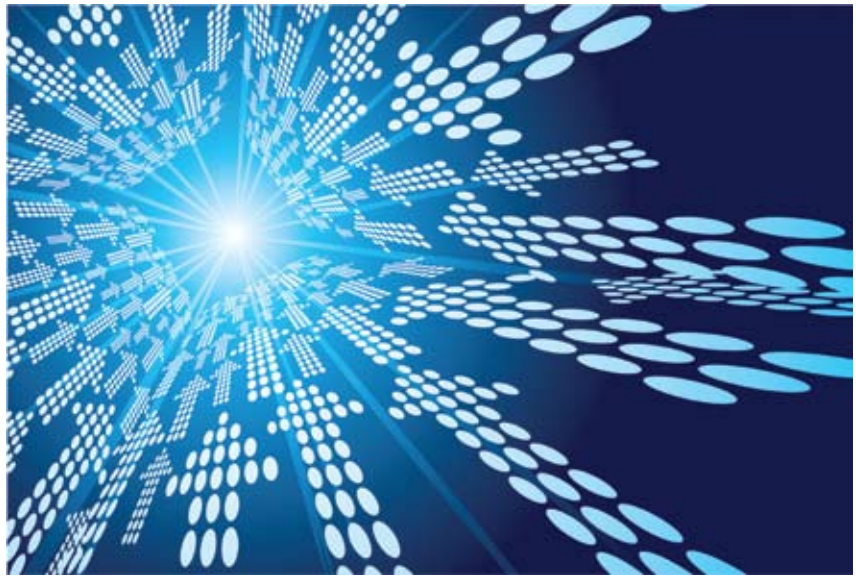


Enterprise Risk Management

A need to hasten the obliteration of legacy IT systems

By Anna DeSimone

Back in the 1980s, IBM mainframe systems were the heart of a bank's computer structure. During this period, integrated retail banking systems were introduced so that branch service representatives had informational database tools to help in cross-selling deposit and consumer loan products.

Soon the industry became flooded with applications that enabled floor personnel to sell loans. Many of these integrated applications took months or years to roll out due to the far-reaching challenges of getting one end of the system to "talk" to the other. Typically, an applications developer would ask, *why duplicate effort or repeat data-entry steps?* Summarily, systems were built with this concept in mind: *if the data exists in our organization, we can access it.* While customer service representatives were able to save a few minutes typing a customer's address in an on-line application for a home loan, an institution's over-reliance on capturing existing data grew problematic.

Venturing into the secondary mortgage market presented mortgage lenders with the opportunity to offer more affordable loans to customers while earning handsome profits. It was very common, however, that secondary market investors or securitizers had compulsory loan amortization algorithm specifications based on 360-day calendar years, a technical obstacle for institutions whose infrastructure was based on a 364-day calendar year. The issuance of a Truth-in-Lending disclosure based on the incorrect calendar year is one example of system incompatibility often discovered after the lender distributed hundreds of thousands of dollars in restitution payments to borrowers as a result of under-disclosed Annual Percentage Rates (APRs).

When something is not working or procedures are vague, employees will often return to their former, often manual, processes. The exception to this is the APR computation — one is very unlikely to see a Hewlett-Packard 93C sitting on a loan officer's desk. Hence the second wave of "bundled applications" was promoted as solutions offering "seamless" integration within the organization's IT architecture.

The priority to hasten the abandonment of legacy systems in favor of robust all-encompassing systems achieves four principal objectives:

First – The Sales Level

Financial institutions need a single platform to control the daily rate quotation for deposit and loan products and their related terms and qualifying parameters.

The scope of the Enterprise Risk Management technology model spans across all divisions and service areas and should cover both internal and external processes.

A regulatory examiner in today's environment is not going to render A-1 ratings to an institution after reviewing a few policy manuals, a small sampling of loans or sampling of anti-money-laundering logs.

Second – The Disclosure Level
Financial institutions need to control the creation and delivery of consumer disclosures and guarantee consistency with respect to form and formulae.

Third – The Monitoring Level
Financial institutions need a system for monitoring activities on an inter-departmental level to ensure that personnel workflow steps and processes conform to internal policy.

Fourth – The Reporting Level
Financial institutions need a system that abstracts information to the Board of Directors, investors, regulators and supervisory agencies.

The scope of the **Enterprise Risk Management** technology model spans across all divisions and service areas and should cover both internal and external processes. Legacy systems generally remain self-contained within their areas of specialty, such as merchant card processing, home equity lending, vehicle leasing, etc. Today's technology choices offer a much wider berth, and with an added bonus —real-time data communications with external agencies and services providers, such as loan settlement agents, mortgage insurance companies, housing finance agencies, and so forth. The graph illustrates the enterprise-wide system operating on a horizontal level.

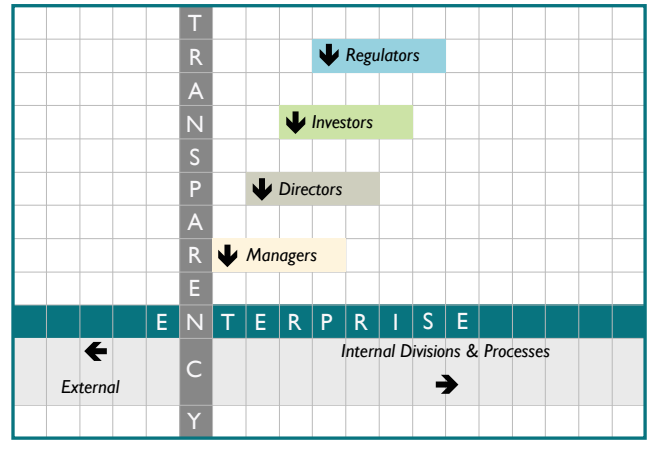
The enterprise-wide system enables compliance managers to monitor timely consumer disclosure of compliance documents in all product areas. Consumer lending risk managers, for instance, are able to view activity reports that segment product by loan type, investor, and rate-lock expire. The risk manager may want to drill down data into segmented groups. Working with information in smaller groups enables managers to monitor risk exposure in critical areas, such as high loan-to-value, lower credit score and so forth.

Sound enterprise risk management systems ideally function as an "early detection warning system" so that incidents are captured early on. Incident tracking is implemented by area of risk, while incident reporting is monitored by area of responsibility. Information becomes aged. The sooner deficiencies are uncovered, the sooner remediation and process improvement can be put into place. The cost of training and re-work diminishes.

Transparency is illustrated as a vertical sector in viewing the operational risk model. Logically, this coincides with the "10,000 foot view" that is a conversational expression used by stakeholders who rely upon executive summaries. A multi-dimensional risk management technology program ideally can produce roll-up summaries of activities across all business units and produce abstracts aptly structured for the administrator or overseer.

Access to federal funds, subsidy programs and secondary market agency programs come with stipulations. A regulatory examiner in today's environment is not going to render A-1 ratings to an institution after reviewing a few policy manuals, a small sampling of loans or sampling of anti-money-laundering logs. The government sponsored secondary market agency or building society in today's risk environment is going to ask the institution to produce reports upon request, such as the rate of defects found in an external auditor's random review of closed loan files.

Twenty-five years ago, financial institutions around the world held on to their unwavering trust and confidence in "Big Blue" and conversions took years to deploy. Times have changed. Banks are vulnerable to lowered safety and soundness ratings, stiff penalties for compliance errors, money laundering and suspicious transaction violations, to name a few. A business unit can become immobilized by unmitigated exposure of confidential consumer information. The need to hasten the obliteration of legacy IT will open the door to implementing state-of-the art technology enhancements that strengthen internal control and promote sound and sustainable banking.



About the Author

Anna DeSimone is President and Founder of Bankers Advisory, Inc., Belmont Massachusetts, USA, a audit and consulting company specializing in mortgage quality assurance and regulatory compliance. She has published 30 guidebooks on many topics of including mortgage fraud, predatory lending, identity theft and international mortgage banking. She can be reached at *anna@bankersadvisory.com*