documented	Data flow diagram	Review the data flow diagrams documentation to understand and confirm that the data feeds from each of the source systems has been documented
ETL not documented	ETL documentation	To ensure that the ETL process has been documented	ETL documentation	Review the ETL documentation to ensure it clearly describes the extraction, transformation and loading processes including any assumptions made.
Filter models not documented	Model documentation	To ensure that the Filtering Program model(s) have been documented	Filter model documentation	Review the filter model documentation to ensure it clearly describes the input, calculation and logic, and output steps involved in each model
Change control procedure not documented	Change management	To ensure that changes to the filter program models follow a prescriptive process	Change control	Review the filter program change control procedure to ensure it covers all the necessary activities from initiating a change request through final implementation

ALERT INVESTIGATION AND DISPOSITION PROTOCOLS (§504.3(a) (7))

This subsection of the Rule prescribes that the institution has "protocols"[xxi] for the investigation and disposition of Transaction Monitoring alerts. The focus of alert management is on the actual processes in place required to investigate and evaluate unusual activity. Sources for the identification of potentially unusual activity include:

- Employee Identification / Escalation – unusual client activity and/or behavior observed. The institution must have a written and communicated method of reporting unusual activity to Compliance (e.g. email, hotline, documentation) and supported by periodic training
- Law Enforcement Requests – including grand jury subpoenas, National Security Letters and 314(a) requests. The institution should have procedures to:
  - Identify the subject of the request
  - Monitor transaction activity of the subject
  - Identify potential suspicious activity and submission of a SAR
- National Security Letters – highly confidential requests submitted by local FBI and other federal government authorities which cannot be disclosed to the subject of the investigation by anyone in the institution
- Manual Monitoring – to include employee identification of unusual activity and unusual activity identified through a manual review of computer printouts, reports, logs, etc.
- Transaction Monitoring (a.k.a. automated client account monitoring) – to identify individual transaction, patterns of activity, or deviations from expected activity. Multiple and overlapping rules may be applied creating a higher level of alert complexity. Uses thresholds and parameters which may be tuned.

Institutions should ensure that their suspicious activity program includes an evaluation and, if required, an escalation of any unusual activity regardless of how identified including referrals from any and all areas of the bank. There should be sufficient staff assigned to the processes who are also provided with ongoing targeted training in order to maintain their expertise in the investigation process. Investigation staff should also have the necessary tools such that research activities and the development of the narratives can be properly performed.

The escalation processes should encapsulate the point of initial detection to the final disposition of the investigation and include the recommendation to file a suspicious activity report (SAR). The key benefits of having a highly prescriptive set of protocols or instructions is *consistency* in the investigation and disposition and *quality* of the evidence collected and narrative provided supporting the disposition of each alert and case.

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine if the ***Transaction Monitoring alert investigation and disposition protocols*** meet the regulatory requirements as illustrated in the table below:

Transaction Monitoring Alert Investigation and Disposition Protocols (§504.3(a)(7))				
Risk	Control Name	Control Objectives	Evidence of Control	Tests of Control
Protocols are not current, not written or not understood	Protocol implementation	To ensure that the protocols are current, written and understood by investigators	Alert investigation and disposition procedure Quality control procedures SAR recommendation and submission procedures	Obtain and review the current version of the investigation and disposition procedure and confirm it matches the actual processes Obtain and review the current version of the quality control procedure and confirm it matches the actual processes Obtain and review the current version of the SAR recommendation and submission procedures and confirm they match the actual processes
Protocols are not understood and therefore not followed	Protocol training	To ensure that the protocols are understood by the investigators	Training log Case reject log Aged report of 'unresolved' cases	Obtain and review the training log to confirm all investigators have been trained on the investigation and disposition protocols Obtain and review the case reject log and identify any investigators who have had an unusually high number of cases rejected due to lack of information or quality or who have had an unusually low number of cases escalated for SAR filing
Protocols are not prescriptive	Protocol detail	To ensure that the protocols are prescriptive	Protocol process review	Obtain and review the protocol and confirm each step in the process is clearly detailed in an easy to understand format

MODEL VALIDATION (§504.3(a) (8))

Both the *Supervisory Guidance on Model Risk Management*, published by the Office of the Comptroller of the Currency ("OCC") in 2011, and the Federal Reserve's Supervisory Letter, *SR11-7*, issued in 2011, describe the term model as "a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates."[xxii] In BSA/AML layman's terms it can be thought of more simply as an algorithm designed to identify suspicious activities or 'red flags'[xxiii] for both money laundering and terrorist financing.

The Rule prescribes that periodic independent model validation to assess relevancy of scenarios, underlying rules, threshold values, parameters and assumptions be performed. There are three components of a model including:

1. "An information **input** component, which delivers assumptions and data to the model;
2. A **processing** component, which transforms inputs into estimates; and
3. A **reporting** component, which translates the estimates into useful business information."[xxiv]

Considering these three components the validation then needs to consider data for inputs, calculations for processing and data outputs for reporting. Critical here is the quality of data which correlates to the accuracy of calculations and output. Best practices for model validation include an assessment of sourced data, assumptions and any data exclusions, design considerations and logic, calculation routines including parameters, thresholds, and specific criteria, and alert output.

The primary purpose of performing the model validation is to ensure that the models are performing as they were designed including the confirmation of model thresholds, limit settings and parameters. This requires a review of model governance, model policies and procedures, source data used by the models, model performance and alert output. The key activities in performing a model validation assessment are:

- Model governance – review of policy and procedures, change management processes, prior model validation reports, management roles and responsibilities;
- Model coverage – linkage of the detection scenario against red flags and the institution's BSA/AML risk assessment and identification of any models that should be either added or considered for decommissioning;
- Model input analysis – review and confirm all applicable source systems are providing the required customer, account, reference and transactional information to the Transaction Monitoring platform and document where any information is being excluded in the extraction and loading process;
- Model logic analysis – review the model documentation and logic design, develop use cases including test data and expected output, process against each model and document results, and assess models from both a qualitative and quantitative basis; and
- Model output analysis – assess the design output of each model and confirm through testing that the output conforms to the design and that the results are accurate.

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine if the ***Transaction Monitoring model validation program*** meets the regulatory requirements is illustrated in the table below:

Transaction Monitoring Model Validation Program (§504.3(a) (8)				
Risk	Control Name	Control Objectives	Evidence of Control	Tests of Control
Does not follow regulatory guidance	Regulatory guidance	To ensure that the model validation program follows regulatory guidance	References to OCC Supervisory Guidance on Model Risk Management	Obtain and review the model validation report and confirm it considers guidance from the OCC Supervisory Guidance on Model Risk Management and the NYDFS Rule 504
Does not incorporate model validation governance	Model governance	To ensure that the model validation program contains a strong governance component	Model validation policy and procedure includes section on governance	Obtain and review the model validation governance documentation and confirm it contains policy and procedures, change management processes, prior model validation reports, management roles and responsibilities

Transaction Monitoring Model Validation Program (§504.3(a) (8))				
Risk	Control Name	Control Objectives	Evidence of Control	Tests of Control
Does not assess if the models address the risk assessment	Model coverage	To ensure that the models address the inherent risks identified in the risk assessment	Coverage model assessment	Obtain and review the coverage model assessment and confirm that all inherent risks have been covered by one or more models or if not then rationale as to why not
Does not include an analysis of model inputs, calculations or outputs	Model component validation	To ensure that each model in the model validation has a detailed assessment of the model inputs, calculations and outputs	Model validation report	Obtain and review the model validation report and confirm each model has an analysis of inputs, calculations and outputs
Not supported by a governance function	Model governance	To ensure that the model validation program has a strong governance requirement	Model validation policy and procedure	Obtain and review the model validation policy and procedure and confirm it incorporates a well-articulated governance function

FILTERING PROGRAM (§504.3(b))

OFAC RISK ASSESSMENT (§504.3(b) (1))

As is the case with BSA/AML, neither OFAC nor the FFIEC BSA/AML Examination Manual state that an institution is required to have an OFAC risk assessment or even an OFAC Program, as OFAC is not itself a bank regulator. However, OFAC requires that financial institutions not violate the laws that it administers, and confirm with their regulators regarding the suitability of specific programs to their unique situations. Therefore, any ambiguity on the requirements of an OFAC risk assessment and Program is now clarified under the new Rule which requires linkage between the OFAC risk assessment and the Filtering Program.[xxv] For example, the statement "that the Filtering Program needs to be based on a risk assessment" prescribes there actually be an OFAC risk assessment for use in identifying what detection scenarios best mitigate the inherent OFAC sanctions risks.[xxvi]

Similar to what was discussed in the BSA/AML risk assessment section, the steps involved in developing an OFAC risk assessment are also beyond the scope of this paper. However, the components of an OFAC risk assessment should include the identification of specific risk categories (i.e. products, services, customers/counterparties, transactions and geographic locations) specific to the institution followed by a detailed assessment of both qualitative and quantitative information toward identification of the institution’s inherent OFAC risks, the effectiveness and impact of mitigating controls culminating in residual risk scores. The institution's products and services may, by nature of their degree of anonymity or volume of currency, pose increased risk of money laundering or terrorist financing. Certain types of customers / counterparties may also subject the institution to increased risk based on the type of customer / counterparty (e.g. nonbank financial institutions, senior foreign political figures, nonresident aliens, etc.), and the geographic locations the institution does business in, where customers open accounts from, or facilitating transactions involving high risk geographies (e.g. OFAC sanctioned countries, jurisdictions consider to be of primary money laundering concern, offshore financial centers, etc.).

Development of the qualitative and quantitative information for the risk assessment includes the collection and analysis of metrics around the customer / counterparty base, transactions processed and in which geographies customers / counterparties and transactions are processed. Existing controls are identified and assessed against the inherent risks to determine the residual risks and overall risk profile of the institution.

The risk assessment process must be periodically updated to reflect changes to OFAC Program prohibited entities and jurisdictions, regulations (e.g. applicability of OFAC licenses) and regulatory warnings and other relevant institutional information. The Rule does not specify what is meant by periodic updates but again, experience indicates that documents, such as a risk assessment, in meeting this requirement should be reviewed and updated annually or when material changes have occurred in the institution's products and services, customers / counterparties and geographies (e.g. opening of a new branch in a high risk geography, divestiture of a line of business, changes to the AML risk appetite, etc.) or when OFAC laws, regulations or regulatory warnings have been issued.

Finally, the OFAC risk assessment should be written to be easily understood by all appropriate parties in the institution and communicated to all business lines, the Board of Directors, management and appropriate staff.

There should be no mistake that the NYDFS now requires a comprehensive risk assessment that lays the foundation for the required OFAC program controls the institution must design and implement to mitigate its risks. In mitigating these risks, the institution under the Rule, must select and implement the appropriate filters, lists and controls to identify sanctions violations.

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine if the ***OFAC risk assessment*** meets the regulatory requirements is illustrated in the table below:

OFAC RISK ASSESSMENT (§504.3(b)(1))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
All products and services have not been identified in the risk assessment	Products / services	To ensure that all the relevant products and services have been identified	Cross-referenced list of the institution's products/services Job aid document Confirmation email from each line of business	Review the OFAC risk assessment and confirm that all of the institution's applicable products and services have been included and addressed in the risk assessment
All customer types have not been identified in the risk assessment	Customer types	To ensure that all the relevant customer types have been identified	Cross-referenced list of the institution's customer types Job aid document Confirmation email from each line of business	Review the OFAC risk assessment and confirm that all of the institution's different customer types have been included and addressed in the risk assessment
All relevant geographies served by the institution have not been identified in the risk assessment	Geographies	To ensure that all the geographies served by the institution have been identified	Cross-referenced list of the institution's geographies served Job aid document	Review the OFAC risk assessment and confirm that all of the geographies served by the institution have been included and addressed in the risk assessment

OFAC RISK ASSESSMENT (§504.3(b)(1))				
Risk	Control Name	Control Objectives	Evidence of Control	Tests of Control
Risk assessment does not indicate what scenarios (models) should be implemented to mitigate the inherent risks	Scenarios	To ensure that each of the applicable inherent risks have been addressed by one or more transaction monitoring scenarios	Coverage model assessment	Review the OFAC risk assessment and confirm there is a cross-reference of inherent risks to transaction monitoring scenarios
Inherent risks have not been fully identified	Inherent risks	To ensure that all the relevant inherent risks have been identified	Quantity of risk matrix in risk assessment	Review the OFAC risk assessment and confirm that the quantity of risk matrix identifies the inherent risks to the organization
Other qualitative risk factors have not been considered	Other qualitative risk factors	To ensure that other qualitative risk factors that may impact inherent risks have been considered in the risk assessment	Assessment of other qualitative risk factors and determination as to use in the risk assessment	Review the other qualitative risk factors assessment document and confirm that these have been considered in the overall inherent risks. Other qualitative risk factors include: • Client base stability • Integration of IT systems • Expected account/client growth • Expected revenue growth • Recent AML Compliance employee turnover • Reliance on third party providers • Recent/planned introductions of new products and/or services • Recent/planned acquisitions • Recent projects and initiatives related to AML Compliance matters (e.g. remediation, elimination of backlogs, off-shoring) • Recent relevant enforcement actions National Risk Assessments

FILTERING PROGRAM NAME AND ACCOUNT MATCHING (§504.3(b)(2))

Filter programs must comply with Office of Foreign Assets Control (OFAC) regulations and ensure that their payment and funds transfer systems are not being used by customers on the Specially Designated Nationals list or other watch lists as provided by the Treasury Department, State Department and Commerce Department including:

- OFAC sanction lists (SDN, Palestine Legislative Council List, etc.);

- Other official watch lists (e.g. Interpol most wanted, etc.);
- Country sanction lists;
- Geographic sanction lists;
- Business specific sanction list (e.g. exporters); and
- Internal lists of the institution's high risk customers.

Filter programs detection scenarios (often also referred to as "filters", "screening" or "matching models") include algorithms for name-matching. These algorithms may include deterministic (exact match) and indirect match (no direct match relationship), or probabilistic matching which could include partial matches, fuzzy logic matching or phonetic matching. The matching algorithms process language translations, misspellings, alternate spellings, abbreviations, synonyms, acronyms, initials, concatenated words, compound words and special search terms.

No matter the solution used, institutions need to establish policies, procedures and processes to review transactions and parties on those transactions. "The program should include written policies and procedures, establish protocols for screening customers and transactions, blocking, rejecting and reporting transactions to OFAC, designated OFAC Compliance Officer, Governance and Oversight Committees, training for employees and independent testing for compliance."[xxvii]

Institutions are required to perform OFAC filtering during the initial customer on-boarding, subsequently when processing transactions, and periodically even when there are no transactions requiring another screening. When on-boarding a new customer, institutions must compare the customer or account name and if applicable any legal entity beneficial owners against applicable OFAC lists[xxviii] prior to the account being opened or shortly thereafter. It is the institution's responsibility to decide whether the review of potential OFAC violations should be performed manually or through interdiction software or through some combination of both. In those instances where the number of funds transfers is extremely low (e.g. 5 per day) then a manual review might be in order otherwise an automated interdiction software solution should be used.

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine if the ***Filtering Program name and account matching*** meets the regulatory requirements is illustrated in the table below:

FILTERING PROGRAM NAME AND ACCOUNT MATCHING (§504.3(b)(2))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
Matching threshold set too high	Threshold	To ensure that the name matching threshold is not too limiting	Model validation report Tuning report	Obtain and review the model validation report and confirm the threshold tuning was tested
Filter does not consider all appropriate lists	List	To ensure that all relevant lists are being referenced by the filter	Filter program requirements document	Obtain and review the filter program requirements document to identify the required program lists

FILTERING PROGRAM NAME AND ACCOUNT MATCHING (§504.3(b)(2))				
Risk	Control Name	Control Objectives	Evidence of Control	Tests of Control
			OFAC risk assessment	Review the filter program lists and updates and confirm all required lists are being processed

END-TO-END PRE-AND POST-IMPLEMENTATION TESTING (§504.3(b)(3))

This subsection of the Rule prescribes a comprehensive set of so called 'end-to-end' control tests of the Filter Program system covering the areas of governance, data mapping, transaction coding, filter screening logic, model validation, data input and program output.

Pre-implementation activities are those required management actions that must occur prior to a new or materially changed Filter Program system going live. The purpose of these activities is to ensure, to the extent possible, that once the system goes live it will produce the required results, operate as intended, protecting the institution from the threats of money laundering and terrorist financing and will provide the means for the institution to adhere to all the relevant laws, regulations and best practices.

Post-implementation activities are those required management actions that must occur after a new or materially changed Filter Program system has gone live. The purpose of these activities is to ensure, to the extent possible, that the system has met the design objectives, that it is appropriately managed and staffed with qualified personnel and that it is protecting the institution from the threats of money laundering and terrorist financing.

The pre- and post-implementation testing steps should be performed to ensure that the required activities were successfully completed and that the supporting programs around data, coding, filter screening logic, model validation and data input/output are operating effectively and regularly maintained.

As previously noted, testing is the cornerstone of auditing the effectiveness of controls of the OFAC program. Controls are the system of internal controls (including policies, procedures, and systems) used to mitigate OFAC risks. To ensure that the OFAC controls are effective the following types of tests should be performed: (1) reperformance using a "new transaction to see which controls are used and the effectiveness of those controls;" (2) observation of "a business process in action and the control elements of the process;" and (3) inspection of "business documents for approval signatures," initials, signoffs or stamps confirming that a particular control has been performed.[xxix]

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine if the ***Filtering Program end-to-end pre and post-implementation testing*** meets the regulatory requirements is illustrated in the table below:

FILTERING PROGRAM END-TO-END PRE- AND POST-IMPLEMENTATION TESTING (§504.3(b)(3))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
Pre-implementation project risks not mitigated	Implementation project risks	To ensure that project scope and related implementation risks are mitigated	Periodic reviews of: • project risks • "to be" design • data conversion • integration testing readiness / go live	Obtain and review: • Adequate budgets and funding have been approved • Steering committee charter • PMO and milestone plans • QA/QC plans and results • Requirements documentation • Implementation staffing • Design model • System interfaces • Integration test plan and results • Training plan and attendance schedule • User acceptance testing plan • Level of vendor involvement • User and business sign-offs • Go live plan • Post implementation plan
Failure to perform post-implementation activities	Post-implementation activities	To ensure that the post-implementation plan is properly executed	Post-implementation results documentation	Obtain, review and confirm: • Business, regulatory, IT and security requirements were met • Controls were implemented as planned • Key controls were tested • Customers, accounts and transactions were successfully processed through integration tests • Approved changes were tested • Users and business have accepted the system • System results map back to requirements • System has appropriate levels of internal and external (vendor) support • Service level agreements are in place • Appropriate BCP tiering (e.g. level 1, 2 or 3) have been assigned to the applications

MODEL VALIDATION (§504.3(b) (4))

Also applicable to OFAC models is the "Supervisory Guidance on Model Risk Management" published by the Office of the Comptroller of the Currency (OCC) and Federal Reserve's SR letter 11-7 which describes the term 'model' as "a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates."[xxx] In layman's terms it can be thought of more simply as an OFAC filter designed to identify individuals on the SDN and Blocked Person list such that they are not on-boarded as customers to the institution. These models are also used to scan business activity to identify transactions that are for or on behalf of individuals on the SDN or Blocked Person list or which originate, pass through or conclude in a listed country covered under economic sanctions, embargo programs or targeted geographic regions and governments.

The Rule prescribes that periodic independent model validation to assess relevancy of scenarios, underlying rules, threshold values, parameters and assumptions be performed. Where the vendor's solution is proprietary and access to the mathematical routines and logic are not exposed a separate process can be utilized to test these filters. One such method is to develop a test bed of data that contains transactions designed to not have any information that should hit on an OFAC Sanctions list and transactions that should hit. Running these both through the vendor's proprietary filter and evaluating the results will assess the accuracy of the filter logic and matching processing.

There are three components of a model including "an information <u>input</u> component, which delivers assumptions and data to the model; a <u>processing</u> component, which transforms inputs into estimates; and a <u>reporting</u> component, which translates the estimates into useful business information."[xxxi] Considering the three components then the validation needs to consider data for inputs, calculations for processing and data outputs for reporting. Critical here is the quality of data which is directly correlated to the accuracy of calculations and output. Best practices for model validation include an assessment of sourced data, assumptions and any data exclusions, design considerations and logic, calculation routines including parameters, thresholds, and specific criteria, and alert output.

The primary purpose of performing the OFAC model validation is to ensure that the OFAC filters are performing as they were designed including the confirmation of filter thresholds, limit settings and parameters. This requires a review of model governance, model policies and procedures, source data used by the models, model performance and alert output.

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine if the ***Filtering Program model validation*** meets the regulatory requirements is illustrated in the table below:

FILTERING PROGRAM MODEL VALIDATION (§504.3(b)(4))				
Risk	Control Name	Control Objectives	Evidence of Control	Tests of Control
Does not follow regulatory guidance	Regulatory guidance	To ensure that the model validation program follows regulatory guidance	References to OCC Supervisory Guidance on Model Risk Management	Obtain and review the model validation report and confirm it considers guidance from the OCC Supervisory Guidance on Model Risk Management and the NYDFS Rule 504
Does not incorporate model validation governance	Model governance	To ensure that the model validation program contains a strong governance component	Model validation policy and procedure includes section on governance	Obtain and review the model validation governance documentation and confirm it contains policy and procedures, change management processes, prior model validation reports, management roles and responsibilities
Exact match filter not performing as designed	Exact match	To ensure that the exact matching filter is performing as designed	Exact match filter design logic and current settings	Test the filter's capabilities to match sanctioned names as they appear on the sanction lists
Risk information match filter not performing as designed	Risk information match	To ensure that the risk information match filter is performing as designed	Risk information match filter design logic and current settings	Test the filter's capabilities to match additional risk information correctly such as BICs and country names
Fuzzy logic match filter not performing as designed	Fuzzy logic match	To ensure that the fuzzy logic filter is performing as designed	Fuzzy logic filter design logic and current settings	Using a pre-developed set of transactional data with fuzzy name variations in different transactions, test the filter's capabilities to match the test set of name variants.

MODEL DOCUMENTATION (§504.3(b)(5))

As is the case with Transaction Monitoring, this subsection of the Rule prescribes that OFAC models have written documentation including any underlying assumptions, parameters and thresholds. Documentation should be formal (e.g. written, dated with approval signatures) and supplemented utilizing the institution's formal change management process whenever changes to the models are required.

The Filtering Program documentation from third parties should also include details around the intent and design of the filtering program tools, processes or technology. Vendor documentation should also include a description of the out-of-the-box underlying filter assumptions, watch-list filtering capabilities, SDN list filtering processes and update procedures, name-matching technologies and implementation considerations, parameters, thresholds and default above / below the line thresholds. The information needs to be linked back to the OFAC risk assessment and include rationale as to why the operational settings have been established to their current values.

Over time it is recognized that certain model changes will need to be made, such as the addition, deletion, deactivation or changes to the model's run schedule, reference period, parameters or thresholds. These changes may be required due to changes in the BSA/AML risk assessment, regulatory changes, industry standards or simply due to the fact that the model is producing alerts of minimal suspicious activity value. When changes are required it is critical to adhere to strict change management processes to document all of the activities and approvals involved. In addition to the necessary governance functions around this process there are several key activities that should be performed. The Information Technology Service Management[xxxii] ("ITSM") organization defines the core activities of a change management process as: [xxxiii]

- "Receiving change requests from appropriate parties
- Determining whether or not the change is appropriate
- Assigning the change to resources within IT for solution identification, sizing and risk analysis
- Accepting or rejecting the requested change
- Assigning the change to solution development resources
- Reviewing the solution prior to implementation
- Scheduling the change
- Communicating change status as required to all interested parties
- Closing the change."

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine if the ***Filtering Program model documentation*** meets the regulatory requirements is illustrated in the table below:

FILTERING PROGRAM MODEL DOCUMENTATION (§504.3(b)(5))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
Source systems not documented	Source systems documentation	To ensure that all the systems of record applicable to the OFAC program have been documented	Source systems diagram	Review the source systems diagram to understand and confirm the feeds to the OFAC platforms have been documented
Data from source systems not documented	Source systems data documentation	To ensure that all the required data from all the applicable source systems has been documented	Data flow diagram	Review the data flow diagrams documentation to understand and confirm that the data feeds from each of the source systems has been documented
ETL not documented	ETL documentation	To ensure that the ETL process has been documented	ETL documentation	Review the ETL documentation to ensure it clearly describes the extraction, transformation and loading processes including any assumptions made.
Filter models not documented	Model documentation	To ensure that the Filtering Program	Filter model documentation	Review the filter model documentation to ensure it clearly describes the input,

FILTERING PROGRAM MODEL DOCUMENTATION (§504.3(b)(5))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
		model(s) have been documented		calculation and logic, and output steps involved in each model
Change control procedure not documented	Change management	To ensure that changes to the filter program models follow a prescriptive process	Change control	Review the filter program change control procedure to ensure it covers all the necessary activities from initiating a change request through final implementation

EACH TRANSACTION MONITORING AND FILTERING PROGRAM (§504.3(c))

IDENTIFICATION OF ALL RELEVANT DATA SOURCES (§504.3(c)(1))

To identify the relevant data sources per this subsection of the Rule, the institution must reference the technical specifications documents ("TSDs") or similar documentation for both the Transaction Monitoring and Filtering Programs. The TSDs describe how the system functions have been designed to perform and what data from each of the systems of record are required. For solutions purchased from third-party vendors, the data requirements will be documented and available from the vendor, who will generally be available to provide assistance in identifying the institution's data sources that contain the required relevant data. It is the institution's responsibility to ensure that the data meets the data quality requirements and is obtained from "systems of record."[xxxiv].

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine if the ***identification of all relevant data sources for both the Transaction Monitoring and Filtering Program*** meets the regulatory requirements is illustrated in the table below:

IDENTIFICATION OF ALL RELEVANT DATA SOURCES (§504.3(c)(1))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
Extraction and loading programs may exclude or drop required information	Data completeness	To confirm that all of the required data from each of the identified systems of record are submitted to the BSA/AML and OFAC platforms	Control report from each system of record Control report for data loaded to BSA/AML and OFAC platforms	For each system of record (e.g. feeder system) develop and execute a query to select and calculate the number of transactions that are extracted and sent to the BSA/AML and OFAC platforms for subsequent loading
A source system may have an extract error, may send duplicate data or may not send data due to a holiday	Data quality	To confirm data quality is not compromised due to an unexpected source system event	Operational and system procedure for data extraction and loading	Review the error recovery system documentation and holiday processing procedures
Source system functions and processes may change impacting the data required	Data availability	To confirm that source system owners don't make changes that impact the data extracts for BSA/AML and OFAC	Service Level Agreement (SLA)	Review the service level agreements and confirm they are current, include a commitment to provide required data and require agreement from Compliance in order to change any of the data extracts for BSA/AML and OFAC

DATA VALIDATION (INTEGRITY, ACCURACY AND QUALITY) (§504.3(c)(2))

Data integrity, accuracy and quality are somewhat general terms commonly used to describe the general state of data. However, they have very different meanings. Data quality means something (such as the data element, record or message, data set or database) that can be measured to determine the quality of data. Within the context of the Transaction Monitoring and Filtering Programs, data quality is understood to have six core dimensions:[xxxv]

1. *Completeness* – the Transaction Monitoring and Filter Programs contain all of the data that are required to perform their respective functions
2. *Uniqueness* – data is recorded only once
3. *Timeliness* – data is available to the Transaction Monitoring and Filter Programs in the time period required
4. *Validity* – data conforms to its required syntax (format, type, range)
5. *Accuracy* – data correctly represents the object or event being described
6. *Consistency* – the data from the source systems is the same as the data received and used by the Transaction Monitoring and Filtering Programs

Data integrity, however, refers to the assurance of accuracy and consistency of data used by the Transaction Monitoring and Filter Programs over its entire life-cycle (e.g. across all the different processes involved). The intent of a data integrity technique is to "ensure data is recorded exactly as intended," and, when subsequently reviewed, "the data is the same as it was when originally recorded."[xxxvi]

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine if the ***data validation for both the Transaction Monitoring and Filtering Program*** meet the regulatory requirements is illustrated in the table below:

DATA VALIDATION (INTEGRITY, ACCURACY AND QUALITY) (§504.3(c)(2))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
Data extracted from source systems may have poor quality	Data completeness	To confirm that the data to be sourced from systems of record does not have data quality problems	Data quality report	Compare the total number of records sent by source systems to the total number of records received by the Transaction Monitoring and Filter Programs
Duplicate data	Data uniqueness	To confirm that the data in the Transaction Monitoring and Filter Programs occurs only once	Data quality report	Sample data from the Transaction Monitoring and Filter Programs and search to confirm the data record only occurs once in the system
Transactions from incorrect time periods	Data timeliness	To confirm that the sourced data is current with respect to the processing requirements of the Transaction Monitoring and Filter Programs	Data quality report	Sample data from source systems to confirm that the extracted data are in the appropriate reference period as required by the Transaction Monitoring and Filter Programs
Data not valid	Data validity	To confirm that the data is in the correct	Data quality report	Sample data to confirm that data sourced from the systems of record and loaded to

DATA VALIDATION (INTEGRITY, ACCURACY AND QUALITY) (§504.3(c)(2))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
		format, represent the correct type of data and are in the range expected		the Transaction Monitoring and Filter Programs is valid
Data not accurate	Data accuracy	To confirm that the data present in the information sourced is accurate in its representation of the information	Data quality report	Sample data to confirm that the data in the Transaction Monitoring and Filter Programs is accurate
Data is not consistent between the various systems	Data consistency	To confirm that the data extracted from the source systems is the same as the data received by the Transaction Monitoring and Filter Programs	Data quality report	Sample data from both the source systems and the Transaction Monitoring and Filter Program systems and compare to ensure consistency

DATA EXTRACTION AND LOADING PROCESSES FOR AUTOMATED SYSTEMS (§504.3(c) (3))

Data extraction and loading is commonly referred to as the process of extract, transform and load ("ETL"), and includes all of the activities involved in obtaining data from each of the respective source systems, transforming that data from its native format to a required format, then ingesting the transformed data into the Transaction Monitoring and Filter Program systems. Characteristics of data quality need to be considered in addition to the ETL processes.

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine if the ***data extraction and loading processes for both the Transaction Monitoring and Filtering Program*** meet the regulatory requirements is illustrated in the table below:

DATA EXTRACTION AND LOADING PROCESSES FOR AUTOMATED SYSTEMS (§504.3(c)(3))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
Data extraction does not contain all of the required data	Data completeness	To confirm that the data sourced from systems of record is complete	Data quality report	Compare the total number of records available for extraction in each source system to the total number of records extracted and received by the Transaction Monitoring and Filter Programs
Incorrect transformation of data from one format to another	Data transformation	To confirm that the data subject to transformation rules is correctly transformed	Data quality report	Take a sample of transactions that have data elements transformed. Compare the data elements before and after the transformation and confirm the result is as expected

DATA EXTRACTION AND LOADING PROCESSES FOR AUTOMATED SYSTEMS (§504.3(c)(3))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
Ingestion of transformed data drops or excludes data	Data ingestion	To confirm that the transformed data is completely ingested by the Transaction Monitoring and Filter Programs	Data quality report	Compare the total number of transactions transformed with the total number of transactions ingested by the Transaction Monitoring and Filter Programs to ensure equal data

GOVERNANCE AND MANAGEMENT OVERSIGHT (§504.3(c)(4))

According to a recent report published by the Banking Law Journal, "every one of the major 2012 and early 2013 [BSA/]AML enforcement actions cited insufficient corporate governance."[xxxvii] The Board of Directors ultimately have responsibility for their institution's BSA/AML and OFAC decisions. Governance is the level of oversight the Board of Directors and senior management have implemented over the BSA/AML and OFAC programs.[xxxviii] Governance includes policies, standards and procedures, assigning ownership through roles and responsibilities, ensuring staff are capable in carrying out their duties by providing frequent training and requiring staff have appropriate certifications according to their roles, within a program of rigorous controls including both compliance testing and independent testing of the control programs.

For those foreign banking organizations' operating entities (e.g. branches, representative offices or other affiliations) within the United States, local senior management has a responsibility to provide regular and sufficient information regarding their BSA/AML compliance to the firm-wide governance functions established by the entity's Home Office. When issues are identified, escalation to Home Office is essential as senior Home Office management has a responsibility to understand the BSA/AML risk and control environment of their U.S. entities and to assist or take corrective action when there are program deficiencies.

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine if the ***governance and management oversight for both the Transaction Monitoring and Filtering Program*** meets the regulatory requirements is illustrated in the table below:

GOVERNANCE AND MANAGEMENT OVERSIGHT (§504.3(c)(4))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
The Board of Directors has not approved the BSA/AML program	BSA/AML program	To ensure the board understands and has approved the BSA/AML program including the risk appetite	Board of directors meeting agenda and notes	Review Board Meeting minutes to determine if the board has approved the BSA/AML compliance program

GOVERNANCE AND MANAGEMENT OVERSIGHT (§504.3(c)(4))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
The Board of Directors is not taking an active role in management oversight of the BSA/AML compliance functions	BSA/AML compliance functions	To ensure the board oversees both the structure and management of the BSA/AML compliance functions	Board of directors meeting agenda and notes	Review Board Meeting minutes to determine if the board takes an active role in overseeing the structure and management of the institution's BSA/AML compliance functions
No or weak tone at the top	Tone at the top	To ensure the board communicates a culture of compliance	Corporate communications	Determine if the board sets an appropriate tone at the top by reviewing corporate communications: - Frequent company communications about the AML regulatory requirements - Publicized risk appetite statement - Prominent support for AML education - Authorization to fund new technologies or major enhancements to the AML program - Authorization to fund sufficient levels of qualified staff to the AML program - Employee incentives/disincentives for support and compliance with the AML program
BSA/AML policies are not board approved	Policy approval	To ensure that the board has reviewed and agreed with the BSA/AML policies	Board of directors meeting agenda and notes	Determine if the board approves all BSA/AML policies
The board has not empowered senior management to perform their duties	Empowerment	To ensure that the board has qualified management to carry out the BSA/AML duties	Organization structure and roles and responsibilities (position description)	Determine if the board has ensured senior management are empowered and qualified to carry out their duties
Organizational structure does not provide required level of authority	Organization structure	To ensure that the board has structured the organization such that the BSA/AML compliance officer and compliance personnel have required authority	Organization structure and roles and responsibilities (position description)	Determine if BSA/AML compliance management and compliance personnel in lines of business have required authority to carry out their duties
Board does not penalize or reward staff based on BSA/AML performance	Culture of compliance	To ensure there are rewards and penalties for staff based on BSA/AML program performance	HR policy	Determine if the annual performance plan incentivizes management for BSA/AML compliance successes and failures

VENDOR SELECTION PROCESS (§504.3(c)(5))

If a third-party vendor is used to acquire, install, implement or test the Transaction Monitoring or Filtering Program or any aspect of it then this subsection of the Rule prescribes there be written documentation supporting the vendor selection process used by the institution. The type, format or content needed to support the vendor selection process, however, is not described in the Rule. In practice, there are several methods used by institutions to select BSA/AML and OFAC consulting and/or solution vendors.

In general, the following activities should be included in the vendor selection process supported by formal written documentation:

- Project approval from senior management;
- Business and regulatory requirements (must haves and nice to haves);
- Technology and security requirements (must haves);
- Market assessment of potential vendors and solutions;
- Request for proposal ("RFP") and scoring model;
- Vendor proposals and costs;
- Short-list of vendors;
- Vendor presentations and reference checks;
- Legal and IT security clearances;
- Vendor selection; and
- Contracting

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine if the ***vendor selection process for both the Transaction Monitoring and Filtering Program*** meets the regulatory requirements is illustrated in the table below:

VENDOR SELECTION PROCESS (§504.3(c)(5))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
Program requirements have not been identified and documented	Requirements documentation	To ensure that the program requirements have been identified and documented	Business requirements document ("BRD")	Review the business and technical documentation for the program to confirm that the requirements were developed and documented
RFP not submitted	RFP	To ensure that several vendors were evaluated for consideration	RFP responses	Review the RFP distribution list to confirm that several vendors who offer the types of solutions applicable to the institution were considered
Vendor selection process weighted to highly on solution cost	Scoring and selection criteria	To ensure that the selected vendor was not determined primarily through cost of the solution	Pricing model	Review the selected vendor's pricing model and criteria used for final vendor selection to confirm primary qualification was not cost

VENDOR SELECTION PROCESS (§504.3(c)(5))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
Vendor solution is used by institution's peers	Representative usage	To ensure that the selected vendor solution is used by peer institutions and recognized by the institution's regulators	Market assessment	Review the market assessment report to confirm that each of the vendor solutions being considered are recognized market solutions

APPROPRIATE PROGRAM FUNDING (§504.3(c)(6))

The Transaction Monitoring and Filter Programs must be adequately funded such that appropriate tools, technologies and sufficient levels of qualified staff are approved and applied to the various BSA/AML and OFAC programs. Each institution must consider and determine what level of funding is appropriate and sufficient considering volumes of activity occurring during an average month such as the number of customers (by type) on-boarded, number of transactions (by type) processed, number of scored alerts created, number of AML relevant lines of business, overall level of AML program automation, number of SARs created, number of 314(a) and (b) information requests processed and so forth. For institutions with higher risk customer types and higher risk transactions, including processing transactions through high risk geographies, a higher level of investment (e.g. people, processes and technology) in the AML program should be sustained in order to address and mitigate the inherent risks.

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine ***if the appropriate program funding for both the Transaction Monitoring and Filtering Program*** meets the regulatory requirements is illustrated in the table below:

APPROPRIATE PROGRAM FUNDING (§504.3(c)(6))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
Insufficient funding for AML training	AML training funding	To ensure that the funding for staff general and targeted AML training is sufficient	Roster of staff trained during the past year Number of AML training programs available Number of AML staff CAMS certified	Review AML training roster and identify staff who did not attend any AML training - Contact employee and determine if training not approved due to lack of funding Review certifications for AML staff and confirm membership in ACAMS is current and CAMS certifications have not expired
Insufficient funding for OFAC filtering technology	OFAC filtering technology or staffing funding	To ensure that the funding to support OFAC filtering and clearing is sufficient	Number of transactions processed by the OFAC function are manageable	Review the volume of transactional activity and confirm that it can be properly dispositioned by the means in place (manual or automated) - Review backlog

APPROPRIATE PROGRAM FUNDING (§504.3(c)(6))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
				- Review unworked alerts at end of month
Insufficient funding for transaction monitoring technology	Transaction monitoring technology or staffing funding	To ensure that the funding to support the identification and clearing of suspicious activity is sufficient	Number of transactions processed by the monitoring function are manageable	Review the volume of transactional activity and confirm that it can be properly dispositioned by the means in place (manual or automated) - Review backlog - Review unworked alerts at end of month
Insufficient funding for customer on-boarding	Customer on-boarding technology or staffing funding	To ensure that the funding to support the on-boarding of customers is sufficient	Number of customers on-boarded in an average month Number of high-risk customers on-boarded in an average month	Review the volume of customers on-boarded during an average month and confirm that the process supports sufficient due diligence and enhanced due diligence - Review backlog of customers in on-boarding queue - Review volumes of negative news - Review volume of high risk customers

QUALIFIED PERSONNEL TO PERFORM THE PROGRAM REQUIREMENTS (§504.3(c)(7))

BSA Compliance Officers should be qualified with extensive knowledge of money laundering and terrorist financing risks to the institution in addition to the applicable money laundering and terrorist financing laws and regulations. It is also important that the BSA Compliance Officer has sufficient knowledge of the institution's business, the products, services, operations, general customer base, as well as a detailed understanding of the BSA/AML and OFAC risk assessments.

Staff responsible for various aspects of the Transaction Monitoring and Filter Programs should also be qualified through regular targeted training and achieve recognized certifications such as the ACAMS Certified Anti-Money Laundering Specialist (CAMS), ACAMS KYC CDD Certificate, ACAMS Counter-Terrorist Financing Certificate, the ACAMS CAMS-Audit Advanced AML Audit Certification or the ACAMS CAMS-FSI Certification.

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine ***if the institution's personnel who perform the program requirements for both the Transaction Monitoring and Filtering Program are qualified*** to meet the regulatory requirements is illustrated in the table below:

QUALIFIED PERSONNEL TO PERFORM THE PROGRAM REQUIREMENTS (§504.3(C)(7))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
Suspicious transactions or transactions involving names/countries on sanctions lists are not identified	Position qualification	To ensure that individuals working in the Transaction Monitoring and Filter Programs have sufficient knowledge and qualifications to recognize suspicious money laundering and terrorist financing activities	Certifications and training records: - CAMS - KYC CDD - Counter Terrorist Financing - CAMS AUDIT - CAMS FSI - Annual training records	Review the position descriptions for employees in each area of the Transaction Monitoring and Filter Program and confirm that employees have appropriate certifications and attended regular targeted training programs
BSA Compliance Officer unqualified	BSA Compliance Officer qualifications	To ensure that the BSA Compliance Officer is qualified to perform the required duties	Certifications and training records; prior employment and position history	Review the BSA Compliance Officer's employment background, position history, AML certifications and AML training to confirm they have the core qualifications to perform the required program duties
No appropriate segregation of duties between employees responsible for tuning models and those investigating the alerts	Segregation of duties	To ensure that there is a clear segregation of duties between employees tuning models and those investigating the resulting alerts	Organization chart Roles and responsibilities	Review the organization chart including the roles and responsibilities of employees involved in model tuning and alert investigation. Confirm that the reporting structure and duties are clearly separate from each other
Number of unusual transactions escalated are low while number of requests for information ("RFIs") are high	Escalation activity	To ensure that investigators are escalating all unusual transactions that require further investigation	Escalation and quality control logs	Review the quality control logs and determine if there are an abnormally high number of alerts that an employee did not recognize as suspicious Review the escalation log and determine if the employee has not escalation for further investigation the number of alerts similar to other investigative staff
Number of alerts that require re-work are excessive	Alert re-work	To ensure that the investigators assigned to clear alerts have the requisite knowledge and training	Number of alerts requiring re-work is less than the control level established	Compare the number of alerts that required re-work during the month to the average of all investigators or a control level set.
SARs are filed late	Late SAR filing	To ensure that once a case has been determined to be suspicious a SAR is filed within the allowed timeframe	SAR filing log	Review the SAR filing log and identify investigators who are late filing SARs. Determine if this is a pattern and if they require targeted training.

PERIODIC TRAINING OF ALL STAKEHOLDERS (§504.3(c)(8))

The failure to conduct periodic employee training on the BSA/AML and OFAC program will render the Program ineffective over the course of time. All employees should have an understanding of the institution's BSA/AML and OFAC requirements, while those employees whose duties include on-boarding customers and transacting business or who are responsible for various aspects of the BSA/AML and OFAC programs should have targeted training to ensure they receive updated guidance on evolving laws, regulations and best practices.

Training for both new employees and those with BSA/AML and OFAC experience at the institution should receive periodic targeted training, including training on related policies and procedures, current BSA/AML and OFAC laws and regulation and best practices within their specific areas of the anti-money laundering programs.

The training program should be supported by the collection and retention of training program records including employees who have received different types of training, when training occurred, content of training, training and testing materials and attendance records. Follow up after training should also be performed to ensure that the training was effective and that employees benefited from the training and are utilizing the knowledge gained.

An example of a simplified BSA/AML and OFAC audit testing program including the risks, controls and tests that can be performed to determine ***if the periodic training of all stakeholders for both the Transaction Monitoring and Filtering Program*** meets the regulatory requirements is illustrated in the table below:

PERIODIC TRAINING OF ALL STAKEHOLDERS (§504.3(c)(8))				
Risk	**Control Name**	**Control Objectives**	**Evidence of Control**	**Tests of Control**
All stakeholders have not received general BSA/AML and OFAC training	General training	To ensure that all employees have received basic information about the institution's BSA/AML and OFAC requirements	Training log	Review training log and compare the total number of employees who attended the general annual BSA/AML and OFAC training program to the number of employees on staff during that year
Applicable stakeholders did not receive targeted training	Targeted training	To ensure that employees in each of the areas of the Transaction Monitoring and Filter Program receive targeted training	Training log	Review training log and compare the total number of employees involved with Transaction Monitoring and Filter Program with the records of attendance for targeted training delivered during the year
Training records not maintained or not properly maintained	Training record keeping	To ensure that the institution maintains records of employee attendance for training	Training log	Review the training log and confirm that it is current and reflects attendance records for all employees attending each of the different types of Transaction Monitoring and Filter Program training taken each year

IDENTIFICATION OF REMEDIAL EFFORTS PLANNED AND/OR UNDERWAY (§504.3(d))

This subsection of the Rule prescribes that "to the extent that the institution has identified areas, systems, or processes that require material improvement, updating or redesign, the institution shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes."[xxxix] This documentation must be available to the Superintendent upon request.

The certifying officer must therefore identify any remedial efforts planned and/or underway however, *the format of the corrective actions response required to support this requirement was not described in the Rule*. Guidance can be obtained from Sarbanes Oxley, which requires that the certifying officer must disclose any corrective actions with regard to significant deficiencies and material weaknesses[xl]. In this regard, the corrective actions are those process and control improvements that management institutes in order to correct a significant deficiency or material weakness in the Transaction Monitoring or Filter Programs.

An example template for the ***corrective actions response*** is illustrated below:

Issue	Impact	Priority	Agreed Management Action Plan	Due Date	R-A-G
BSA/AML and OFAC Risk Assessments The Branch's Risk Assessment will be re-performed using a more detailed and granular risk assessment methodology to address the Part 504 requirements by the end of Q2 2017 and in response to the prior regulatory findings. During the review period the enhanced Branch BSA/AML and OFAC Risk Assessments were not completed or implemented. After a review of the proposed additions to the Risk Assessments it was noted that they do not fully address all of the Part 504 requirements. The Risk Assessment should also be updated with relevant quantitative data including year-over-year comparisons. ISSUE OWNER(S): Sally Johnson, Chief Compliance Officer	A key purpose of the BSA/AML and OFAC Risk Assessments is to identify controls to mitigate inherent risks, provide a view of the effectiveness of those controls and to drive improvements in the BSA/AML and OFAC risk management program through the identification of money laundering risks faced by the Branch – its customers, products and services, and geographies served. Without updated risk assessments that support and comply with Part 504 requirements, the Branch will not be properly identifying the risk profile and effectively delegating its resources to reasonably manage the Branch's overall BSA/AML and OFAC risks.	High	• Identification of Part 504 risk assessment requirements • Develop 'gap' between current risk assessments and requirements • Identify required changes to risk assessments and other linked programs • Remediate risk assessment methodologies and assessments • Remediate associated policy, procedures and processes • Communicate risk assessments to all Branch personnel • Establish training calendar and roster • Develop and deliver targeted training ACTION PLAN OWNER(S): Jeff Trumpet BSA Compliance Officer	Q2, 2017	GREEN

(§504.4) ANNUAL BOARD RESOLUTION OR SENIOR OFFICER COMPLIANCE FINDING

An annual Board resolution or Senior Officer Compliance finding is required by each Regulated Institution which attests to the best knowledge of its Board or Senior Officer that the institution is in compliance with the requirements of the Rule. The institution must determine if the Board of Directors will be required to adopt a certifying resolution to be submitted to the Supervisor or if a Senior Officer will be required to submit a finding that the Transaction Monitoring and Filtering Programs satisfies the requirements of the Rule. This requirement is fulfilled through the submission of an annual certification (Attachment A to Rule 504[xli]), which must be either signed by each member of the Board of Directors or a senior officer(s) and submitted to the Department of Financial Services on April 15th of each year beginning in 2018.

The certification by the Board of Directors or Senior Officer(s) requires that:[xlii]

- the Board of Directors or Senior Officer(s) "have reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals as necessary" to provide the certification;
- the Board of Directors or Senior Officer(s) have "taken all steps necessary to confirm" that the New York Regulated Institution has a Transaction Monitoring and Filtering Program that complies with the Program requirements; and
- to the best of the Board's or Senior Officer(s)' knowledge, the Transaction Monitoring and Filtering Program of the Regulated Institution for the prior calendar year complies with the Program requirements.

(§504.5) PENALTIES / ENFORCEMENT ACTIONS

Interestingly, the Rule does not specifically impose penalties for the failure to maintain an adequate transaction monitoring and filtering program, failure to file the annual certification or criminal penalty for filing an incorrect or false annual certification. However, it is likely that the NYDFS will continue to step up its enforcement actions and monetary penalties toward ensuring Regulated Institutions fully comply with the Rule.[xliii]

CONCLUSION

The NYDFS Part 504 Rule implements TWO significant challenges toward compliance program standards and governance of control deficiency issues related to the BSA/AML and OFAC program requirements that Regulated Institutions must adhere to beginning January 1, 2017.

First, the Rule creates stringent control standards through implementing prescriptive requirements and detailed attributes for the BSA/AML and OFAC transaction monitoring, filter program and related program elements such as transaction monitoring, OFAC sanctions filtering, governance, data, model validation, vendor selection, funding, use of qualified personnel and training.

Second, program testing is critical to document and detail that the institution is performing to the standards which is then required to be attested to on the annual certification. Without significant testing, senior management and the BSA Compliance, Officers cannot fully understand the gaps between their existing BSA/AML and OFAC programs and the new requirements to identify deficiencies and develop remediation action plans with ownership and target completion dates clearly spelled out. These remediation action plans then must be available, attested to and presented to the NYDFS, or the institutions face the risk of additional potential program violations, enforcement actions, and/or monetary penalties can be imposed strictly for failure to adequately govern and provide oversight and ownership of the BSA/AML Program and remediation efforts.

Part 504 essentially requires an institution to build, maintain, and test BSA/AML/OFAC control environments that comply with the NYDFS prescriptive standards that exceed the regulatory guidance provided by the FFIEC and OFAC. Furthermore, the Rule permits the NYDFS to levy fines, penalties, and/or actions against an institution for the inability of senior management to identify, address, and remediate any prescribed control deficiencies and further requires management to disclose and attest to these documented efforts to the DFS upon request.

While the Rule is specific to New York DFS Regulated Institutions, it is quite possible that other regulators in New York, such as the OCC, FDIC, FINRA, etc. may adopt these new certification requirements for their regulated institutions. Additionally, and depending upon the success of this new regulation, other states may adopt these or similar measures for their own respective regulated institutions.

REFERENCES

[i] Section 302 of the Sarbanes-Oxley Act, titled Corporate Responsibility for Financial Reports, requires: a) CEOs and CFOs must review all financial reports; b) financial reports must not contain any misrepresentations; c) information on financial reports must be "fairly presented"; d) CEOs and CFOs must be responsible for the internal accounting controls; e) CEOs and CFOs must report any deficiencies in internal accounting controls, or any fraud involving the management of the audit committee; and f) CEOs and CFOs must indicate any material changes in internal accounting controls. Sarbanes-Oxley Act §302, 15 U.S.C.A. § 7241 (West 2002).

[ii] *SEC Requires CEO and CFO Certification of Quarterly and Annual Reports*, Morrison Foerster (Sept. 4, 2002), https://www.mofo.com/resources/publications/sec-requires-ceo-and-cfo-certification-of-quarterly-and-annual-reports.html#.

[iii] "Maria T. Vullo was confirmed by the New York State Senate as Superintendent Financial Services on June 15, 2016." *Maria T. Vullo*, New York State Department of Financial Services, http://www.dfs.ny.gov/about/mvullo.htm (last visited Sept. 27, 2016).

[iv] NYDFS has identified "regulated institutions" to include "all Bank Regulated Institutions and all Nonbank Regulated Institutions." Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications, 3 N.Y.C.R.R §504, Dept. of Financial Services Superintendent Regulations, (June 30, 2016), *available at* http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp504t.pdf. "Bank regulated institutions" include "banks, trust companies, private bankers, savings banks, and savings and loan associations chartered pursuant to the New York Banking Law (the "Banking Law") and all branches and agencies of foreign banking corporations licensed pursuant to the Banking Law to conduct banking operations in New York." Id. "Nonbank regulated institutions" include "check cashers and money transmitters licensed pursuant to the Banking law." Id.

[v] Christopher L. Allen, Robert C. Azarow, David F. Freeman, Jr., Michael A. Mancusi, Brian C. McCormally & Kevin M. Toomey, *New York's New AML Rule: Strategic Considerations and Alternatives*, Arnold & Porter (July 11, 2016), http://www.arnoldporter.com/en/perspectives/publications/2016/07/new-yorks-new-aml-rule.

[vi] Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications, 3 N.Y.C.R.R §504.6.

[vii] Id. §504.4.

[viii] Id. §504.3

[ix] Id. §504, Attachment A.

[x] Steven Bragg, *What are Tests of Controls?*, Accounting Tools (April 16, 2014, 9:47 AM), http://www.accountingtools.com/questions-and-answers/what-are-tests-of-controls.html.

[xi] *Bank Secrecy Act Anti-Money Laundering Examination Manual*, Federal Financial Institutions Examination Council Bank Secrecy Act/ Anti-Money Laundering InfoBase 11 (2015), https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014_v2.pdf.

[xii] Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications, 3 N.Y.C.R.R §504.4.

[xiii] Id. §504.3(a)(1).

[xiv] Id. §504.3(a)(4).

[xv] "A predicate offense is a crime that is a component of a more serious criminal offence. For example, producing unlawful funds is the main offence and money laundering is the predicate offense." Robert Charles Lee, *What Is The Meaning Of 'Predicate' in the Following Sentence, 'Government Should Make Tax Evasion Of Rs. 50 Lakh and Above, a Predicate Offence?'*, Quora (Dec. 16, 2014), https://www.quora.com/What-is-the-meaning-of-predicate-in-the-following-sentence-Government-should-make-tax-evasion-of-Rs-50-lakh-and-above-a-predicate-offence.

[xvi] Charles Doyle, Cong. Research Serv., RL33315, Money Laundering: An Overview of 18 U.S.C. 1956 and Related Federal Criminal Law 2 (2012), *available at* https://www.fas.org/sgp/crs/misc/RL33315.pdf.

[xvii] Bragg, *supra*.

[xviii] Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications, 3 N.Y.C.R.R §504.3(a)(6).

[xix] ITSM refers to the "entirety of activities performed by an IT service provider to plan, deliver, operate and control IT services offered to customers. Note: the activities carried out in the ITSM context should be directed by policies and structured and organised by processes and supporting procedures." *Part 0: Overview and Vocabulary*, FitSM Standards for Lightweight IT Service Management 7 (Version 2.4, 2016), http://fitsm.itemo.org/sites/default/files/FitSM-0_Overview_and_vocabulary.pdf.

[xx] ITSM, IT Change Management Procedure, (last visited Sept. 29, 2016), http://www.itsmcommunity.org/downloads/Sample_Process_Guide_-_Change_Management.pdf

[xxi] *Protocol Definition*, Merriam-Webster, http://www.merriam-webster.com/dictionary/protocol

[xxii] *Supervisory Guidance on Model Risk Management*, Office of the Comptroller of the Currency, U.S. Dept. of Treasury 3 (April 4, 2011), https://occ.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf; *Guidance on Model Risk Management*, Board of Governors of the Federal Reserve System 2 (April 4, 2011), https://www.federalreserve.gov/bankinforeg/srletters/sr1107.pdf.

[xxiii] *Bank Secrecy Act Anti-Money Laundering Examination Manual*, *supra*, at F-1.

[xxiv] *Supervisory Guidance on Model Risk Management*, *supra*, at 3.

[xxv] Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications, 3 N.Y.C.R.R §504.3(b)(1).

[xxvi] Id.

[xxvii] Tara Johnston, *OFAC and the Role of the Three Lines of Defense*, Advancing Financial Crime Professionals Worldwide 7 (last visited Sept. 30, 2016), http://www.acams.org/wp-content/uploads/2015/08/OFAC-and-the-Role-of-the-Three-Lines-of-Defense-Tara-Johnston.pdf.

[xxviii] Lists include the Specially Designated Nationals and Blocked Persons list ("SDN List") at www.ustreas.gov/offices/enforcement/ofac/sdn and economic sanction and embargo programs that target geographic regions and governments at www.ustreas.gov/offices/enforcement/ofac/programs. Specially Designated Nationals List (SDN), U.S. Dept. of Treasury (Sept. 29, 2016), https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx; Sanctions Programs and Country Information, U.S. Dept. of Treasury (Sept. 29, 2016, 11:02 AM), https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx.

[xxix] Bragg, *supra*.

[xxx] *Supervisory Guidance on Model Risk Management*, Office of the Comptroller of the Currency, *supra*, at 3; *Guidance on Model Risk Management*, Board of Governors of the Federal Reserve System, *supra*, at 2.

[xxxi] *Supervisory Guidance on Model Risk Management*, Office of the Comptroller of the Currency, *supra*, at 3.

[xxxii] ITSM refers to the "entirety of activities performed by an IT service provider to plan, deliver, operate and control IT services offered to customers. Note: the activities carried out in the ITSM context should be directed by policies and structured and organised by processes and supporting procedures." *Part 0: Overview and Vocabulary*, FitSM Standards for Lightweight IT Service Management 7 (Version 2.4, 2016), http://fitsm.itemo.org/sites/default/files/FitSM-0_Overview_and_vocabulary.pdf.

[xxxiii] *Change Management Process Guide*, ITSM Community (Aug. 1, 2006), http://www.itsmcommunity.org/downloads/Sample_Process_Guide_-_Change_Management.pdf.

[xxxiv] "A system of record (SOR) or Source System of Record (SSoR) is a data management term for an information storage system (commonly implemented on a computer system) that is the

authoritative data source for a given data element or piece of information." *System of Record*, Wikipedia (last visited Sept. 29, 2016), https://en.wikipedia.org/wiki/System_of_record.

[xxxv] DAMA UK Working Group, *The Six Primary Dimensions for Data Quality Assessment* 8-13 (October, 2013), *available at* https://www.em360tech.com/wp-content/files_mf/1407250286DAMAUKDQDimensionsWhitePaperR37.pdf.

[xxxvi] *Data integrity*, Wikipedia (last visited Sept. 29, 2016), https://en.wikipedia.org/wiki/Data_integrity.

[xxxvii] Russell J. Bruemmer & Elijah M. Alper, *AML: A Corporate Governance Issue*, The Banking Law Journal, November/December 2013 867, 868, *available at* https://www.wilmerhale.com/uploadedFiles/WilmerHale_Shared_Content/Files/PDFs/bruemmer-alper-banking-law-journal.pdf.

[xxxviii] Kathe Dunne, *The Expanded Expectations of Corporate Governance in BSA/AML and the Impact on the Audit Function*, Advancing Financial Crime Professionals Worldwide 4 (March 2014), http://www.acams.org/wp-content/uploads/2015/08/The-Expanded-Expectations-of-Corporate-Governance-in-BSA-AML-and-the-Impact-on-the-A.pdf.

[xxxix] Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications, 3 N.Y.C.R.R §504.3(d).

[xl] Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, U.S. Securities and Exchange Commission (Aug. 14, 2003), *available at* https://www.sec.gov/rules/final/33-8238.htm.

[xli] Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications, 3 N.Y.C.R.R §504. Attachment A.

[xlii] *New York Banking Regulator Issues Anti-Money Laundering Rules for Transaction Monitoring and Filtering Programs*, Sidley (July 7, 2016), http://www.sidley.com/news/2016-07-07-banking-and-financial-services-update.

[xliii] Alistair Gray, *New York's Top Finance Regulator is No 'Clint Eastwood'*, Financial Times (June 22, 2016), https://www.ft.com/content/64a00f68-388b-11e6-9a05-82a9b15a8ee7.