

AML and Control Self-Assessment

6th CLADIT Conferencia
Ciudad de Guatemala
8 de Mayo, 2009

Efficiency gains –

According to a KPMG survey conducted last year -

- AML budgets realized a 58% growth over the past 3 years.
- Continue to grow, but at a decreasing rate
- With increase **regulatory focus**, this appears to be very optimistic
- Unless we become much more efficient, the resources required to adequately address AML may become prohibitive to the business

AML Process

The core monitoring process that includes:

- Customer Due Diligence
- Transactional behavior monitoring
- Systematic alert generation
- Detailed alert analysis
- Comprehensive investigations
- Suspicious Activity Reports decision making process
- SAR analysis including:
 - Categorization of existing typologies AND
 - Identification of new typologies

We tie it all together and ensure the pieces of the puzzle are working properly through our Control Self Assessment program.

What is Control Self-Assessment?

- ◆ A Process* to Let Management Know Timely When Things are Going Wrong.
- ◆ An Ongoing Process to Ensure Controls are Adequate and Working Properly.
- ◆ A Mechanism to Record and Monitor Issues and the Status of Corrective Actions.

* - Formal, Documented, Visible, Tested, Reported

Objectives of Control Self-Assessment

- ◆ **The objectives of the program include:**
 - Proactive management of risk
 - Problem identification and correction
 - Facilitate other control initiatives (e.g., FDICIA)
 - Broad awareness of risk and control
 - Upward communication to senior management:
 - Significant Risks and Control Issues
 - Corrective Action Plans

5 BASIC ELEMENTS OF CSA

1 IDENTIFY & ASSESS RISKS

Identify and document all significant control risks throughout the entire business. (Not limited just to financial controls and disclosure controls)

2 CONTROL MECHANISMS

Formulate, implement and document all significant control policies, procedures and mechanisms which are intended to prevent, mitigate or detect the occurrences of control breakdowns.

3 SELF-ASSESS/SELF-RATE

Self-assess/self-rate the controls based on formal and documented review of the controls in place on a quarterly basis, including required periodic self-testing (at a frequency commensurate with the underlying risk), to determine the efficacy of the controls in place - and to ensure that the policies, procedures and mechanisms continue to function as intended.

4 CORRECTIVE ACTION PLANS

When control breakdowns or deficiencies are detected, corrective action plans are required to be formulated with remediation tracked to completion. The corrective action plans should include description of the control, the deficiency, and required corrective action to correct the deficiency, a target date for completion and the responsible officer.

5 PERIODIC REPORTING

Periodic reporting to succeeding levels of management regarding status of controls, control deficiencies and breakdowns as well as businesses self-rated less than satisfactory. In addition, business reviews should include coverage of the status of self-assessments and control issues.

Independent Monitoring Unit

- ◆ Ensure Efficient/ Effective Program Implementation
- ◆ Review CSA Programs for Continuing Effectiveness
- ◆ Summarize CSA Results for the Business
- ◆ Monitor Compliance with CSA Program Requirements and Quality of CSA Testing by Departments
- ◆ Report Results to Local Management, Group Management, Applicable Function Heads, and Financial Control
- ◆ Track Issues and Related Corrective Actions
- ◆ Perform Periodic Validations
- ◆ Conduct Training; Provide Consulting Support

Perform a Detailed Review at the Unit Level

Identify and document for each functional area:

- ◆ all significant processes
 - understand the relationships among all cross-functional processes
- ◆ evaluate risks (inherent/specific) in each process
- ◆ assess controls used to manage/ mitigate risks*
- ◆ evidence of control operations
- ◆ action plans to correct weaknesses

* - Control concerns can be identified before any testing is performed.

Developing the Self-Assessment Test Program

Step One – Identify the risks

Step Two - Assess Controls

Step Three - Determine appropriate method of testing

Step Four - Define population and minimum sample size.

Step Five - Determine frequency of testing.

The method of testing you will perform is determined on the **strength** of the control and the **reliance** that can be placed on the control.

- Compliance Tests
- Substantive Tests

Tools

- ◆ Peer Group Materials (Better to Borrow than to Reinvent)*
- ◆ ‘Standard Audit Programs’
- ◆ Citi/Industry Guidance
 - Departmental Control Function Checklists
 - Risk Assessment Matrices
 - AICPA, Institute of Internal Auditors
 - Regulatory Compliance Service
- ◆ Cross-Functional Process Mapping

Process Vs. Control

What is the difference between a process and a control?

- ◆ A ***process*** is the method or tasks performed to achieve an objective. It is how a transaction is completed. For example, data is input into the system and a report is generated.
- ◆ A ***control*** is a mechanism to ensure the objective or process is achieved. For example, review of data input by a person independent of input.
- ◆ The presence of an individual or MIS is not a control. Controls are always *action or reaction* oriented.

There Are Different Kinds of Controls

Preventive Vs. Detective

The definition of a preventive control and a detective control normally depends on the placement of the control within the process, regardless of the actions being completed.

- ◆ **Preventive Control** - Usually there to prevent an error or exception from occurring (e.g., system edit checks or password procedures to restrict access, etc.).
- ◆ **Detective Control** - Usually there to detect an error or exception after it has occurred (e.g., Quality Control review process, reconciliation process, monitoring of key performance indicators, etc.).

Determining which type of control is critical in developing solid test programs.

Identification of Controls

(Key Items to Consider)

- **COMPLETE** - How do you ensure that all the transactions were processed?
- **ACCURATE** - How do you ensure that all transactions were processed accurately?
- **TIMELY** - How do you ensure that all transactions were processed within the established time standards?
- **AUTHORIZED** - How do you ensure that all transactions were appropriately authorized?
- **SECURED** - How do you prevent unauthorized use of checks or access to customer information?
- **COMPLIANCE** - How do you ensure compliance with the applicable laws, regulations, accounting and corporate policies?

Answers to these questions generally result in the identification of the control .

What Method of Testing Should I Use?

- ◆ **Compliance tests**
 - Strong controls
- ◆ **Substantive tests**
 - Weak or non-existent controls
- ◆ **Combination of Compliance and Substantive Tests**
 - Moderate or new controls
 - Failed controls
 - Changing environment
 - To gain or reinforce confidence in the controls
 - Significantly high level of risk with the process

Compliance Testing

(Does the Control Work?)

- ◆ Tests the existing preventive and detective controls to determine if they operate effectively.
- ◆ The three techniques for performing compliance testing are:
 - **OBSERVATION** is appropriate only when the controls do not leave an audit trail or documentary evidence, e.g. control over counting and examining physical assets.
 - **INTERVIEWING** the control person to determine his understanding of what and why controls are performed and the nature and follow up of exceptions.
 - **EXAMINATION** of documentation certifies the controls are operating throughout the period. This is the predominant technique that should be used in developing compliance testing for CSA.

Substantive Testing

(Reenacting the Process)

- ◆ Substantive testing verifies the accuracy of transactions, processes and account balances, i.e., the “end products” of the process. Substantive tests include analytical reviews and test details of transactions and account balances.

Types of substantive tests:

- Review of detail for unusual items
- Recompilation and test of clerical accuracy
- Inspection of critical forms and documents
- Third party confirmation
- Observation of assets
- Cutoff or timing tests
- Analysis of accounts
- Account reconciliation

Compliance Vs. Substantive

- ◆ **Compliance (If controls are strong)**

- Verify account reconciliation balances and review for management signoffs.
- Review exception report to ensure all outstanding items were researched and cleared.
- Validate check request & review for appropriate management signoff on journal wire transfers.

- ◆ **Substantive (If controls are weak)**

- Perform reconciliation to ensure account was reconciled accurately.
- Re-research items on an exception report to validate research was completed properly.
- Review of detailed back up to ensure check requests, etc., are valid.

Sample Size

- ◆ The size of the sample should be based upon the following characteristics:
 - Reliance on existing controls
 - Level of risk associated with the process
 - Minimum sample size should be
 - 20 - 30 items for populations greater than 1,000**
 - 15 or 10% whichever is lower for populations less than 1,000**
 - Sample size may need to be expanded based upon the evaluation of errors
 - JUDGMENT!
- ◆ Document your rationale for the sample size and selection criteria

Documentation of Testing

- ◆ Perform Testing as outlined in the test program
- ◆ Document Testing
 - Document the population covered
 - Determination and rationale of sample
 - Record results *
 - Maintain documentation *

* Sufficient documentation to recreate the testing.

Analysis of Results of Testing

- ◆ Once the test work is completed, it is important to analyze the results where errors are detected to determine the appropriate course of action to take. The first step is to determine “What caused the error?” To adequately answer this question, research is required to determine the root cause.
- ◆ Symptoms vs. Diseases
- ◆ Results can be classified into three categories:
 - Systemic Problem
 - Isolated Incident
 - Indeterminable - Sample size and scope should be increased, consider using judgmental sampling techniques (e.g., look other transactions handled by the same employee responsible for the errors found).

Performance Requirements

- ◆ The CSA should be performed by an individual:
 - independent of the control or transactions being tested.
 - reasonably knowledgeable about the process being performed.
 - in a lead or supervisory capacity.
- ◆ Testing frequency is based on risk level. Controls associated with:
 - high risks are tested quarterly.
 - medium risks are tested semi-annually.
 - low risks are tested annually.

RCSA System

