CAPITALIZING ON IT INFRASTRUCTURE SERVICES FOR AN EFFECTIVE IT RISK MANAGEMENT IN BANKS
Table of Contents

03 Capitalizing on IT infrastructure services for an effective IT risk management in banks

03 Risk Management in Bank

04 Managing IT Risks

04 Basel

06 Leveraging Cloud Computing for Managing IT Risks and Compliance

06 Conclusion
Capitalizing on IT infrastructure services for an effective IT risk management in banks

This paper examines the importance of IT risk management in banks. The various frameworks used to adhere to regulatory compliances and manage risks better are detailed with emphasis on Basel II/III. While there are prebuilt frameworks that can be deployed on several industry leading Risk & Compliance platforms including SAP, Archer, and Oracle, can IT Infrastructure, being at the bottom layer of the overall architecture, enable compliance and risk management? The paper explores this question and also discusses Infrastructure, Security and Cloud offerings that can help banks better manage these risks.

Risk Management in Banks

The recent downturn has highlighted the need for careful identification and management of risks in the banking industry. There has also been a renewed focus on regulatory and compliance frameworks.

There are several frameworks that are in play in the financial sector including Basel II/III, PCI DSS (Payment Card Industry – Data Security Standards), and SOX. We also have GLBA / US Safe Harbor / EU DPA, ISO 27001 and SAS 70/SSAE16 for Privacy compliance. The complex set of regulatory and compliance frameworks address the various enterprise risks that banks face on an ongoing basis. How can IT enable business to better meet the Regulatory and Compliance needs? Going forward, we discuss the various risks that Banks could face especially from the IT infrastructure perspective, how companies can help better manage them and enable banks to comply with such frameworks.

Managing IT Risks

Risk management is very critical to the functioning of banks. With several types of risks such as interest rate and foreign exchange fluctuations, liquidity affecting global banks, there is a pressing need to have a robust system in place to identify, assess, monitor, track, manage and mitigate these risks.

Inadequate risk management can have serious implications on an organization. The September 11th attack on the World Trade Centre took down an entire datacenter and about 5000 desktops of a leading financial institution. The company managed to be back in the business by invoking its Disaster Recovery Plan and reorganizing/relocating people to alternate offices. Another example highlighting the importance of a risk management system is the blackout of Aug 2003 in Manhattan, USA that crippled around 320 data centers and affected over 1000 companies, 240 of which were financial institutions.

As per CISA (Certified Information Systems Auditor), Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what counter measures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization.

Several regulatory frameworks including Basel II/III, require adequate measures/controls to be in place to identify, assess, track and manage risks. IT can enable businesses to increase their compliance levels to these frameworks and manage risks better. However can IT Infrastructure which is at the foundation layer of the overall architecture, enable compliance and risk management? To understand this, let us examine the Basel framework.
Basel

Basel is a set of banking regulations put forth by the Basel Committee on Bank Supervision, which regulates finance and banking internationally. Basel II came into effect in November 2005 and Basel III is slated for implementation by December 2019. The Basel Accord aims to produce uniformity in the way Banks and its regulators approach risk management across national borders.

Basel has three interconnected pillars:

Pillar 1 deals with calculating capital required for covering losses due to Credit Risk, Operational Risk and Market Risk. The Credit Risk is the risk of loss arising out of a borrower not paying back as promised. The operational risk focuses on the people, processes and systems through which a company operates. Examples of operational risk leading to losses include disasters, vandalism, terrorist attacks, hardware/software failures, data entry errors, employee health and safety etc. The market risk deals with fluctuations in stock prices, interest rates, foreign exchange rates and commodities.

Pillar 2 focuses on the supervisory review of the amount of capital required to cover the risks mentioned in Pillar 1. Additionally it includes risks such as liquidity risk, reputation risks, legal risks that are not part of Pillar 1 and cannot be easily quantified.

Pillar 3 focuses on market discipline by requiring lenders to publicly disclose details of their risk management activities, risk rating processes and risk distributions. The IT related risks would fall under the Operations risks category as per the Basel framework.

The Basel Accord aims to produce uniformity in the way banks and banking regulators approach risk management across national borders.
Some of the most common operational risks faced by the financial institutions are:

<table>
<thead>
<tr>
<th>Risk</th>
<th>Solutions</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Example Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datacenters disasters</td>
<td>Disaster recovery planning and management</td>
<td>****</td>
<td>High</td>
<td>RTO (Recovery Time Objective)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RPO (Recovery Point Objective)</td>
</tr>
</tbody>
</table>
| Loss of sensitive data due to a breach    | • Intrusion detection and prevention services  
• Data loss prevention                    | Depends on security posture and sensitivity of data involved | High   | Anomalies detected  
• Cryptographic strength  
• Mean time to attack                     |
| Network threats and vulnerabilities       | • Unified threat management, security event log correlation, analysis  
• Security device management (e.g. firewalls) | Depending on the security posture | High   | Number of threats or attacks prevented |
| File based threats, spyware               | • Antivirus, anti spam management  
• Unified threat management               | Depending on the security posture | High   | Number of threats or attacks prevented |
| Operations risks – human errors – such as erroneously shutting down wrong servers in production environments | Quality processes such as change management for minimization of these errors increased use of automation | Low      | Medium/High | Number of incidents/outages due to human errors |
| Operations risks - downtime of online systems or ATM switch etc. | Quality processes such as change management for minimization of these errors increased use of automation | Low      | Medium/High | Number of incidents/outages due to system/infrastructure failures |

The standard way of measuring a risk is:  
Risk = Likelihood \times Impact

Basel gives guidance on measuring risks by using methods such as Basic Indicator Approach, Standardized Approach and Advanced measurement approaches. The first two methods use a percentage of the revenue to set aside capital for Operational risks while the advanced measurement approach uses the internally developed risk management framework within the bank.

After a detailed assessment of the IT risk environment, the risk manager will be able to identify the root cause and assign actions.

Cloud computing is a fast growing technology, that has tremendous potential in business applications. In the banking sector, a number of factors need to be taken into account before cloud computing can be used to better manage these risks.

Risk management and compliance will include the sphere of emerging technologies such as Cloud Computing, Mobility and Social networks.
Leveraging Cloud Computing for Managing IT Risks and Compliance

**Stress Testing:** Financial institutions need to perform extensive calculations (stress testing) using statistical models to assess the financial risks. The stress testing takes into consideration extreme conditions often to a breaking point, in order to observe the results. The stress testing exercises need a significant amount of computational resources.

This is a very good use case for variable compute workloads. The benefits of using an elastic/scalable solution using cloud for stress testing are:

- No Capital expenses
- Pay as you go - Variable Costs
- Quick provisioning and Implementation
- High scalability

**Outsourcing Risks & Compliance:** The service delivery models related to outsourcing risks and compliance have evolved over a period of time. Multi-tenancy models/ Flex Delivery models are proposed to bring in non-linearity and cost savings. From a compliance perspective, some of the issues that need to be taken care of are:

- The impact of the Shared Services Delivery model/ Flex Delivery Model on the various regulatory frameworks that require the client's compliance
- The controls that have to be put in place so that the Banks are compliant with the necessary frameworks
- Whether the partners or vendors have adequate controls and policies in place

**Future Trends:** Continuous changes and updates in regulatory frameworks and new regulations are likely to be introduced. This will increase spend on risk management and compliance by financial services organizations and it comes at a time when businesses are under pressure to optimize costs.

Organizations will also move away from template-based risk and compliance to comprehensive, automated, continuous and auditable risk programs with added focus on using tools and automation for managing risks and compliance.

Analytics is going to play an important role in assessment of risks and understanding compliance requirements. Risk management and compliance will include the sphere of Emerging technologies such as Cloud Computing, Mobility and Social networks.

**Conclusion**

The regulatory and compliance environment is becoming more complex by the day, demanding significant efforts and focus from banks. Many banks are global and continue to expand across multiple geographies exposing them to a variety of risks. Hence, there is a need for IT Risk management to align with the overall Enterprise Risk management.

IT Risks need to be identified, assessed and managed continuously. IT Risks in particular can be managed using the various frameworks and solution accelerators that have been discussed in this paper. It is also important that the IT organization has an open culture in sharing of information. Risk management is not the sole responsibility of the Chief Risk Officer or the Risk manager. Every individual has a role to play.

**Reference**

- Pulling the Plug on Wall Street - Disaster Recovery Journal
- www.forrester.com
- www.gartner.com
- www.mcafee.com
Global Infrastructure Services

Wipro’s Global Infrastructure Services (GIS) is a pioneer in the Infrastructure Management services space with revenues of $2Bn USD. This division contributes to over 30% of IT revenues of Wipro Ltd, with a headcount of over 26,000+ technical specialists. Our strong domain capabilities and specialized offerings help businesses across the globe transform their vision to results. Backed by our strong network of iGCCs (Integrated Global Command Centers) and 10 owned datacenters spread across US, Europe and India, GIS is enabled to provide cost variabilization, accelerated growth and continuous innovation for global businesses. Few of our industry specific service offerings include Wireless Place, Shoptalk™, Bank-in-a-Box while our traditional offerings include data center management, cloud, managed network, managed security, end user computing and business advisory services.

About the Author

Harish Sudhamalal has led solution definition for large multi-tower infrastructure wins in BFSI accounts. He has diverse experience spanning across infrastructure support, storage engineering, end-to-end solution architecting, practice incubation, practice development and global service delivery. He successfully championed the Run Book Automation initiative which has been integrated with Wipro’s Global Command Center. His key areas of focus include “verticalization” such as “Bank-in-a-Box”, Mobile Banking and Enabling Banks to comply with Basel III. He has 25+ years of IT infrastructure experience.

Disclaimer: The material in this document is provided "as is" without warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. The material are subject to change without notice and do not represent a commitment on the part of Wipro. In no event shall Wipro be held liable for technical or editorial errors or omissions contained in the material, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the material. The materials may contain trademarks, services marks and logos that are the property of third parties. All other product or service names are the property of their respective owners.