The Idola Report

Volume 2, Issue 1 May 2010

Information to Vision

Excellence, reliability, and value are core principles followed by Idola while working with its clients and partners. This newsletter provides current information to help financial institutions meet their risk and compliance mandates. It is with current, meaningful information that appropriate vision is developed to meet today's challenges.

To subscribe, add a colleague, or to opt out of the Idola Report, simply send an email request to: newsletter@idolainfotech.com.

Featured Article

Migration of Compliance Systems

FINCEN advisory

The Financial Crimes Enforcement Network (FinCEN) has recently issued an advisory to inform and assist the financial industry in reporting suspected instances of trade-based money laundering. This advisory contains examples of "red flags" based on activity observed in Suspicious Activity Reports (SARs) that may indicate trade-based money laundering.

For further information, click on:
http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2010-a001.pdf

FDIC Nov 2009 – Feb 2010 – Enforcement Action

The FDIC processed a total of 64 matters in February. These included 36 cease and desist consent orders; three removal and prohibition orders; thirteen civil money penalties; five prompt corrective actions; six orders terminating an order to cease and desist; and one notice of intention to prohibit from further participation, notice of assessment of civil money penalties, findings of fact, conclusions of law, order to pay and notice of hearing.

The FDIC processed a total of 67 matters in January. These included 35 cease and desist consent orders; ten removal and prohibition orders; sixteen civil money penalties; one Section 19 orders; one modification of order to cease and desist; and four orders terminating an order to cease and desist.

The FDIC processed a total of 57 matters in December. These included 27 cease and desist consent orders; one temporary cease and desist consent order; seven removal and prohibition orders; seven civil money penalties; three prompt corrective action directives; one voluntary termination of insurance; two Section 19 orders; one modification of order to cease and desist; six orders terminating an order to cease and desist; and two notices of charges and of hearing.

The FDIC processed a total of 51 matters in November. These included 34 cease and desist consent orders; nine civil money penalties; three prompt corrective action directives; three Section 19 orders; one order terminating an order to cease and desist; and one notice of charges and of hearing.

For more details, please click on:
http://www.fdic.gov/news/news/press/2010/pr10065.html (Feb 2010)
http://www.fdic.gov/news/news/press/2010/pr10039.html (Jan 2010)
http://www.fdic.gov/news/news/press/2010/pr10020.html (Dec 2009)
http://www.fdic.gov/news/news/press/2009/pr09241.html (Nov 2009)

FINRA Guidance on Blogs and Social Networking Sites

In September 2009, FINRA organized a Social Networking Task Force composed of FINRA staff and industry representatives to discuss how firms and their registered representatives could use social media sites for legitimate business purposes in a manner that ensures investor protection. Based on input from the Task Force and others, and further staff consideration of these issues, FINRA has issued - Regulatory Notice 10-06 to guide firms on applying the communications rules to social media sites, such as blogs and social networking sites.

For more details, please click on:
http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p120779.pdf

Interagency Policy Statement on Funding and Liquidity Risk Management

The OCC, FRB, FDIC, OTS, and NCUA in conjunction with the Conference of State Bank Supervisors (CSBS), are adopting Interagency Policy Statement on Funding and Liquidity Risk Management. The policy statement summarizes the principles of sound liquidity risk management that the agencies have issued in the past and supplements them and harmonizes with the "Principles for Sound Liquidity Risk Management and Supervision" issued by the Basel Committee on Banking Supervision (BCBS) in September 2008

For more details, please click on:
http://www.fdic.gov/news/news/press/2010/pr10055a.pdf

The FFIEC releases the revised Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual

On April 29, 2010 The Federal Financial Institutions Examination Council (FFIEC) released the revised *Bank Secrecy Act/Anti-Money Laundering (BSA/AML)* Examination Manual. The revised manual reflects the ongoing commitment of the federal and state banking agencies to provide current and consistent guidance on risk-based policies, procedures, and processes for banking organizations to comply with the BSA and safeguard operations from money laundering and terrorist financing.

For more details, please click on:
http://www.fincen.gov/news_room/nr/pdf/20100429.pdf
http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf

Consumer Compliance under the E-Sign Act

As e-banking becomes increasingly more popular, it is important for financial institutions to become familiar with the requirements of the E-Sign Act. An article in the Consumer Compliance Outlook for the fourth quarter of 2009 (from the Federal Reserve Bank of Philadelphia) provides an overview of the E-Sign Act's general compliance requirements

Please read details below:
http://www.philadelphiafed.org/bank-resources/publications/consumer-compliance-outlook/2009/fourth-quarter/q4_02.cfm

FINRA fines for Inadequate AML Program

On 2nd February 2010, The Financial Industry Regulatory Authority (FINRA) announced that it has fined Pension Financial Services, a Dallas-based securities clearing firm, $450,000 for failing to establish and implement an adequate anti-money laundering (AML) program to detect and trigger reporting of suspicious transactions, as required by the Bank Secrecy Act and FINRA rules and other violations.

In a similar matter, FINRA has censured and fined Pinnacle Capital Markets of Raleigh, NC, $300,000 for failing to implement AML procedures reasonably designed to detect and cause the reporting of suspicious activity as well as to verify the identity of customers.

For more details, please click on:
http://www.finra.org/Newsroom/NewsReleases/2010/P120859

Wachovia Settles Money-Laundering Case

Wachovia Bank reached a $160 million settlement with the Justice Department over allegations that a failure in bank controls enabled drug traffickers to launder drug money by transferring money from Mexican currency-exchange houses to the bank.

For more details, please click on:
http://online.wsj.com/article/SB10001424052748704059004575128062835484290.html

Migration of Compliance Systems

By Gokul Kallambunathil CAMS, Managing Partner at Idola Infotech, LLC

"Change is inevitable. Change is constant" - Benjamin Disraeli.

Financial institutions adapt to change with varying degrees of reluctance, especially when it comes to automated compliance systems. This article discusses the top reasons that are driving change in the compliance space today, factors to consider when selecting a new system and best practices to apply during the process of migration.

Reasons for Migration

Business Drivers

Shifts in industry trends: Shifts in industry trends force existing providers to make significant changes to their legacy systems or lose out to new products that are better designed from the ground up. For example, the convergence of AML, Fraud and Risk require systems that can cater to the wider scope as well as provide the ability for personnel with the diverse skill sets to collaborate on a unified platform with a seamless workflow.

Mergers/acquisitions: Mergers and acquisitions lead to major operational changes in financial institutions, including making decisions on which systems have to be kept and which need to be phased out.

Business Growth: As an institution's business grows, so does the need for more sophisticated systems with better detection technology, enhanced workflow, audit trails, security etc. There is also an increased awareness and reputational pressure to keep up with the best practices in the market. Newer business lines and expansion to new jurisdictions may also create the need for change if the existing system is not suited to the change in requirements.

Product Limitations: Over time, product limitations and ability of the product vendor to keep up with changing requirements may force an institution to look for alternatives. Some of the limitations that may be encountered are

- Inability to keep up with the latest regulatory requirements in a timely manner
- Inability to keep up with changes in industry standards (example SWIFT, International ACH)
- Inability to interface with different external systems (Core banking, payment systems etc)
- Inability to expand the system for better detection (New AML typologies, red flags, new fraud schemes)
- Inability to use market data from third party sources (for KYC, Watch lists, Risk ratings etc)
- Inability to cater to Multinational / Multilingual / Globalization / Localization requirements
- Poor product support
- Lack of product vision

Global Standards: As AML regulations mature across the globe and catch up with US and European standards, many international banks have or are moving towards a global standard. Products have also matured to handle the specific nuances and reporting requirements of different jurisdictions. This results in the Head Office systems and standards being moved into all international branches replacing the different systems they may be using.

SaaS: With the Software as a Service model evolving rapidly and many institutions are using it for their day to day functions, some organizations are inclined to adopt a SaaS approach for compliance to reduce overall costs in the long term and overcome the maintenance headaches of an on-premise solution.

Outsourcing: Though Compliance Process Outsourcing has not caught on in a big way, there is a slow trend and definite interest in this area. While institutions can outsource the job but not their responsibility, doing so will involve a substantial change in how the compliance function is handled.

Cost Reduction: There are several situations in which a change in systems may be undertaken just to reduce costs. Some of the scenarios that may prompt this are

- Elimination of multiple systems used by different branches or business units and standardization on a single platform and enterprise licensing.
- Some core banking solution providers offer compliance products bundled with their software at substantially lower price than independent compliance products. While many of these products may not be as mature or sophisticated as solutions provided by companies focused on developing compliance solutions, they may meet the organization's current and anticipated requirements. Some Core banking solution providers have acquired or developed partnerships to provide better solutions at a lower cost.

Audit Issues: Audit issues that cannot be remediated using the current solution or specific observations /criticism of the inadequacy of the monitoring system would prompt a change.

Technology Drivers

In some cases the need to migrate to a different system may be a result of technology considerations, some of which are:

Obsolete Technology: Older systems that use obsolete technology for watch list screening and suspicious activity detection may need to be replaced as more efficient and competitive products enter the market and are adopted by industry peers.

Scalability: With the growth in business volume and the amount of archived data, system performance may be affected. If the systems are not designed using a scalable architecture or uses underlying products (like the database engine) that are not highly scalable, there may not be an option but to migrate to a different system.

Enterprise Standards: The technology that is used by the product may not meet the current Enterprise standards such as

- Single sign-on
- Application Security
    - Access limits and granularity
    - Workflow/Approval requirements
- Data Security
    - Customer Data and Privacy
- Performance and SLAs
- Internal IT Support capability
- Availability of support for underlying products (database engine, Java or .Net framework, reporting engine etc)
- Disaster recovery and replication / warm standby requirements.

New System Considerations

Migrations are generally expensive and a proper evaluation of the available options needs to be made before embarking on a migration effort. Some of the major considerations are:

Feature Set: Evaluate the feature set of the products and ensure that they meet the current and anticipated needs of the institution. Without being limited by what was or was not available in the old system, define an ideal solution and look for a system that best suits the requirements.

Scalability: Ensure that the new system will be scalable based on anticipated growth in business volume and archived data. Request the vendors to provide performance benchmarks. This will also be useful for capacity planning.

Standards: The system should preferably use open standards so you can integrate easily with other enterprise solutions like workflow, document management, case management and popular third party market data providers.

Workflow: Ensure that the system has a robust workflow engine that can be customized based on the organization's policy.

Documentation: Verify that the system provides detailed documentation including user manual, online help and also supporting documentation for fine-tuning the system algorithms and rules.

Custom Solution: Custom solutions are very expensive to build and maintain in-house and are not feasible for most organizations. However, large institutions do develop custom solutions to meet the unique business needs and reduce dependency on vendors.

Data Archival: Evaluate if the new system will be able to archive the data from the current system for future use and reference. Transactional data archives will be useful to establish baselines for customer monitoring. Past cases will be required for reference as well as during review of new cases.

Staffing: Ensure that staffing levels are available for the migration. The migration project will require substantial effort from decision makers, IT staff and Compliance personnel to install implement and test the new solution.

Training: Evaluate training needs for staff to be optimally productive on the new solution.

Downtime: Factor in the downtime that would be required for the actual cutover.

Cost: Calculate the total cost of migration taking into consideration all aspects including

- License, maintenance, data subscriptions, third party product licenses
- Communication or bandwidth requirements (SaaS or ASP model)
- Training
- Customization
- Implementation
- Resources involved in the migration effort
- Hardware and other overheads

Retiring the old system: If all the data from the old system is not being migrated to the new system, evaluate the need to have continued access to the old system, even if with limited capability. Consideration should be given to archival, availability, access restrictions and ongoing support.

Migration Process

To ensure the success of a migration project, it is essential to define a strategy and manage the entire process

Planning: As with any critical project, detailed planning of the migration effort is essential for success. Planning should take into consideration all aspects of the project including the resources, timelines and infrastructure requirements.

Resources: It is critical to the success of the migration to involve a pool of expert level resources with knowledge of each system as well as the business.

Data Migration: Determine what data needs to be migrated. It is not always necessary or feasible to convert all existing data from the old system. The determinations should be based on process and workflow requirements of the business as well as the archival policy. Continued availability of the old system in a read-only or archive mode also determines what data is migrated.

Policies and Procedures: As part of the migration process, evaluate how the current policies will be affected. Update or rewrite procedures to reflect the new workflow and system capabilities. Also define how old system will be accessed when the need arises.

Business Continuity Planning /Disaster Recovery (BCP/DR) strategy: The new system may require a major change in the BCP/DR strategy. Ensure that this is part of the plan and is implemented along with the migration project. The new system may provide better capabilities for DR.

Conclusion

Change should be embraced as an integral part of continuous improvement. Migration to a new compliance system should be considered as a great opportunity to review and improve workflow processes, streamline operations, align with industry best practices, and strengthen the overall monitoring program.

There is no substitute for diligent planning, controlling and execution of a migration project which needs to factor in the various considerations as discussed in this article, to ensure success and derive the maximum mileage from the new system.

Share Your Knowledge

Knowledge sharing among peers is an essential service that helps us all navigate through our responsibilities in our risk and compliance professions. The Idola Report is dedicated to facilitating this valuable service. If you have information that you believe should be shared with other subscribers of the Idola Report or would like to submit an article for publication, please contact RamaSubbaRao Pappu at the address below.

About Idola

Idola Infotech was founded in 2002 by a team that specialized in software product development and the deployment of complex technology projects. Its management team consists of banking experts, leaders of the regulatory compliance market, and senior technology specialists. They have developed commercial products for one of the largest vendors of financial services software. Project management experience has been earned across a wide range of financial institutions from some of the largest in the world to small community banks. Idola has implemented and deployed software solutions domestically and internationally earning its reputation for ***excellence, reliability, and value.***

Idola News

Idola is pleased to announce that it's Managing Partner, Gokul Kallambunathil, was recently re-certified with his CAMS designation, for demonstrating continued competence, knowledge, ethics, study and experience of anti-money laundering.

Careers at Idola

Idola is looking for individuals who possess the drive and determination to succeed and be part of a growing and dynamic team. Please click on the link below for current job openings.

http://www.idolainfotech.com/careers.php

Products and Services

- Regulatory Compliance Consulting
- Independent Review of AML Compliance
- Compliance Process Outsourcing
- Financial Services Vendor Support
- Technology Services for Financial Institutions
- Data Research and Aggregation
- SWIFT Support Services and SWIFT Message Director
- Aegis – an OFAC solution for International ACH Transactions (IAT)

Contact

For further information contact:
RamaSubbaRao Pappu
Idola Infotech, LLC
120 Wood Avenue South, Suite 407
Iselin, NJ 08830
Tel: 908-397-3095
Email: ramapappu@idolainfotech.com
Web: www.idolainfotech.com