Using Risk Management Architecture to Power Enterprise Agility

Abstract

Modern day risk management is no longer limited to dealing with potential losses, but also extends to managing organizational reputation and customer goodwill, as well as ensuring cyber strength and security. With bots and emerging technologies playing a significant role in banking operations, implementing an integrated cloud and data management solution is a must. This not only solves complex infrastructure challenges in the financial ecosystem but also helps build and nurture customer relationships.

This paper explores how risk management agility can be achieved by leveraging the cloud as a solution for a unified platform across financial instruments and integrating cloud and big data management with built-in intelligent automation solutions. The paper also focuses on the need for gathering data in real time and reporting through a unified system, bringing in enterprise level agility in risk management.

The Bot Age: Tackling Banking Security Challenges

Modern day banks use bots for a variety of tasks to drive customer experience, increase sales conversion rates and improve revenue opportunities. However, it puts banks at an increased risk of virtual attacks. According to VMware Carbon Black's report on 2020 threat landscape, attacks on financial institutions spiked by a massive 238% from February to April 2020.[1] When combined with the steady growth of mobile and internet banking, the risk landscape is ever expanding, creating opportunities for a wide range of attacks such as ransomware campaigns, distributed denial of service (DDoS) attacks and business email compromise (BEC) scams. Though bots can minimize such risks to some extent, it is critical that organizations become more serious about handling vulnerabilities, minimizing chances of such incidents and safeguarding customer interests.

Simplifying the Risk Function to Reinforce Security at Every Level

So far, risk management has been a complex function. Organizations realize that it has become imperative to build agility into robust planning and execution of risk identification, mitigation and audit. The mandate is clear: identify quick wins, simplify structure of risk management, and decentralize functional stratums to build an agile and robust risk management system with multiple levels of security.

Each financial institution handles complex transactions that result in operational, customer, management or strategic risks across various stages of profiling of individuals involved in the transactions. A robust risk management tool that helps study patterns and map the risk as high, low or medium based on such profiling results in proper decision making at each level of transaction.

An architectural risk management approach (see Figure 1) is key to simplifying and implementing intelligent digital automation at an enterprise level. Organizations can explore automated reporting and predefined rule engines for complying with various regulatory requirements across functions in the banking industry. This will help build a

[2]   VMware Carbon Black, Modern Bank Heists 3.0 (May 2020), accessed January 2021,
       https://www.carbonblack.com/wp-content/uploads/VMWCB-Report-Modern-Bank-Heists-2020.pdf

robust, industry-standard risk management ecosystem. Such a system can mimic a human brain, identify existing risks in the systems, and trigger risk events using big data analytical tools fed with possible risk scenarios. This helps avert risks at a transactional level.
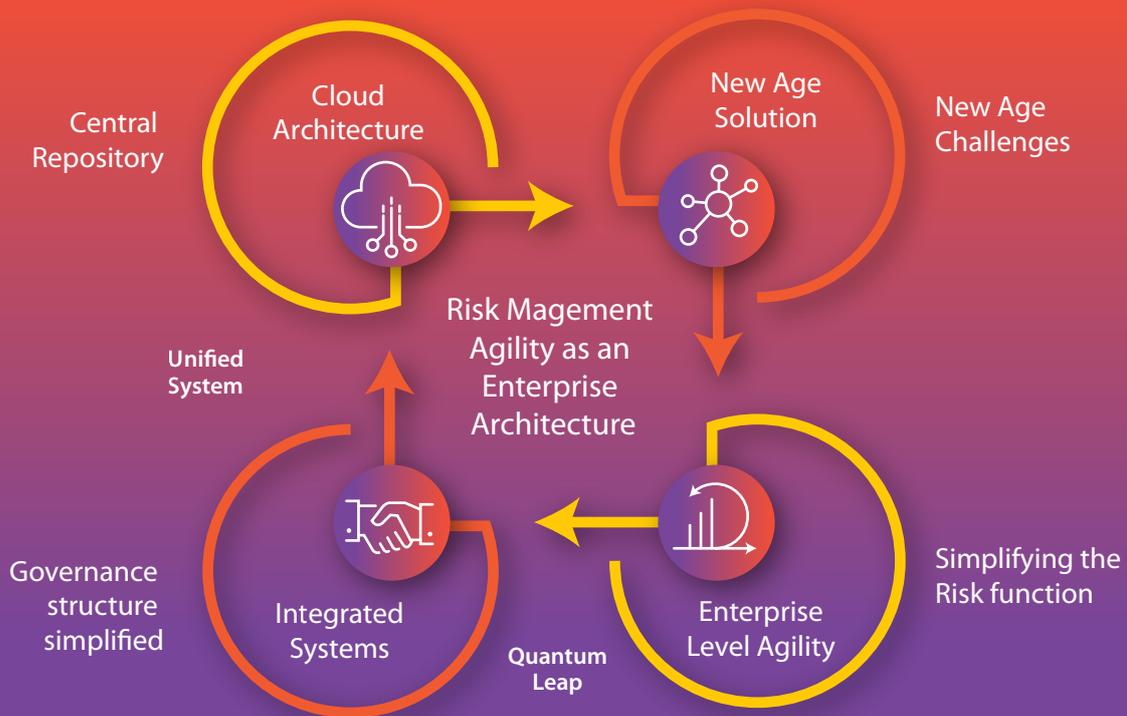

Figure 1: Risk Management Agility and Enterprise Architecture

Turning to the Cloud

What's missing from current risk management strategies of most financial services firms is a robust mechanism to store and retain data. To help close the gap, banks can build a customizable, secure and efficient cloud infrastructure. It is also paramount to build a user interface (UI) for real-time data availability. The upshot? Enhanced regulatory compliance with real-time data for improved auditing. In addition, historical data helps provide more insights into risk patterns for handling the system cautiously while mitigating any risk.

Adopting a Unified System for Real-time Data Processing

It is not enough to just build a cloud architecture to manage big data. Organizations need to set a rule to define risk at each stage of a transaction. This helps trigger the risk event to the next two levels for analyzing and reporting such anomalies as a visual representation for easy decision-making.

Analytical tools and bots based on defined rule engines can help run complex algorithms to gather, build queries and retrieve knowledge bank and process data. However, these tools need to be integrated to identify risk events in the ecosystem at each stage of the lifecycle for all transaction levels. For example, in cash management, the system should identify potential risks while posting entries and flag any manual interventions when reporting data to treasury systems. On the other hand, manual intervention in treasuries funding should trigger flags to senior decision-making boards for a thorough appraisal before any action is taken.

While AI tools can help identify risks in processing, storing and transferring data across platforms and messaging systems, it can be a challenge to unify different platforms for reading, analyzing and storing data. A unified rule engine can enable organizations to build a seamless, risk-free, real-time data processing environment. This boosts data reporting and gathering to meet various auditing standards such as Capability Maturity Model Integration (CMMI), International Organizations for Standardization (ISO), Office of the Comptroller of the Currency (OCC) and Customer Service Provider Standard (COPC) and SSAE standards.

A deeper understanding of keyword management proves beneficial in flagging risks in real time before they get archived for future processing. This helps identify patterns and proactively trigger so-called risk events in the system. This can be achieved through a global unified system like the Sanctions and SWIFT ecosystems built exclusively for risk management. It can even simplify such ecosystems due to the ever-expanding UI and design thinking scalability that will replace the existing legacy platforms that would lead to more transparent expression of data for such audit requirements.

A Quick Take

Understanding Advanced Risk Management Tools

Banks can use artificial intelligence (AI) tools that gather and build queries for retrieving the knowledge bank and processing data. This can help identify risk events in the ecosystem at various levels across the transaction lifecycle. An example is cash management where an AI tool can trigger flags to senior decision-making boards before any manual intervention in an existing treasury system that is stress tested and automated.

Setting a rule that defines the risk of a particular action and triggers the risk event before the said action is authorized at each stage of a transaction can enable banks to identify anomalies and improve decision making at each stage of the transaction.

Reshaping the Governance Structure with Integrated Systems

Once the central data repository is in place, integrating client and organizational systems in a unified structure is crucial to calibrate and check various inputs that are fed into the setup. This improves data interpretation across various platforms while helping address rule based models and mimicking risk scenarios based on simulations and algorithms to prevent any risk beyond human intervention and control.

Currently, the systems integration across transaction processing is usually independent of the function carried out by that division. The bane of legacy systems lies in consolidating and building dashboards. Financial institutions are dependent on third-party dashboards for efficient risk analysis and assessment which is possible only when systems are integrated.

Banks realize the importance of such risks and have started managing risk at source to mitigate them. This requires robust infrastructure to build an integrated system.

Risk governance usually covers basic elements such as identification of risk and the underlying factors to ensure the event does not occur in the first place. Assessment ensures risk events are identified before they happen, management of risk ensures all risk

events are managed efficiently and relevant risk mitigants are applied for a safe environment involving financial transactions. Risk reporting must be transparent with an enterprise architecture that reports events of risk without bias.

In a typical risk management team, each department has an independent and diversified risk team. This practice is effective when the products are homogenous. However, institutions that are heterogenous in nature, with multiple legacy platforms, need to individually enforce risk mitigation practices. Collective risk management is absent in such an environment – this necessitates an enterprise level architecture to integrate systems and record events holistically.

Taking a Quantum Leap to Protect Financial Systems

As organizations increasingly embrace the work-from-home model, an industry-level unified system becomes paramount to protect financial systems and institutions from vicious attacks that test the stress levels of systems. Engaging with the right partners can help develop prototypes for migrating to the high-end complex field of quantum computing. However, quantum computing is at a nascent stage and demands larger infrastructure to analyze and store sensitive information. Given the increasing complexity of cyber-attacks, financial organizations that leverage quantum computing will be able to create a safer and secure banking environment. High-end computing capability will help organizations embark on a new risk-free journey, providing opportunities for building an ecosystem and establishing robust risk management.

About The Author

Karthik Venkataraman

Karthik Venkataraman is a domain expert with TCS' Banking, Financial Services, and Insurance business unit at TCS. He is currently part of the business development function for multiple clients across the APAC region. With over 18 years of experience in banking sector, Karthik has worked with clients in multiple domains including retail banking, capital markets, and wealth. He has extensive experience in project management, consulting, and operations and has been instrumental in building and managing teams for several relationships. Karthik has a Bachelor's degree in Commerce from the University of Madras, India, and a Diploma in Business Administration from IGNOU, Delhi, India.

Contact

Visit the https://www.tcs.com/analytics-and-insights page on https://www.tcs.com

Email: analytics.insights@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that has been partnering with many of the world's largest businesses in their transformation journeys for over 50 years. TCS offers a consulting-led, cognitive powered, integrated portfolio of business, technology and engineering services and solutions. This is delivered through its unique Location Independent Agile™ delivery model, recognized as a benchmark of excellence in software development.

A part of the Tata group, India's largest multinational business group, TCS has over 453,000 of the world's best-trained consultants in 46 countries. The company generated consolidated revenues of US $22 billion in the fiscal year ended March 31, 2020, and is listed on the BSE (formerly Bombay Stock Exchange) and the NSE (National Stock Exchange) in India. TCS' proactive stance on climate change and award-winning work with communities across the world have earned it a place in leading sustainability indices such as the Dow Jones Sustainability Index (DJSI), MSCI Global Sustainability Index and the FTSE4Good Emerging Index.

For more information, visit us at **www.tcs.com**

Experience certainty. IT Services
Business Solutions
Consulting