Institute of Internal Auditors
Risk based audit planning using data analytics
February 2016
Agenda

2015 financial services compliance testing survey
Data analytics in internal audit
Using data analytics for defining scope of audit plan
Discussion
2015 financial services compliance testing survey

Survey results
The survey focused on 2nd Line of Defense testing for compliance with U.S. banking regulations within their institutions. A total of 40 financial institutions responded to our survey, representing a broad cross-section of asset sizes ranging from $7 billion to more than $250 billion. Nearly 80% of the respondents are headquartered in the US, and 42% operate globally.

The responding institutions are engaged in a wide variety of products and services, including consumer banking (82% of respondents), commercial banking (75%), wealth management (61%), treasury/securities services (58%), asset management and capital markets (both 48%), and private and investment banking (52% and 36%, respectively).

The size of the respondents’ compliance testing organizations in terms of number of employees ranged from five to more than 200.
Key observations

Organization & Structure
The benefits of centralization and the regulatory focus on independence of the compliance testing function are broadly acknowledged.

Plans for Expansion
Advancing regulatory expectations are being met with increases in the number and quality of testing resources, and via efficiency gains through collaboration and automation.

Use of Co-sourcing
Leading banks are finding ways to overcome challenges around scarcity in technical and human resources, including use of service delivery centers and data analytics as accelerators.

People & Tools
Training and hiring are fundamental solutions, but have not been fully effective in closing the capabilities gap. Improvements in use of professional standards in testing and work paper practices can increase reliance by internal audit and regulators, enhancing both credibility and efficiency gains.
Key observations (continued)

3 Lines of Defence
- Strong collaboration among the testing functions minimizes redundancies and inefficiency.
- First line compliance control functions are of fundamental importance but are frequently lagging.

Annual Test Plan Development
- Regulators are looking for a well-thought out methodology.
- Good documentation of plan derivation and coverage are critical.
- Use of residual risk for testing prioritization should be based on confirmation that an effective control environment is present.

Test Plan Execution
- Testing of controls provides deeper insight into deficiencies and facilitates root cause analysis
- Regulators continue to look for transaction testing, but its extent and balance remains a gray area
- QA is often in place, but without professional standards as a basis.

Information Technology
- Capabilities and investment in information technology are often insufficient to drive innovation and effective implementation.
While there is consensus around the criticality of intelligent data use, banks are not keeping pace with technology innovations. Even where financial institutions are deploying data analytics, capabilities tend to be at a lower maturity level.

In the absence of clear regulatory guidance, sampling methodology remains a gray area. Regulatory criticism around insufficient sample sizes continues to be a pain point. A well-documented methodology and consistent approach in sampling is critical.

Some organizations have tried thematic reporting to escalate accountability, to better address root causes and improve coordination in remediation activities; however, individual process-level deficiencies can remain unaddressed. Some organizations continue to report only individual exceptions, without root cause analysis or recommendations. Use of key metrics is often lacking.
Data analytics in internal audit
Analytics enabled IA methodology

Analytics-Enabled Internal Audit Methodology

Data Enabled Risk Assessments

Analytics Driven Audit Scoping

Intelligent Sampling and Modeling

Analytics Governance and Methodology
When fully integrated, the data analytics initiative is not a separate workstream; rather, the techniques are fully embedded into all elements of the audit lifecycle.

Deliver solutions.. not problems
Sample of an ideal IA analytics setup

**Methodology**
- Ongoing (e.g., quarterly) data-enabled risk assessment
- 70% of audits using repeatable analytics during planning
- Obtaining coverage of lower risk areas through ongoing monitoring as opposed to physical auditing
- Interactive audit reports
- Fully developed policies and procedures for analytics embedded in each audit area or phase

**People**
- Core team of analytics professionals supported by power users in the IA department
- Defined training curriculum for entire IA department, focused on analytic mindsets and problem solving
- Formalized job descriptions, roles, responsibilities and recruiting
- Established analytics career path

**Technology**
- Library of re-useable analytics material across processes and units
- Audits and auditable units supported by dashboards displaying results of transactional data testing
- Continued access to timely and reliable data as needed, with connection to data tailored to existing ERP or source system
- Coordination and SLAs with IT as necessary
- Capabilities to perform lookback, visual and predictive analytics
- Approach for maintaining awareness of emerging technologies and applications to the audit process
Using data analytics for defining scope of audit plan

Assessment steps
Overview

Assessment Steps

1. Define Each Auditable Unit
2. Determine KPI's and Set Thresholds
3. Determine KRI's and Set Thresholds
Defining each auditable unit

Auditable units are parts of the organization that are exposed to risk.

Examples:

- Various retail stores within a company
- Product promotion effectiveness

An organization is broken up into auditable units in order to identify and target risks.

- They can be broken up in a number of ways, such as function, organizational unit, or project.
Determining KPIs and setting threshold

- A **Key Performance Indicator** (KPI) is used to evaluate the success of an organization based on the activity which it engages. Typically, a KPI is a repeatable, numerical measurement.
- Examples of KPI include; average price per transaction in the retail industry or occupancy rate for hospitality industry or unemployment rate for the government.
- We can determine KPIs by answering the question, ‘What is an important measure to stakeholders that shows them that progress is being made towards achieving their objectives and goals?’
  - KPIs can be tied to an organization’s strategy.
  - Should be a small set of variables to show how the process is performing.
  - Typically, KPIs are used to set a value on difficult-to-measure activities.
Determining KRI and setting threshold

- A Key Risk Indicator (‘KRI’) is anything with the possibility of an adverse impact. These quantitative indicators help to provide warnings and indicate an activity’s level of risk that may impact the risk management process.

- Examples of KRI include, excessive employee turnover at a hotel location, excessive returns at a retail store, or unpatched computers in a particular department.

- A KRI can also be linked to multiple risks already seen by the organization.
  - KRI need to be quantifiable and the data must be available.
  - Determine thresholds and triggers.
    - All stakeholders must agree on the threshold.
Using data analytics for defining scope of audit plan

Embedding analytics
Analytics in risk assessment steps

• Analytics can help in each step of Risk Assessment
• Data can be used to determine auditable units if they are not already apparent. These could cost structures, common product types, geographical units etc.
• Data can also help with identifying KPI’s that are in alignment with organizational objectives
• It can assist in developing metrics that can help in identifying risks before they become issues
• KRIs can also be better designed and monitored
Analytics in risk assessment – Demo

• Analytics assist in determining areas to be focused during an audit
• They can help in either determining functions to be audited or identifying units that need to be audited
• For example, using analytics one can determine that controls on the AP process are working as needed and that the AP process need not be audited in the current cycle
• Another example is using analytics to determine risks for all locations of a retailer or hotel chain. This can then be used to determine the frequency for auditing and in speeding up the audit process
Demo – Example of how we can use data analytics to determine scope of an audit

IA Analytics Video - Beyond Fieldwork - September 2015 (Basic_Small - WEB_MBL (H264_400)).mp4
Using data analytics for defining scope of audit plan

Key advantages
Aligning audit resources to risk

- Analytics in the risk assessment process allow audits to be driven by the intersection of risk and your audit mandate.
- Analytics provide coverage for common or lower risk areas which allows you to shift audit hours to more targeted or emerging risk areas.
- Site or location audits are performed based on risk indicators as opposed to on a rotational or ad hoc basis, allowing you to align your audit resources with your organization risks.

Perform audit scoping based on risk, not based on historical workprograms.

Use the data to understand the why and the how behind the what.

Use the data to dictate the areas that require additional auditing.
Risk based scoping

- Audits driven by the intersection of risk and your audit mandate
- Analytics provide coverage for common risk areas to shift audit hours to more targeted or emerging risk areas
- Site or location audits are performed based on risk indicators as opposed to on a rotational or ad hoc basis

Use the data to dictate the areas that require additional auditing.
**Risk based scoping** (continued)

<table>
<thead>
<tr>
<th>Audit, Risk, and Compliance</th>
<th>Business Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Are my Agents currently providing the level of service that matches their licensure?</td>
<td>• Are there any outliers in Mortgage Lending that may be receiving policy benefits outside of the normal parameters?</td>
</tr>
<tr>
<td>• What SOX controls are most consistently being checked by Ext Audit and how effective is the change management?</td>
<td>• What Mergers and Acquisitions should be monitored at a detailed level?</td>
</tr>
<tr>
<td>• Who are the top earners in commissions?</td>
<td>• What are the critical bottlenecks within the supply chain?</td>
</tr>
<tr>
<td>• What safety measures are in place to prevent IP leakage?</td>
<td>• Who are my most important customers?</td>
</tr>
</tbody>
</table>

**Operational**

- How can I ensure the quality of data and the accuracy of my transaction monitoring for AML?
- What regional tax laws may leave us with the most exposure?
- Who are our top spending units by region/product/division?

**Financial**

- Who are my top commissions earners?
- What areas are giving us sustainable margin growth and what attributes can be replicated?
- How effectively are we managing revenue streams and backlog?
- How effectively are Marketing dollars being spent?
- What are my key conversion and upsell metrics within the sales org?
Discussion...