Experis™
Finance

Model Validation and Risk Modeling

Carolinas Chapter ACAMS Learning Event

Presenters:

Shari Lembach, CAMS
Engagement Manager
Risk Advisory Services

Bill Pierce, CPA, CISA
Senior Manager - IT
Risk Advisory Services

Tuesday, April 21, 2015

ACAMS Carolinas Chapter

Agenda

- Introduction
- Customer Risk Modeling
- Guidance on Model Risk Management
- Independent Model Validation

Experis™ Finance

Risk Advisory
Finance and Accounting
Tax

Introduction and Capabilities

Business Operations	Information Technology	Risk Advisory	Finance and Accounting
Chief Operating Officer Line of Business Executive(s)	Chief Information Officer Chief Technology Officer	Chief Risk Officer Chief Compliance Officer Chief Credit Officer Chief Audit Executive	Chief Financial Officer
Business transformation Program/Project management Business and process analysis Post M&A/divestiture services Change management Communication management Business analytics Corporate performance management Systems conversions and upgrades Business resiliency Policy and procedure optimization Risk operations Operational support services	Project delivery Data analysis and mapping Systems architecture Data warehousing Development solutions System, network and database administration Data center management Business intelligence Infrastructure and data solutions ERP Global content lifecycle management Analytics and SAS Outsourced managed solutions	Internal audit strategic sourcing Regulatory compliance - Compliance program development - Regulatory exam support - Targeted file reviews Model Validation and Risk Modeling IT audit Information security Enterprise risk management Basel Credit risk assessment and mitigation Loan review Interest rate risk Operational risk assessment and mitigation Loss mitigation Fraud risk assessments	Financial statement preparation Regulatory report preparation Technical accounting support Account reconciliations Internal controls optimization Sarbanes-Oxley Act Tax compliance Charter consolidations Executive reporting Financial process improvement

Customer Risk Modeling

Customer Risk Modeling

- **Customer Risk Rating**
  - Purpose
    - To utilize in identifying customers who pose a higher risk
    - To perform BSA / AML enhanced due diligence based on level of risk
    - To better manage risk related to customers
    - To better align suspicious activity monitoring program with areas of higher risk
    - To monitor change in a customer relationship

Customer Risk Modeling (continued)

- **Initial Customer Risk Rating**
  - Define risk levels and criteria used to risk rate a customer.
    - Samples of criteria to include but are not limited to:
      - Method of account opening e.g. in person, online, mail, etc.
      - Type of customer i.e. consumer versus business
      - Type of product or service, i.e. savings, checking, loan, etc.
      - Geography of customer i.e. within the institution’s CRA area, is the customer in a HIDTA or HIFCA?
      - Length of relationship with institution
      - Occupation or business type (NAICS code), business types that can not be exempt from CRT reporting may be considered higher risk
      - Source of funds
      - Expected activity based on questions at account opening i.e. cash deposits/withdrawals, international transactions, wires, etc.
      - OFAC / Watch List Screening

Customer Risk Modeling (continued)

- **Enhanced Due Diligence**
  - Collection of additional customer information
  - Ongoing Customer Risk Rating and additional items to consider but not limited to:
    - Number of referrals for suspicious activity and number of SARs filed for customer. Law enforcement inquiries
    - If customer is an entity, are they eligible to conduct business within your state? Are they licensed and in good standing with the state, if applicable?
    - Compare actual activity to expected activity. Determine average dollar and number of transactions to identify transactions that appear out of the ordinary
    - Update expected activity
    - Assess risk based on transaction activity for example, volume of cash deposits compared to total deposits, volume of international wires versus all wire activity for the customer

Customer Risk Modeling (continued)

- **Enhanced Due Diligence** (continued)
  - Assess risk based on categories of customers (peer groups) such as Privately Owned ATM customers or industries (e.g. restaurants, grocery stores). This will aid in detecting a customer whose activity is significantly different than others in the same peer group. If using software and available, use peer groups for analytical comparison of transactions to identify customers who are out of the norm
  - Social media searches for negative news such as Google, Facebook, Twitter, LinkedIn
  - Onsite visit if deemed necessary
  - Internal sources may also have additional information such as front line or loan department
  - Know your Customer’s Customer i.e. what do you know about who your customer does business with. For example, customer wires funds to China to purchase supplies, does the Chinese company produce supplies needed?
  - Updated OFAC List Screening

Guidance on Model Risk Management

Supervisory Guidance on Model Risk Management

- Joint Guidance
  - OCC 2011-12 issued April 4, 2011
    - Board of Governors of the Federal Reserve System
    - Office of the Comptroller of the Currency
  - Purpose - To provide comprehensive guidance for banks on effective model risk management.
    - Rigorous model validation
    - Sound development, implementation, and use of models
    - Model risk management encompasses governance and control mechanisms
- Federal Housing Finance Agency
  - Advisory Bulletin AB 2013-07 – Model Risk Management Guidance

Regulatory Guidance

- Overview of Model Risk Management
  - Models by their nature are simplifications of reality and real world events may prove those simplifications inappropriate
  - The use of models invariably presents model risk, which is the potential for adverse consequences from decisions based on incorrect or misused model outputs and reports
  - Model Risk occurs for two basic reasons:
    - Errors in the assumptions, design, or use of the model produce inaccurate outputs
    - Model misapplied or misused
  - Model Risk should be considered and managed like any other type of risk
  - Managing model risk requires "effective challenge“

Regulatory Guidance

- Overview of Model Risk Management (continued)
  - Model Risk cannot be eliminated. Therefore it is necessary to use other tools to effectively manage model risk
    - Establishing limits on model use
    - Monitoring model performance
    - Adjusting and/or revising models over time
    - Supplementing model results with other analysis and information
  - A bank's Model Risk management framework should be more extensive where model outputs have a material impact on business decisions

Regulatory Guidance

- Model Development, Implementation, and Use
  - Model Development and Implementation
    - Model development must be aligned with the intended use. The design, theory, and logic, underlying the model should be well documented and supported by published research and sound industry practice
      - Smaller banks that rely on vendor models should choose models and variables appropriate to their size, scale, and lines of business
  - Testing
    - Testing must determine whether the model is performing as intended, including the model's accuracy, demonstrating that the model is robust and stable, assessing potential limitations, and evaluating the model's behavior over a range of input values
    - It should also assess the impact of assumptions and identify situations where the model performs poorly or becomes unreliable

Regulatory Guidance

- Model Development, Implementation, and Use (continued)
  - Model Use
    - During use, banks should assess model performance over time as conditions and model applications change
    - Reports that provide a range of estimates for different input-value scenarios and assumption values can give decision makers important indications of the model’s accuracy, robustness, and stability as well as information on model limitations
    - Banks should demonstrate an understanding of model uncertainty and inaccuracy and account for them appropriately. Accounting for model uncertainty can include judgmental conservative adjustments to model output, placing less emphasis on that model’s output, or ensuring that the model is only used when supplemented by other models or approaches
    - If data are not representative of the bank’s characteristics, especially external data related to new products or activities, these factors should be analyzed for potential limitations

Regulatory Guidance

- Model Validation
  - Model validation helps ensure models are sound. It also identifies potential limitations and assesses their possible impact
  - Validation should generally be performed by someone who does not have a stake in whether a model is determined to be valid
  - The guidance sets expectations for effective model validation:
    - Evaluation of conceptual soundness, including developmental evidence
      - This is challenging when using vendor products
      - Banks need appropriate vendor selection processes
    - Ongoing monitoring, including process verification, and benchmarking
      - Understand impact of changes in products, exposures, activities, clients, or market conditions on model performance
      - Verify that data inputs are complete and accurate
      - Analyze overrides (where model output is ignored or altered) for indications the model is not performing as intended. For AML systems, overrides are often the result of benchmarking

Regulatory Guidance

- Model Validation (continued)
  - Outcomes analysis, including back-testing
    - Compare model outputs to actual outcomes and assess the reasons for variances
      - May include statistical tests or other quantitative measures
      - Can also include expert judgment to confirm results make sense
      - For AML systems, review of alerts and the use of expert judgment on decisions to file Suspicious Activity Reports is on-going
        - False positives are constantly identified in daily reviews of alerts. Banks should challenge excessive variance in number of alerts versus SARs
        - Too few alerts are more difficult to identify and pose greater risk

Regulatory Guidance

- Governance, Policies, and Controls

  The extent and sophistication of the bank’s governance function is expected to align with the extent and sophistication of model usage

  - Board of Directors and Senior Management
    - Model Risk Management is generally delegated to senior management, but should include regular reporting to the board
  - Policies and Procedures
    - Should be commensurate with the bank’s relative complexity, business activities, corporate culture, and overall organizational structure
  - Roles and Responsibilities
    - Divided among ownership, controls, and compliance. Reporting lines and incentives should be clear, with conflicts of interest addressed
    - Model risk controls include risk measurement, limits, and monitoring
      - Model operation controls should include controls over input data and model access, parameters, and software

Regulatory Guidance

- Governance, Policies, and Controls (continued)
  - Internal Audit
    - A bank's internal audit function should assess the overall effectiveness of the model risk management framework to address the model risks of:
      - Errors in model assumptions or design
      - Misapplied or misused models
    - If some internal audit staff perform certain validation activities, they should not be involved in the overall model risk management assessment
  - External Resources
    - Banks may engage external resources to help execute certain activities related to model risk management
    - Activities could include model validation and review, compliance functions, or other activities in support of internal audit

Regulatory Guidance

- Governance, Policies, and Controls (continued)
  - Model Inventory
    - Banks should maintain a firm-wide inventory of all models
    - Guidelines for what the inventory should include:
      - Description of purpose and products for which the model is used
      - Any restrictions on use
      - Type and source of inputs
      - Output and their intended use
      - Date last updated
      - Date last validated

Regulatory Guidance

- Governance, Policies, and Controls (continued)
  - Documentation
    - Should be sufficiently detailed that those unfamiliar with the model can understand how it operates, limitations, and key assumptions
    - For vendor/third party models, banks should document information leading to the selection
    - Documentation provides for continuity of operations, makes compliance with policy transparent, and helps track recommendations, responses, and exceptions

Independent Model Validation

Experis - Conducting An AML Model Validation

	Evaluate Risks & Requirements	Establish Validation Scope	Execute Test Program Phase 1	Client Tuning of Model	Execute Test Program Phase 2	Communicate / Report Results
Objective	Assess and prioritize high risk components including business lines, operations, products/ services, locations, and customers.	Effectively allocate Internal Audit resources to key issues focusing resources on high-risk, strategic or rapidly emerging issues.	Test controls/processes established to mitigate high risk components to validate effectiveness.	Client reviews and implements recommendations.	Test controls/processes established to mitigate high risk components to validate effectiveness.	Detailed communication of key findings, addressing status of high-risk and strategic issues.
Key Activities	• Review strategic plans and objectives • Understand current business lines, channels, products and services offered • Interview key personnel to understand components of the Model utilized and identify potential gaps • Establish roles and accountabilities • Identify and evaluate Model performance relating to transaction monitoring, customer risk scoring and other components utilized	• Prioritize key components for testing • Review risk assessment and identify high risk customers, products/services, geographic locations to determine areas of focus • Review Audit Plan with Management based on Joint Model Risk Bulletin 2011-12 guidance • Establish communication plan	• Review AML and OFAC Risk Assessments and policies and procedures for Model processes • Review Model outcomes • Verify core system balances to Model data in total dollar amount by Tran code • Review Model rules/alerts/worklists for reasonableness and linkage to AML and OFAC Risk Assessments • Review Risk Scoring utilized within the Model • Test OFAC system utilized within the Model • Evaluate criteria used to establish rule/alert thresholds • Verify Model calculations are accurate	• Client reviews recommendations • Client reviews and determines appropriate thresholds for rules/alerts/worklists • Client creates action plan to implement management approved changes to the Model • Model changes implemented	• Review Model outcomes • Verify core system balances to Model data for a selected time period in total dollar amount by Tran code • Review Model rules/alerts/worklists for reasonableness and linkage to AML and OFAC Risk Assessments • Test OFAC system within the Model if applicable • Evaluate criteria used to establish rule/alert thresholds • Review Risk Scoring utilized within the Model • Verify Model calculations are accurate including Risk Scoring Module if applicable	• Draft report • Communicate results with Internal Audit or designated persons • Clarify audit findings • Review action plans and responses • Finalize report
Deliverables	• Audit Universe • Request list • List of potential gaps	• Detailed validation plan based on identified high risk areas and applicable regulatory components as outlined in the Statement of Work and documented in the Validation Program	• Workpapers • Status reporting • Observations and recommendations	• Client Internal Work papers • Client Internal Status Reporting • Client Internal Documentation of Model Changes	• Work papers • Status reporting • Observations and recommendations	• Audit findings • Draft report • Final report • Presentation to Audit Committee or the Board if requested

Tuning Your Model

Some basic steps, Experis typically recommends during our validation process, to ensure an effective AML BSA monitoring system.

Tuning your model:

- Core Balancing Reconciliation – Perform a daily reconciliation of the data transferred from the core to the monitoring system to identify any out of balance situations timely
- Transaction Code Mapping – Prepare a list of Transaction Codes with descriptions utilized by your core processing system; compare this list to the Transaction Code list utilized by your AML BSA monitoring system. Identify any discrepancies in descriptions or codes not mapped or specifically excluded from the monitoring system. If codes have been excluded, be sure to document management's reasoning regarding the exclusion
- Transaction Code Changes – Establish a documented approval process for changes or additions to Tran Codes which includes the AML BSA Officer to ensure changes are input into the monitoring software prior to going live
- Rules/Alerts/Worklists and Risk Scoring modules – Map your rules and risk scores to your AML BSA and OFAC Risk Assessments to verify assigned scores and rules agree with areas identified as higher risk within your risk assessments
- OFAC – Verify OFAC countries are included and properly risk scored, also review filtering criteria or "fuzzy logic" used to detect potential matches

Validating Your Model

- Independent Model Validation
  - Perform or obtain an independent model validation to validate the integrity of your data and that the model is operating as designed and intended by management
  - The joint guidance on model validation indicates that "Banks should conduct a periodic review—at least annually but more frequently if warranted—of each model to determine whether it is working as intended and if the existing validation activities are sufficient"
  - The validation needs to be independent and can be performed internally by a knowledgeable person or a third party
  - Further if have you upgraded your core systems; you most likely need to re-validate your transaction monitoring system

THANK YOU!

Shari Lembach
shari.lembach@experis.com
414-640-5024

Bill Pierce
william.pierce@experis.com
919-696-5067

Cyndi Duvall
cynthia.duvall@experis.com
301-452-8409

Experis™ Finance

Risk Advisory
Finance and Accounting
Tax