What Keeps ASEAN Bankers Awake at Night? A Survey of Risk Appetites and Concerns

WHITE PAPER

Sponsored by: IBM

Cyrus Daruwala
March 2012

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.620.5533 F.508.988.6761 www.financial-insights.com

IN THIS WHITE PAPER

This White Paper discusses the findings from IDC Financial Insights' survey on the topics of governance, risk and compliance (GRC) among banks in the ASEAN region. It expounds the significance of GRC technologies in supporting the banks' decision making and risk appetite. The findings also unearthed some "top-of-mind" concerns of pre-selected Chief Risk Officers across the ASEAN region, spanning the areas of Big Data, data management, application integration, regulations and business intelligence.

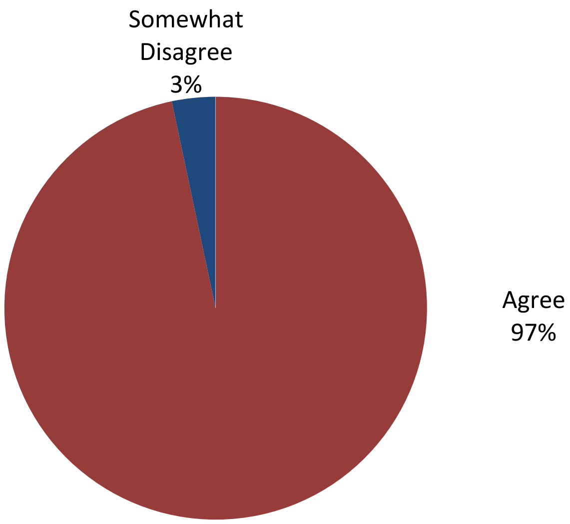
SITUATION OVERVIEW

Technology is an inseparable constituent of today's financial institutions, together with increasing reliance on standardized business processes. The majority of industry practitioners concur that their IT and operational spend will increase by 10-20% compared to last year (see Figures 1 and 2). Analytical tools supporting business decisions and helping assess risk are becoming must-haves for financial institutions. However, in the absence of clean data and a fully integrated business decisioning framework, the real impact of these forward-looking analytical tools is limited. Banks we met with are continuously battling with the issues of siloed data, unclean/unstructured data, and line-of-business heads (LOBs) pushing for top-line growth – finance and risk heads pushing for less risky bets. In addition, there is insufficient enterprise-wide view of data and a lack of ability for enterprise-wide computing of risk. All these issues are further compounded by the impact of regulations and IT/data governance, as well as other IT, operational and compliance challenges.

FIGURE 1

2011 IT Spend Expectations

Q. For this statement: "In 2011, my bank has increased its amount of governance, risk and compliance (GRC) technology spending as a percentage of overall IT spending" - do you:



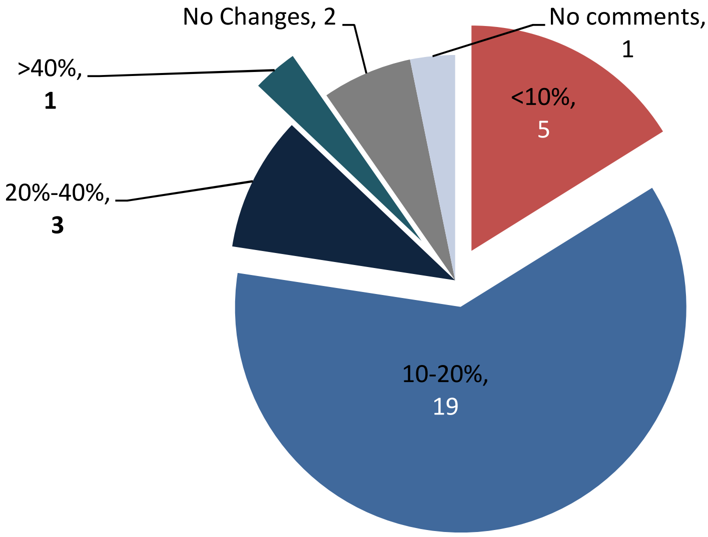
n=30

Source: IDC Financial Insights, 2012

FIGURE 2

Growth in GRC Technology Spend as an Overall IT Spend

Q. My bank is expected to increase the absolute amount of our GRC technology spending in 2012 (vs. 2011) by:



n=30

Source: IDC Financial Insights, 2012

GRC Technology Spending

Risk vs. Rewards

Asian banks now look at their peers in the US and are very concerned with assuming risk they do not understand or cannot forecast. The ongoing crisis in Europe has caused further anxiety among shareholders of the banks and regulators alike. On the other hand, there are serious concerns around "over regulations" too. Do too much and it could eat into the banks' margins and profits, do too little and that opens the bank up to unseen, uncalculated risk. Taking the human element out of risk assessment – using highly sophisticated technology – could be the way out.

A good 97% of banks surveyed in the ASEAN region concurred that the IT/Operations spend related to GRC will increase significantly in 2012 and 2013. Some banks, who are currently not using fully integrated, bank-wide data visualization and comprehensive real-time feed of information, will end up spending as much as 40% more on their IT/Operations budgets (one-time capex and opex costs). However, those who have progressively and consistently addressed the various regulatory mandates thrown their way may get away with as little as a 10% jump in IT/Operations spend.

The maturity of the bank is correlated to the variation in their IT/Operations spend.

Risk Appetite

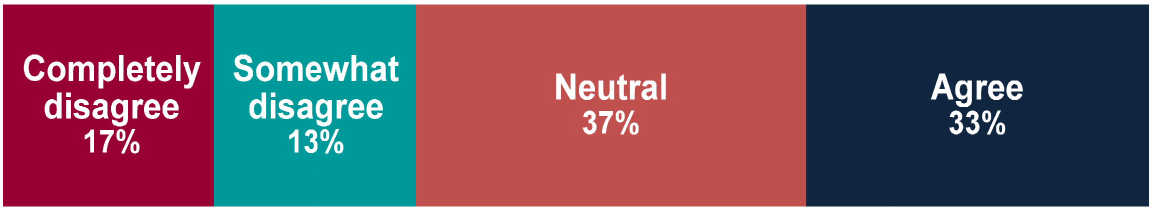
The current uncertainty in the EU zone, the recent lackluster performances by the Chinese and Indian markets and the sluggish recovery of the US have pushed the ASEAN banks to make hay while the sun shines and increase their market and wallet share of customers, grow their loan books and acquire riskier portfolios. That said, only about 33% of the banks surveyed agreed to taking 'more' risk compared to the past couple of years. The others prefer to rest on their 'comfortable' present risk structure and exposure, while a small percentage seems to have become a bit more risk adverse.

Opinion from the industry experts endorse these findings; ASEAN bankers are cautiously optimistic, and hence 'slightly' risk adverse. Regardless of the business and the financial risk appetite, the IT and operational risks are however, non-negotiable.

FIGURE 3

Current Risk Appetite/Risk Tolerance Level

Q. For this statement: "In 2011, my bank has generally increased its appetite for risk versus becoming more risk adverse" – Do you:



n=30

Source: IDC Financial Insights, 2012

GRC Projects – Priorities and Focus Areas

In addition to the standard monitoring of both operational (people, processes, access, physical risk, etc.) and financial risks in the banks, CXOs are increasingly focusing on the constantly changing regulations, and on the severe penalties regulators can and are handing out for non-compliance. When banks were asked to grade their main focus areas within the GRC spectrum – based on resources allocation (monetary, time, labor resources) – 50% of them cited monitoring and managing regulatory obligations as their primary focus/concern (Figure 4).

FIGURE 4

GRC Projects –Priorities

Q. Please list in order of importance, which of the following GRC projects your bank would be focused on for 2012 (Level of importance would be based on resource allocation – monetary, time, labor resources):

Ranked as 1st/Highest Focus Areas	N	%
Managing financial risk	10	33%
Preventing, detecting and remediating financial crime	2	7%
Efficiently mitigating and managing operational IT risk	3	10%
Monitoring and managing compliance with regulatory obligations	15	50%

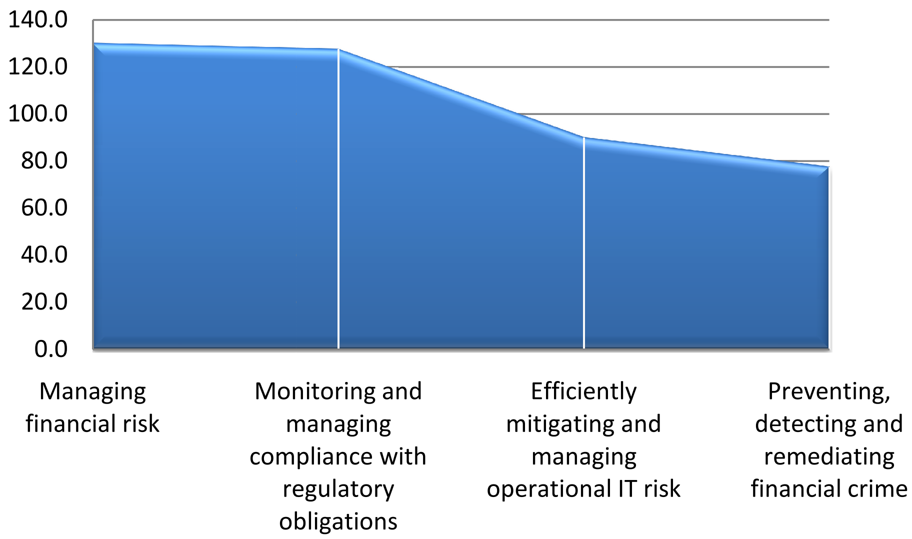
n=30

Source: IDC Financial Insights, 2012

The mounting regulatory mandates are adding to the already expensive, yet necessary, compliance budgets. From a level of importance scale, 'Astute management of financial risk' was termed as most important, followed by 'Monitoring and managing new regulations', and then 'Identifying and mitigating IT risk in a timely manner' (Figure 5).

FIGURE 5

GRC Projects – Main Focus Areas



n=30

Source: IDC Financial Insights, 2012

The larger regional banks that ranked "Management of financial risk" as their first focus area within GRC projects (Figure 5) already have a fully integrated risk management system in place, where compliance tends to be a secondary concern. These banks have consistently been ramping up their governance and compliance "tick-the-boxes".

Data Management

All banks and financial institutions aspire to create real-time/near real-time availability of Big Data anywhere, to enhance their business decision-making process, or to identify and mitigate risk. Furthermore, just a reactive approach towards new governance, risk and compliance mandates are no longer adequate.

When it comes to systems that assist with enterprise-wide risk management of data (transactions and records), nearly 60% of the interviewed banks lacked the capabilities or ability to utilize a robust management information system. They argue that the urgency with which such information is needed constantly varies, hence the capabilities seem to be never adequate.

Market risk, on the other hand, is inherently capricious. The huge amount of external forces, the volatility of the various markets, the fact that we are now – as markets – very global and interlinked, makes it very difficult for banks and financial institutions to factor in all the possible scenarios and possibilities.

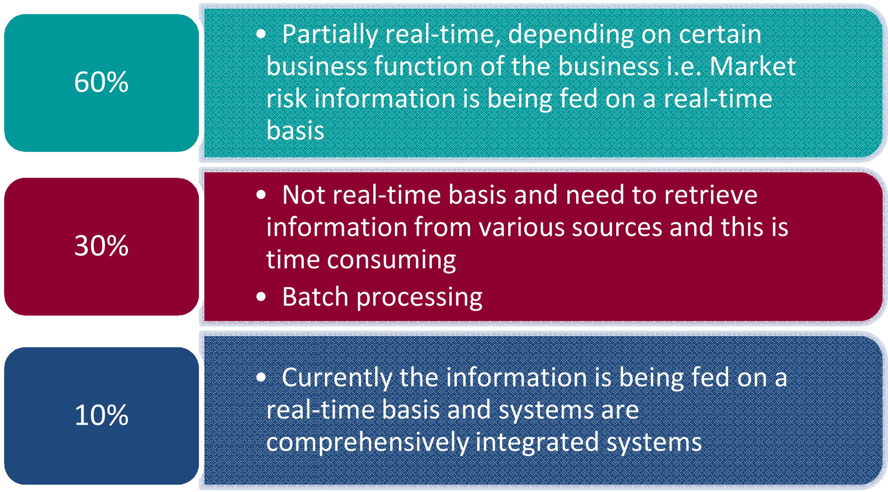
Yet again, this highlights the dire need for a fully integrated system to be able to collate third-party and transactional (historical) data to run real-time market risk simulations (and stress tests). While all organizations would love to have this in place, the costs of creating these systems (which may be severely under-utilized or redundant during off-peak hours) are huge.

Nearly 30% of banks surveyed do not have any real-time market data compilation capabilities (Figure 6). Transactional data and reporting data is presently extrapolated from various sources and are then batch processed. This is expensive and time consuming. Only 10% of the larger and more mature banks (by assets and loan values) within ASEAN can claim to have 'some form of real-time' view of financial risk – at least for the mission-critical financial systems and market-based information systems.

FIGURE 6

Real-Time Data Management

Q. How do your risk management systems provide you with a view of your commercial/retail banking business and your risk environment? How often is the information updated, or is the information being fed on a real-time basis?



n=30

Source: IDC Financial Insights, 2012

Risk Reporting

Ineffective data inputs and absence of valid precedent data inhibits the banks' ability forecast a forward-looking view of the business, or the risk therein.

Only 5 banks (or 23%) interviewed received up-to-date banking forecast from their enterprise data warehouse, and were able to consolidate that data from various sources – to facilitate fast and informed decisions (Figure 7). An ideal state for banks is to be on a real time and fully integrated data warehouse, where even the LOB managers are able to gather and access data as they need, when they need it.

Not surprisingly, as many as 25% of banks we surveyed were dramatically lacking behind the international standard. With sluggish internal data processing that failed to analyze risk information in a timely manner, they relied on consolidated data which are only made available the end of the month. By placing huge reliance on month-end data, a bank inhibits its ability to react to an adverse market turn, or any financial instability in the market.

FIGURE 8

Decentralized Risk Data Analysis

Q. How do your line of business (LOB) managers receive or create reports? How timely are these? Can they also create their own risk reports?

All risks reports are produced by the risk management department. LOB managers can also create their report. Mainly customer information.	9
LOB mangers have access to all data and are able to create their own specific risk reports according to their specific needs.	6
There is no need to for specific risk reports by LOB managers. All the risk exposure and guidelines are laid out by the group risk management board.	14
Trying to move towards the centralized credit risk data mart for pull reporting functionality.	1

n=30

Source: IDC Financial Insights, 2012

For almost 50% or more of the banks in ASEAN, risk reports are churned out by the risk management department on a weekly or monthly basis (Figure 8).

Furthermore, most LOBs and controllers cited that risk reporting and the risk reporting parameters are a top-down management mandate, sometime narrated by a risk committee.

Sophistication of Analytical Tools

Utilizing Analytical Tools

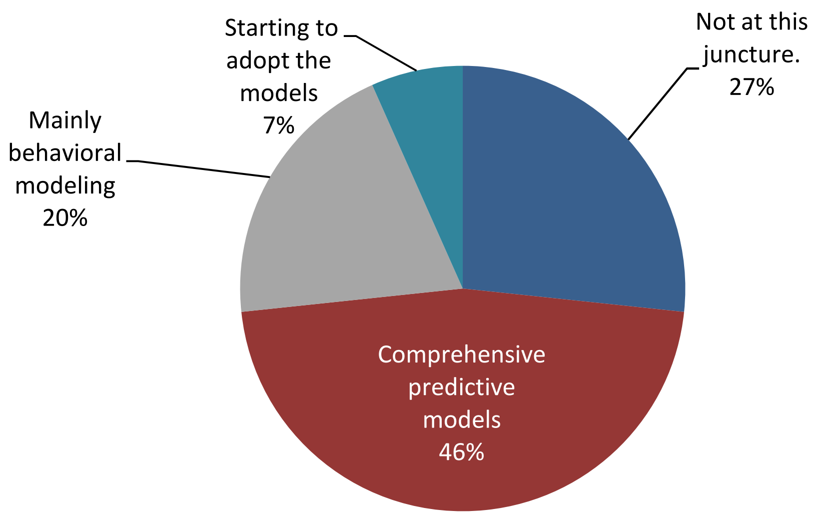
Banks in the ASEAN region (and Asia in general) are actively fine-tuning their predictive and analytical tools and systems, so that they can accurately predict and forecast business, business expansion, stress test their portfolios, and perform scenario planning.

Nearly 46% of the banks that participated in the survey claimed that they had some form of risk-based predictive and behavioral modeling tools to knowledgeably generate business and risk forecast (Figure 9). Foreign banks' subsidiaries in the region often inherit the pre-developed predictive tools used in their respective head offices. Local banks, however, have resorted to buying more off-the-shelf applications (coupled with an extensive data integration exercise) to output predictive reports.

FIGURE 9

Use of Risk-based Predictive and Analytical Tools

Q. Can you provide forward-looking views of the business with risk-based predictive and behavioral modeling at the bank level?



n=30

Source: IDC Financial Insights, 2012

Siloed vs. Integrated Approach to Risk Management

Single view of the business (or even customer) exposure is still on the "wishlist" for many banks across ASEAN. Only 33% of the interviewed banks claimed they have the capability to pull together customer and risk data in one integrated database across risks, products and geographies (Figure 10). To achieve this single view of the business, teams depend on the banks' legacy core and MIS systems. Once these disparate systems are fully integrated and standardized, coupled with some best-of-breed applications and analytical (BI) tools, single view of the business risk (or computing complicated forecast) becomes attainable.

FIGURE 10

Approach to Risk Data Management

Q. Can you pull customer and risk data in one integrated database across risks, products, and geographies? How is this done and how long does it take? Is it in a single view?

Approach	N	%
The level of data integration **does not** allow them to pull together all the relevant data into one single view. Need to perform manual consolidation processes.	18	60%
The integrated database is able to pull customer and risk data in one single view but based on month-end data. They have query tools sitting on top of the database that allow them to set business objects and extract objects via different dimensions.	10	33%
Future target; various measures have been taken to ensure all the necessary model enablers are in place to facilitate greater integration of risk and business.	2	7%

n=30

Source: IDC Financial Insights, 2012

Technology Risk

While technology promises to help banks to grow, simplify their processes and understand risk, ironically, technology in itself is also a risk. The increasing reliance and indispensability of IT systems today calls to task another mandate – understanding the IT footprint and understanding the inherent risk of these convoluted systems.

System failures (some minor, some catastrophic) have plagued practically every bank in the Asia/Pacific region. Astute CROs work very closely with the C suit of CIOs, COOs and CFOs to understand what these risk are, and their preventive measures.

There are assorted methodologies employed by these banks to prevent any major failures – strong corporate governance and periodic systems review were top of mind. Extensive (UAT) testing and simulations are also common practices before implementations/go-live. Industry best practices, standard benchmarks, regulatory mandates and above all, team/professional experience, are the guiding beacons for such ongoing IT (systems) assessments.

In addition, GRC technology development is not a simple one-time process. With the Basel II and Basel III mandates continuing to overwhelm all the CXOs we surveyed, a lack of understanding on what these mandates really are was a consistent feedback. Excessive and (sometimes) irrelevant mandates were also cited for this lack of understanding. Some banks we spoke with (especially those within the less developed markets) tend to bestow the IT and the compliance responsibilities solely on the CIO and the COO. Sure, they may have a risk office, or even a CRO, but their mandate is to literally, tick the boxes and churn the reports.

Vendor Commentary

When it came to vendors/solutions providers in the GRC field, IBM and SAS were seen as distinct thought leaders, with a few others such as Oracle, SunGard and Misys also showing up on the radar.

Very often, local branches of larger retail banks inherit systems from their headquarters (or may procure a local license from their "preferred global vendor").

IBM is largely seen by ASEAN CROs and CIOs as the omni-present risk vendor in terms of hardware, software and innovation. Almost all of the banks would have had some dealings with IBM in the risk and compliance space (some could be just hardware or middleware or solutions procured by a LOB division).

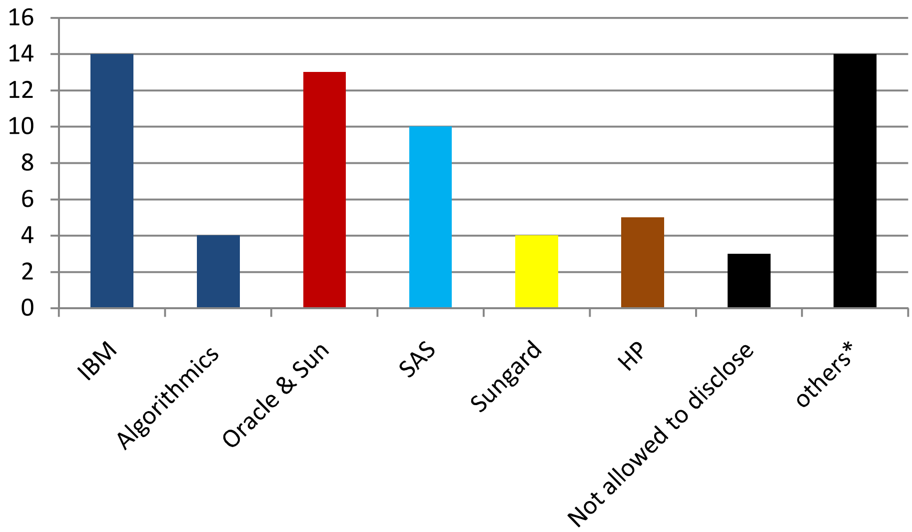
On the other hand, SAS is known as an all rounder – often showcasing their products and is seen as a leader in their areas. SAS is also well recognized in constantly innovating in the risk and compliance space. In addition, their private ownership and independence seems to win accolades.

A good and visibly present competitor to SAS is FICO. Quite a few of the interviewed bankers think FICO and SAS compete head-on, and they agree that both are seen as best-of-breed solutions for end-to-end risk management.

Oracle is seen as leading the pack in databases, data security and a few customer-centric solutions.

FIGURE 11

Respondents' "Top of mind" GRC Solutions Providers



* Others: Murex, TEP Technology, Actimize, Infosys, Fermat, FICO, Guava

n=30

Source: IDC Financial Insights, 2012

FUTURE OUTLOOK

Financial Performance & Enterprise Risk

Investments in risk management and compliance will be strong, representing spending on critical systems and process standardization activities to cope with an adverse economic climate. This would include spending on the suite of applications that support financial performance and enterprise risk and regulatory compliance, such as analytics, data management, document management, and reporting.

New Business Models Risk

Thinning interest margins and loss of fee revenues appear to be the major driver for banks in the region to create new business models. Here, the ideas vary, depending on maturity of the institution and country – new revenue opportunities could include debt recovery services, advisory and consulting, etc.

All these new revenue opportunities would have their corresponding risk implications that the banks would have to deal with.

Fraud in Payments Risk

Increasingly sophisticated fraud techniques keep payment risk management at the top of the CROs' priority list. Asia/Pacific banks will need to be more proactive and adopt an aggressive approach to payments security to more readily protect themselves.

Critical Infrastructure

Lack of human resources with the appropriate (older) technology skill sets becomes a major risk in supporting legacy systems. In addition, institutions that are attempting to reduce cost or meet regulatory deadlines by speeding IT projects to market could be cutting corners with testing and creating additional outages as they bring new features online.

Another risk stems from the fact that incidences of outsourced service failures and operational outages in 2011/12 have proved damaging to confidence in innovative delivery of IT as a service. The banks have to ensure that these do not repeat from 2012 onwards.

Analytics & Financial Crime Management

Firms continue to design a standardized analytics platform to be used throughout the enterprise in various functions ranging from marketing, risk, and operations. Analytics would also be used to assess financial crimes, and involve improvements in customer screening and transaction analytics for anti-money laundering, payment fraud, and employee misconduct management.

ESSENTIAL GUIDANCE

Based on the survey described in this report and IDC Financial Insights' forecast of the outlook for ASEAN banks, these are the recommended actions for financial institutions in the region:

- **Risk should be an organization-wide responsibility.** While the risk management department should be the central point of coordination, if risk management is thought of as issues of concern for just that the risk (and possibly the finance) divisions, chances are high that significant risk exposure would remain. Instead, risk management need to transcend divisional boundaries and be addressed from a horizontal perspective. It is vital that risk management is escalated to an organization-wide responsibility.

  The various business units need to be deeply engaged in the risk management process and should, in turn, manage and maintain ownership of the risk they assume.

  Here, an obvious way to change the entrenched culture and mindsets is to modify performance measurements and incentives, assign accountability for managing critical tasks, and provide personnel with adequate performance feedback and financial compensation for achieving their risk management objectives. KPIs that are closely correlated with risk objectives and desired risk behaviors should be instituted.

- **Prioritize key risks and vulnerabilities that need to be addressed.** Banks are obviously constrained by resource availability and cannot devote all of the attention (and dollars) to managing and mitigating all relevant risk. For instance, when it comes to data protection and fraud prevention, encryption is relevant, but trying to encrypt all enterprise data would be akin to trying to boil the ocean.

  Instead, vulnerability to specific risks should be weighed alongside the probability of their occurrence and impact of losses. Responses would vary from merely tracking a risk and keeping it on the radar without taking any mitigating action to identifying the mission-critical risks that would have the highest adverse impact on the organization's value and strategic objectives and creating early warning signals to recognize these risks.

- **Invest in risk programs for the staff (and perhaps even the customers).** To further ensure longer term sustainability for risk projects, consider instituting a training and certification program (perhaps in collaboration with the regulators or professional associations) to ensure that risk management skills are developed across all strata of the bank and that best practices do not fall on the wayside once risk champions leave the organization.

  This could, for instance, include ascertaining standard operating procedures are in place to address risk issues, diligently conducting orientation risk training for new hires, and ensuring that all staff are trained on proper customer due diligence and data protection.

  Similarly, as part of the customer outreach effort, educational programs can be packaged to build greater awareness among the customers on how they can identify and guard against occurrences such as identity theft during payment card or Internet banking usage. These would be especially valuable for the semi-urban and rural clientele and also has the added benefit of driving branding and goodwill for the banks.

- **Focus on the data infrastructure.** We are well aware that a bank's risk analysis is only as good as its ability to manage considerable volumes of disparate data. It is essential that data is being correctly retrieved, cleaned, and stored because without a strong data foundation, all subsequent risk analysis will be rendered useless. Organizations with a primary focus on data and working toward computations and analysis will surpass those progressing on the reverse.

  They can also look to circumvent the lack of quality data by supplementing internal data on default and recovery with external sources. Where available, this can be done by applying industry benchmarks from data bureaus to fill in any data gaps required for risk calculations, or purchasing vendor-based models to support risk measurement applications that are well established, such as market and credit risk modeling.

- **Consult and collaborate with the appropriate vendors.** As risk solutions grow in complexity and strategic importance, making the best use of limited strategic IT dollars to invest wisely in new capabilities becomes increasingly essential. Utilize in-house development for proprietary risk models that would give the bank a competitive edge, but do also consider purchasing vendor-based applications for the readily available and well-established solutions.

  On the latter, decide which of the risk vendors' offering are most suitable based on your underlying architectures and components. Verify that these financial technology vendors are reputable, offer products that effectively cover both the existing portfolio and can accommodate future updates, are committed to their systems via ongoing research and development, and can administer the support and training required.

- **Finally, Look beyond risk management for regulatory compliance.** Building sophisticated risk measurement models to ensure regulatory compliance is only half the battle won. Compliance to risk regulations should not be an onerous burden on time and resources, but rather an opportunity to translate your risk IT applications into integrated components within business process that can improve efficiencies and deliver bottom-line benefits.

  Technologies for passive risk reporting and proactive decision making are significantly diverse — ensure that your bank is astute enough to make investments in technology infrastructure that go way beyond just complying with tick-the-box regulatory risk requirements.

ABOUT IDC FINANCIAL INSIGHTS

IDC Financial Insights is the region’s leading research and advisory firm, helping banks, insurers and financial institutions choose or short-list solutions and vendors, assess their business or IT master plans, and devise operational best practices. Local practices in Asia/Pacific, Europe, Latin America, and Canada add in-depth regional viewpoints. Our access to senior executives from both business and IT divisions enables us to accurately depict and document trends, best practices and industry benchmarks in the region. For more information, please visit www.idc-fi.com.