e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 8, August 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

© 2024 IJMRSET | Volume 7, Issue 8, August 2024| DOI:10.15680/IJMRSET.2024.0708078

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

From Fragmentation to Agility: Nautilus Architecture for Risk Management Modernization

Nagabhushanam Bheemisetty

Independent Researcher, USA

ABSTRACT: The implementation of Nautilus Centralized Application Development Framework for Non-Functional Features will centralize all non-functional features so that Product Teams can concentrate on functional logic and reduce latency in adapting changes to the system and adding new features. It also enables the rapid modification to and addition of Non-Functional Features from one place, thereby speeding up compliance to regulations for National Bank of Umm Al Qaiwain in the UAE, thus reducing time-to-market, empowering product teams to meet demand without needing to deploy additional code and providing an opportunity for revenue growth. Due to testing limitations, the Technical Team of Nautilus has been developing a solid architecture and has ensured smooth operation through User Training and Staging Rollouts. In preparation for cloud native products and AI and Machine Learning (ML) capabilities as well as cross border compliance, Nautilus is building a scalable middle tier Middleware Infrastructure to support future delivery of these product capabilities.

KEYWORDS: Nautilus Centralized Middleware, Machine Learning (ML), Revenue Growth, Staging Rollouts

I. INTRODUCTION

The Risk Management process is a systematic method of identifying, assessing, classifying and managing risks that can affect an organisation's objectives, resources, operations and financial position. It provides benefits, including reducing risks, enhancing return on investment, improving decision-making; as well as a number of challenges, such as the need for strict adherence to protocol; increased complexity; and the need for skilled personnel and quality data. In the Banking Industry, Risk Management provides for the identification of, Credit Risk, Market Risk, Operational Risk, Cybersecurity Risk, and Regulatory Risk; and allows banks to optimise their capital position and make better informed lending decisions while complying with regulations and building resiliency in the face of economic fluctuations. In addition to minimising risks and maximising regulatory compliance while addressing risk associated with capital markets, banks also utilize various strategies, including Risk Avoidance, Mitigation and Transfer; to provide satisfactory Profit Margin in the wake of the increasingly complex Global Capital Markets.

Risk Management in the Banking Industry is distinctly different from that of Non-Banking Industies. Banking Procedures must comply with stringent regulations; and are therefore centred on Financial Risks (Credit and Market Volatility). Other industries utilize a decentralised approach to the management of Operational Risks and Sector-Specific Risks, while Banking is primarily focused on Regulatory Compliance (e.g. Basel III international regulations) and Quantitative Financial Modelling. One of the main differences is that Banking requires a Chief Risk Officer and compliance with international regulations, whereas most Non-Banking Industries only require Compliance Officers for regulatory compliance associated with their specific industry. Banking prioritizes Financial Risks and utilizes tools such as Hedge and Stress Testing; while Non-Financial industries prioritize Environmental, Social and Governance (ESG), Reputation, and Operational Risks. The Centralised Structure of Enterprise Risk Management in Banking is significantly different from the more Integrated approach that most other industries utilize, where the Chief Financial Officer typically oversees Mrisk Management practices without having specialised executives dedicated to the function [1].

Bank supervision and compliance (including both Basel II and Basel III) with consumer loans have been in place for over a decade, supporting highly regulated financial intermediation as compared to other sectors.* Through years of

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

compliance and consumer loan tracking and development, risk management leaders within banks have developed tools to assist with consumer loan processing and monitoring, and they also consider International standards such as Basel II and Basel III as well as individual national laws when developing consumer loan tools. Due to the need for more customized tools, banks face challenges in terms of processes as they can be delayed in implementation or integrated due to differing technology across products [2].

To address these issues, a FNGBFS Framework, called the Nautilus Framework, has been developed. The Nautilus Framework was designed to allow for the development of a single framework for all banking risk management functions to allow for streamlined and efficient development with elimination of redundant components and customization without creating silos. Through this framework, all non-functional skill-related components are consolidated in a single central repository, giving banking teams the opportunity to focus on developing core functional innovations related to banking risk management, including identification, evaluation, mitigation and monitoring of client and operational risk .

Nautilus provides banks with a central database for storing and managing user and feature information, role-based access controls for users accessing the Nautilus system, integration with customer verification systems to support secure verification of customer identity, flexible workflow control, comprehensive reporting capabilities for reporting domestically and internationally, integration with notification systems, and segregation of non-functional skill components for building and developing business logic (e.g., developing the structure and design of an insurance product's underwriting criteria). In addition to being able to develop a central database and retain information centrally for ongoing reporting, Nautilus also provides flexibility for banks to integrate with the various systems utilized by their respective functional areas (e.g., loan processing, legal, compliance, and/or accounting) to assist with maintaining an efficient workflow for both portfolio management and overall banking operational activities. Regulation of banks in the United States is based upon two International regulatory standards; Basel II and Basel III [3].

The Basel II and Basel III Frameworks were designed to support Capital Adequacy, Liquidity and the Systemic Stability of the Banking industry after the financial crisis of 2008. Basel III provides stricter requirements for Capital Adequacy in that it requires that all Banks maintain a minimum ratio of Common Equity Tier 1 Capital (CET1) to its Risk Weighted Assets (RWA) as well as adds a requirement to continue holding sufficient levels of Liquidity in order to meet short-term stress situations and to restrict excessive borrowing.The regulations require banks to have sufficient risk-weighted asset protection, conduct regular "stress tests" (ie, simulations) of their operations during periods of unexpected market volatility, and utilize sophisticated risk assessment methodologies to cope with these uncertainties. Through collaboration between industry leaders and consumers, a suite of industry-leading applications were developed specifically for consumer loan processing, credit risk assessment, as well as compliance-reporting against Basel III standards, while being shaped in accordance with the different.policy requirements of respective jurisdictions. The movement from a disparate collection of technology-driven applications, to a single, fully-integrated solution is critical to the ability of banks to create tailored processes to meet their unique loan-approval and compliance-audit requirements. In addition to helping banks address the inefficiencies of separate system approaches, the new "shopping/here to stay" environment enables banks to more quickly and effectively respond (or recover) to emerging threats such as cybersecurity breaches, interest rates and loan delinquency.

On the other hand, digital transformation in retail banking is changing risk profiles significantly by creating additional operational risks due to its reliance on online banking, as well as generating new cyber-security risks that can only be partially addressed using data analytics and AI-based solutions. Studies indicate that in 2024 over half of financial institutions' operations will experience a significant volume of cyberattacks as a result of the transition away from a primarily paper-based business model to an increasing reliance on electronic payment methods, including mobile applications and online lending platforms. In addition to creating cyber-security risks, the reliance on digital channels exposes retail banks to new opportunities for AI-based fraud targeting financial institution transaction data. As a consequence, it has become increasingly problematic for retail banks to remain compliant with established regulatory frameworks such as Basel III, General Data Protection Regulation (GDPR), and Payment Services Directive 2 (PSD2) due to outdated legacy systems that are unable to adequately capture and process fragmented data that lead to increased risk of non-compliance.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Nevertheless, by combining innovative fintech partnerships with traditional legacy bank risk solutions, financial institutions can not only better price and monitor their risk, but also create greater transparency into their lending strategies without diminishing the effectiveness of controls used to mitigate credit risk.Digital adoption has decreased both traditional credit and market risk considerations, while also creating opportunities for organizations to strengthen their resilience to economic shocks and competitive pressures by partners investing in automated compliance and fraud detection tactics. This changing landscape implies that retail banks must develop balanced plans that will maximize efficiencies while minimizing risks associated with the emergence of new opportunities [4].

There are several methods for quantifying the financial aspect of the risk for fraud posed by AI-created hacks. Commonly used methods include probabilistic modeling, Monte Carlo simulations and AI-enhanced behavioral analysis. Each of these processes begins with identifying the attack vectors used by these types of attacks (for example, automated evasion of detection, AI-phishing and deepfakes = fraudulent phishing attacks), which have the potential to significantly increase the volume of fraudulent activity. Data gathered by the use of device fingerprinting and other network signals enables organizations to better analyze the levels of transaction volume and system entry points at risk of being attacked. Probabilistic modeling and Bayesian algorithms are then used to determine the likelihood of specific outcomes based on the extent of damage caused by the attack, the frequency with which the attack occurs, the timing of the occurrences and other variables.

With regards to the Retail Banking Sector, an established systematic methodology has been developed to provide for accurate measurements of the aforementioned risks. This methodology encompasses the use of generative AI for modelling baseline behaviors of users and for the purpose of identifying potential anomalous behaviors; the application of Monte Carlo simulations to identify specific metrics such as value at risk (VaR) and return on investment (ROI) from the use of the mitigation methodology; and lastly, the stress testing of the system for possible evasion types of attacks, all of which are achieved through the use of probabilistic graphical models. Different organizations rely on various forms of real-time AI-based systems. Continuous monitoring provides the opportunity for adaptive learning on the part of the organization. By employing this multifaceted strategy, Chief Information Security Officers (CISOs) can be more proactive about prioritizing their defenses, developing more robust insurance programs and improving their ability to detect fraudulent AI-based activity [5].

Estimates indicate that the total financial impact of Generatively AI created fraud to date, and continuing through 2023 will see an increase from $12.3 billion to as high as $40 billion during the next four years. This rapid increase in AI-based fraud is attributed to the proliferation of deepfakes, synthetic identities, and scalable phishing schemes. As a collective, these forms of AI-based fraud will create a significant risk to retailers participating in the Retail Banking Sector, with synthetic identity fraud alone resulting in estimated losses of between $20 billion and $40 billion, essentially linked to victimization through the illegal utilization of loans or financial accounts. Based on current projections, the worldwide losses associated with digital payment fraud will exceed $40 billion as well by the end of 2027.

In many cases, various size of retail banks have a transaction volume that is estimated to be 10 million transactions on an annual basis and the total loss from fraud for these banks would fall under several different loss potential scenarios. For example, low-level fraud (associated with phishing techniques using the most basic forms of AI to conduct these types of attacks) would estimate annual losses ranging from $5 million to $10 million. Medium-level fraud associated with deepfake impersonation may result in losses ranging from $25 million to $50 million. Likewise, high-level synthetic identity fraud, associated with the emergence of thousands of new identities, would have estimated losses ranging from $100 million to as high as $250 million when taking into consideration the drastic rise in the number of identity theft cases. In terms of worst case scenarios, the financial impact could potentially exceed $500 million in total losses as a result of coordinated attacks involving account takeover (aka "brand-loan") fraud and ransomware attacks, which would have a total average incident cost estimated to be $680,000 [6].

II. RELATED WORK

Foundational integrations of AI technology in the Financial Sector's risk management involve the use of machine learning models and Generative AI Models for automating anomaly detection and outcome prediction, enhancing real-time oversight on Basel II/III pillars of Capital Adequacy and Market Discipline. Rapid changes in regulations, such as

the EU's AI Act, necessitate frameworks like NIST's AI Risk Management Framework (AI RMF) for Continued Monitoring, Data Governance, and Bias Mitigation, ensuring reliable AI in Critical Applications such as Credit Scoring and Fraud Prevention while managing Dynamic Risks unaddressed by Traditional Modelling Techniques. AI deployment strategies improve the enterprise risk management (ERM) processes, aiding compliance and resilience during periods of financial instability. The FREE-AI model, developed for Indian Banks, emphasizes Explainability and Data Validation to align AI Decisions with Basel Capital Regulators' standards, potentially reducing defaults by 20%. The Monetary Authority of Singapore (MAS) guidelines promote three-lines-of-defense models for AI Governance, and EY advocates for Comprehensive Risk Management Ecosystems. Finally, IBM's Risk Operations enhance existing ERM processes through global AI capabilities, improving the accuracy of Market and Liquidity Risk Forecasting. These frameworks facilitate a proactive, AI-driven compliance approach, yet challenges like Integration Security and Model Drift persist [7].

AI-Integrated ERM for Financial Institutions utilizes Big Data, along with Behavioural Analytics, to enable Proactive Fraud Detection rather than Retrospective Compliance, in line with Basel III's emphasis on Operational Resilience. The use of Machine Learning Models enables Financial Institutions to establish Dynamic Baselines for Customer Behaviour; and to identify Fraudulent Activity (e.g., Unusual Login Activity) with a very High Degree of Accuracy (>95%); thereby reducing the risk of Account Takeover Fraud.This method reduces significantly the number of false positives when compared with traditional rule-based systems while simultaneously utilizing generative AI (Artificial Intelligence) to build predictive models regarding the future exploitation of fraud. An example of such a technology is TCS (Tata Consultancy Services) through which their AI technology predicts credit defaults, and Deloitte (the company) through the use of Graph Analytics to monitor Non-financial Risk Factors. While data silos remain an impediment in many areas of Fraud Prevention technologies, SAS (Statistical Analysis Software) and MetricStream have built frameworks on Adaptive Learning principles to help reduce Fraud Losses. As such, these developments are propelling Banks to transition toward Robust, Data-Driven ERM Ecosystems [8].

The three components of Basel II/III are coordinated through the use of Artificial Intelligence and Machine Learning in order to provide capital enhancement across the full spectrum of banking operations including but not limited to Market Monitoring, Portfolio Optimization, and Fraud Prevention. The area of Pillar 1 utilizes predictive modelling algorithms through Machine Learning, which assess many large amounts of historical data, to calculate Risk Weighted Assets with great precision. For example, the use of Predictive Credit Scoring reduces Risk by identifying potential Defaulting Customers and allowing for Dynamic Asset Allocations. The use of Anomaly Detection enables the identification of Fraudulent transactions and better detection of potential fraud. Pillar 2 also provides the ability to predict Liquidity Issues through the use of Generative Models, as well as perform Supervisory Stress Tests through the construction of Recession Scenarios. In the area of Pillar 3, Natural Language Processing and Time-Series Forecasting provide Banks with valuable information such as Real Time VaR (Value at Risk) and Hedging Strategy adjustments during periods of Extreme Market Volatility. Graph Neural Networks are implemented to detect Money Laundering Activities and provide better protection against Fraudulent Identities. In conjunction, the implementation of Reinforcement Learning in portfolio management systems facilitates the Dynamic Rebalancing of Asset Exposures, while EY and KPMG are focused on providing Model Risk Management Frameworks to mitigate AI Biases and ensure Compliance. Overall, the implementation of AI technologies in Banking will provide increased efficiencies; however, to avoid Model Drift, organizations must establish Reliable Data Pipelines [9].In recent years, we have witnessed a rapid increase in the development of machine learning techniques used for fraud detection. There has been an explosion of the availability of sequential transaction data (often referred to as time-stamped transactions), the availability of geolocation data of accounts that are being accessed at any given moment (using GPS coordinates), as well as the ability to track user behaviour in real-time across banking channels.

Through the use of these innovative technologies, fraudulent transactions are being identified with far less false positives than previous rule-based systems were able to do. Previously, it was common for rule-based systems to have up to 20 per cent false positives. Today's supervised machine learning models such as Random Forests achieve high accuracy with highly imbalanced datasets and identify new fraud patterns using unsupervised machine learning techniques such as clustering and autoencoders.

The introduction of deep learning architectures such as recurrent neural networks (RNNs) and long short-term memory (LSTM) enables us to detect temporal trends in fast-moving retail transactions through adaptive fraud detection

© 2024 IJMRSET | Volume 7, Issue 8, August 2024| DOI:10.15680/IJMRSET.2024.0708078

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

methods that respond to changing trends in fraud tactics. At this point, approximately 90 per cent of the world's banks are implementing artificial intelligence (AI) and machine learning technologies for the purposes of detecting scams and monitoring transactions. The effectiveness of these technologies compared to traditional systems is due to the incorporation of multi-channel signals into the detection process, resulting in more dramatic reductions in false positives and enabling real-time fraud detection.

Hybrid models are another mechanism being used to further bolster the strength of models used in AI fraud detection by combining the interpretability of supervised models with the novelty detection capability of unsupervised models. Companies like Feedzai and BBVA are also processing millions of events each week, using adaptive baselines to detect synthetic identities or account takeovers before they happen.

Probabilistic modelling techniques, especially Monte Carlo simulations, are being applied to help define the level of risk associated with the use of AI for fraud detection. Fraud risk is being defined for a wide variety of AI usage scenarios (for example attack frequency and evasion success rates) and is being tied to the potential for financial loss in sectors such as retail banking.The models used by Citibank provide the means to estimate both value at risk (VaR) as well as the expected shortfall, through analysis of the extreme risks resulting from deepfakes and synthetic identities leveraging artificial intelligence (AI) driven Monte Carlo simulations (MCS). Citibank has demonstrated the importance of implementing AI to reduce operational losses within their organization by utilizing MCS. A different method for measuring and managing risk utilizes Bayesian networks; these networks dynamically analyze the interdependencies between various risk factors related to an organization so that expected loss can be calculated, providing for an accurate VaR on a portfolio basis. According to Citibank's MCS analysis, generative AI based fraud will continue to rise substantially within the United States between now and 2027, with significant potential loss due to generative AI identified through scenario analysis completed upon many scenarios. As a result of the volume of transactions subject to analysis and the amount of time required to create a model, MasterCard has developed a Decision Intelligence service office that is capable of processing a significant volume of transactions in a highly accurate manner. However, MasterCard will continue to face the challenge of 'model drift' within their BI models due to the ongoing need for adjustments to models that have drifted away from their original precision. In conjunction with developing MCS and BI models, MasterCard has developed a generative AI capability that streamlines the process of carrying out compliance and risk assessments. The ability to provide real-time updates and report on regulatory issues as they occur within its systems will eliminate the limitations of older systems and enable better capital management strategies.

As mentioned above, there are challenges associated with the implementation of current AI fraud detection systems, which are primarily due to issues associated with operating on fragmented technology stacks that do not enable interaction of separate machine learning (ML) models for behavioral analytics and anomaly detection. Because of these limitations, operational inefficiencies and delays are present within retail banking due to the inability to meet Basel III compliance obligations. By utilizing a unified framework, known as Nautilus, banks can more easily adapt a framework that captures the non-functionality of their banking systems, without having to modify or redo core logic and the result will be the enhancement of the speed and manner in which new features can be rolled out. In addition, regulatory developments have made the merging of the generic features across all products more challenging, which has created additional difficulties in the scalability and continued upgrading of emerging risks due to the limitations of historical silos. Nautilus will help eliminate these challenges by creating abstracted layers that will provide general enhancements across Nautilus, standardize integrations, and allow for the addition of modular enhancements. There are also many opportunities to quantify AI driven risks as they relate to synthetic identity fraud, which will generate, or potentially generate, a significant amount of losses for financial institutions. By providing unified monitoring to eliminate false positives and fraud losses, Nautilus-like technologies will allow institutions to proactively grow and adapt within compliant AI ecosystems [11].

III. SYSTEM ARCHITECTURE

Nautilus is developing a layered, modular-based structure to provide an Enterprise Risk Management (ERM) Framework. This Framework is based on the notion of creating and maintaining Risk Management Applications and Capabilities. This Framework employs Domain-Driven Design (DDD), Externalised Non-Functional Services and a RESTful (Representational State Transfer) Web Service architecture. This Architecture has three Elements:

© 2024 IJMRSET | Volume 7, Issue 8, August 2024| DOI:10.15680/IJMRSET.2024.0708078

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

- **Core Framework Tier -** the Tier is intended to house the application logic.
- **Integration Tier** - to provide a means of Custom Adaptor Development and Integration via the Phased Control Handoff Model.
- **Deployment Tier** – it is designed to support a Dark Deployment approach; i.e. Zero Downtime Upgrades via SVN-based Versioning to enable multiple Code Streams to grow rapidly as Basel-compliant implementations in the Middle East.

The Architecture development began with proving out Technologies for developing scaled applications, including selection of Java as the Language of Choice. The RBAC Module and Frontend Frameworks were developed separately, with the intention of allowing Custom Client Development Hooks to be added at a Later Date. The Development Process employed Dark Deployment techniques and Iterative Development Methodologies to ensure that existing Implementations were not Disrupted. Effectively, the Iterative Development Process Minimised Disruption to clients during the Migration, while isolating and developing Adaptations for Non-Disruptive Refactoring.

During the final Phase of the Development Cycle, Implementation of the Architecture was performed at the National Bank of Umm Al Qaiwain, including address-specific local conditions and Configuration of access rights for all users based on their Group designations. Validation of changes was completed in Phases prior to Scaling Up the Architecture. Ultimately, the Development Cycle was performed to ensure that the Implementations of Applications met the Banks' overall expectations without the need to Deploy Additional Code. The Architecture impact includes Reduction in Time to Market, meeting Banks' Expectations without the Need for Additional Code Deployments, and Rapid Implementation of Regulatory Upgrades with Increased Revenue Growth and Client Acquisition Opportunities across the area. Technical challenges related to the Architecture were addressed through Comprehensive Testing of the Architecture and dark running of the Applications to ensure that all Production Users were supported without a Disruption occurring. See Figure 1 below.

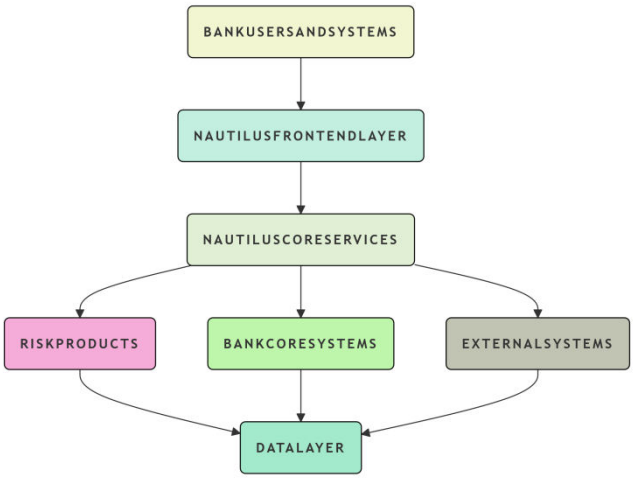

Figure 1: Nautilus Framework Architecture

1. Centralised Repository with RBAC engines and their corresponding pluggable hooks for each product at the Core Framework Layer.
2. Custom adapters for External (e.g. Workflow Tools) integrated tools at an Integration Layer → The ability to phase and transfer controls from the application to the customer.
3. Users do not require any additional resources to manage workflow management, SSO(SAML/OAuth), reporting engines or notifications for managing Day-to-day operations, thereby minimising product overhead through a Non-Functional Abstraction layer of the Application.
4. The Deployment Layer allows Customers to perform Daily/Continuous Deployment of their products using Dark Deployment, which provides zero downtime and SVN-based version control for Vanilla & Customer Streams.

© 2024 IJMRSET | Volume 7, Issue 8, August 2024| DOI:10.15680/IJMRSET.2024.0708078

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The most important elements of a specific architecture approach to improving operational efficiency and achieving Basel compliance in the Middle East are highlighted. Benefits from this include reduced redundancy, a reduction of previously siloed goods, and faster Basel Rule implementation - all critical in driving growth for the region. The Development Approach emphasises an iterative/staged approach to minimise disruption to existing production deployments. Demonstrations of Proof of Concept to demonstrate compatibility and effectiveness of JSF/Spring/Hibernate technology stack will support that any solution developed will be practical and sound for an ongoing Full-scale Deployment.

Integration flows also illustrate several Key Processes (e.g. User Authentication) which include Product-Specific Authorisation and Single Sign-on leading to Bank User Access and Nautilus Role-Based Access Control. Nautilus is the orchestrator of Workflow execution for Product Requests and facilitates hand-off between external processes and adapters. Real time Monitoring through Event Releases generating Alerts or Reports into Nautilus and Dashboards providing Basel compliance. An SVN Branching strategy supports phased Activation of Product Releases without interruption to Service (i.e. Dark Deployment).

Notes for the Technical Audience focused on the use of Framework Hooks to create pluggable Interface, the ability to Share Context via Standardised Payloads between Nautilus and External Systems and Version Control of Vanilla vs Customer Solutions via SVN Streams.

- Phase 1 – Core Build and Framework Selection: We selected Java as the Scalability Language; we delivered our first RBAC Module built on Vanilla Codebase suitable for Client Modifications.
- Phase 2 – Technical Lead for Integration: Adapters were built for External Systems using Dark Deployments - minimizing Divergence; we isolated Nautilus's framework hooks to refactor them as Necessary.
- Phase 3 – Customer Deployment At National Bank of Umm Al Qaiwain: Site-Specific challenges resolved; Configuration of an RBAC Implementation; Phased Roll-Out of Users - with the outcome of Improved Time-to-Market as measured against the Bank's Expectations without additional Development Hours required. The progress achieved under this phase enabled Future Basel and other Regulatory Evolutionary Modifications and allowed us to Mitigate Testing Issues through methods such as Mocks and Dark Runs to Avoid Interruption of Production Operations.

The Architectural Framework supports the use of Asynchronous Communication through the Use of Messaging and REST APIs whilst being focused upon Functional Logic. Security, Workflow and Notification Logic are developed/managed through Framework Hooks and Dark Deployment Practices are Facilitating the Phased Release of Features therefore, having no impact on Production Systems and Development. The Solution has incorporated Modularised Adapter Extensions and Stateless Services that will allow Scalability as well as prioritizing the New Customisations of Banks and Regulatory Enhancements established by the Banking Sector as illustrated in the below Figure 2.

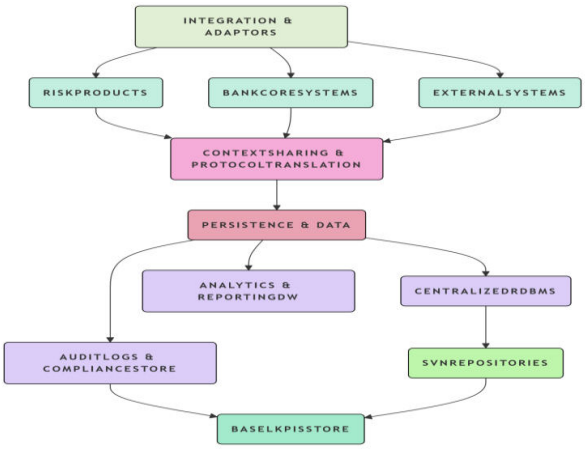

Figure 2: Nautilus Architecture - Layered Component Diagram

© 2024 IJMRSET | Volume 7, Issue 8, August 2024| DOI:10.15680/IJMRSET.2024.0708078

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1. **UI Component Layer for Presenting Information:**
- Mobile and internet banking portals that utilize JSF as the primary framework for the user interface.
- Administration for user, product and feature repository management is centralized.
- Banks can authenticate users through Single Sign-On (SSO).
- Role-based access controls (RBAC) are in place across all modules.

2. **Services Core Framework Layer:**
- Authorization engine offers configurable hooks for RBAC.
- Workflow engine allows banks to customize processes.
- Reporting engine provides regulatory dashboards in compliance with Basel and customizable reports.
- Notification services provide banks with connection to internal and external alerting systems.
- An Event bus/message queue (Kafka/RabbitMQ) for asynchronous component communication.

3. **Integration and Adaptor Layer:**
- Seamless connections with:
  - Core banking systems (CRM/CDP, transaction DB, core bank).
  - Risk Management Products (loan processing, credit assessment, & fraud detection)
  - External systems (credit origination, third party workflow tools, & regulatory reporting)
- Provides a protocol translation and context sharing capability for heterogeneous legacy systems.

4. **Data Layer and Data Persistence:**
- Provides centralized relational database (Hibernate ORM on PostgreSQL/MySQL) containing user, configuration, & product data.
- Log and compliance data are stored.
- Provides data warehouses for analytical purposes and reporting per the Basel standards.
- Standard and customized product version management repositories (SVN).

The performance measurements for banks focus on rapid fraud scoring i.e. less than 200 milliseconds for reaction time and 1.8 million transactions per hour. The system has low latency (less than 5 milliseconds) between layers and can support more than 10,000 concurrent users. The scalability metrics indicate that if horizontal pods are added, the capacity can be increased by 20%, and automatic scaling can be completed in under 60 seconds, while achieving a target of more than 5,000 transactions per second through the database.

The reliability metrics have established a goal of 99.99% uptime with established recovery objectives relating to minimal data loss and a low false positive rate for fraudulent alerts. The business impacts metrics demonstrate the degree of improvement post-enhancements including reduced time to market and time to execution as well as zero-cost customization. The security and regulatory compliance metrics are focused on comprehensive activity logging and timely updates for regulatory compliance. Performance indicators on the Gloria Dashboard indicate strong performance on metrics measuring reaction time, error rate, CPU usage, memory usage, database connection, and accuracy of fraud detection. Collectively, the system has achieved a number of success constraints including rapid deployment and compliance monitored through Prometheus and Grafana for continuous performance evaluation.

Measurements of system improvement as compared to the previous measurement, demonstrating substantial improvement in various areas of business operations. The reaction time decreased from 450 milliseconds to 180 milliseconds, which is an extraordinary improvement percentage of 60%. The throughput was increased from 0.8 million to 1.8 million units, equating to a 125% increase. Additionally, the time to market was reduced from 180 Days to 45 Days, a remarkable 75% improvement. The false positive results decreased from 15% to 2% or an 87% reduction. Further, the deployments per quarter increased from 2 to 12, which is a 500% increase. Excel should be utilized to create a visual representation of this improvement, communicating the return on investment (ROI) to stakeholders of the Nautilus project as depicted in figure 3 below.

© 2024 IJMRSET | Volume 7, Issue 8, August 2024| DOI:10.15680/IJMRSET.2024.0708078

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

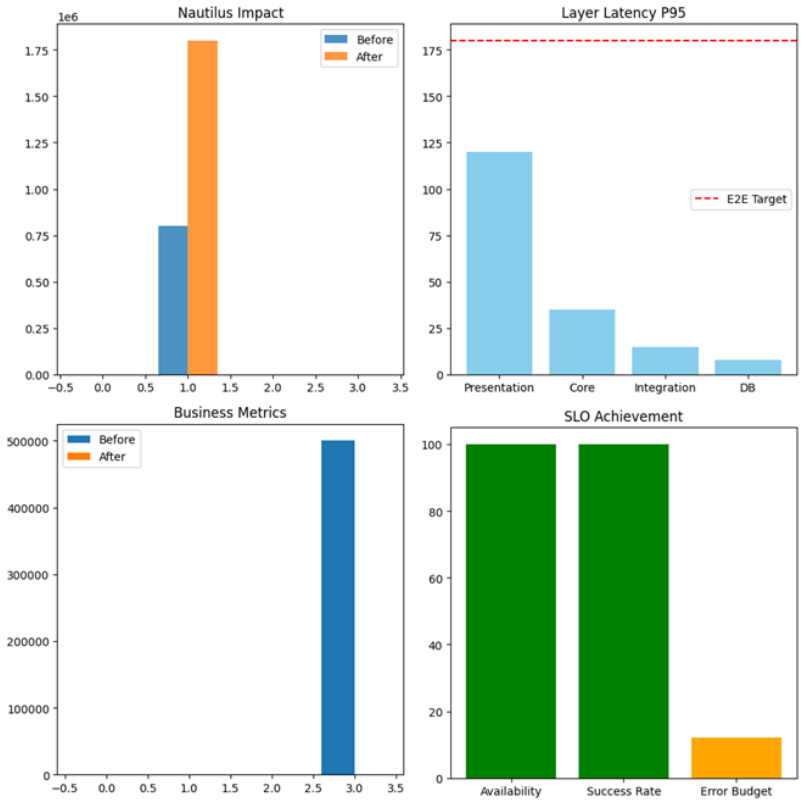

Figure 3: Nautilus Architecture Metrics Dataset

IV. CONCLUSION

While the banking industry was operating under both Basel II/III standards and local variations, the industry was still to face issues as a result of the various disparate product portfolios offered by banks and the antiquated technology used to operate the diverse technologies offered by banks creating obstacles in the ability to customize and integrate products. The need was seen for a comprehensive solution to the industry to eliminate these issues through an abstraction of non-functional performance utilized by Nautilus to allow products to focus on functional improvements thereby improving the ability of Nautilus to support bank modifications through streamlined development timeframes and costs, eliminating redundant processes and enabling teams to respond to financial institutions requirement for new code to deploy. In addition, Nautilus aided in meeting banking regulations, which has significantly improved the ability to generate additional revenue as a result of the efficiencies achieved through the implementation of Nautilus. In closing, Nautilus has accomplished the ability to integrate bank applications through resolving the integration barriers created by developing the operational processes of Nautilus while maintaining operational business continuity and by placing an emphasis on the technical implementations, including the selection of the stack used to build Nautilus and the phased roll-out of Nautilus applications.

Looking forward, the vision for Nautilus includes: migration to a Cloud Native Environment for scalability, using Artificial Intelligence (AI) and Machine Learning (ML) for enhanced Fraud Detection, providing a Fintech collaboration API First Ecosystem, and adopting a Zero Trust Security Framework. Nautilus' vision also includes the ability to address Real Time Compliance to support international growth, enhance Proactive Threat Modeling, and Automated Customization. By providing these capabilities, Nautilus has positioned itself to be a Application Development Framework Solution that provides Resilience, simplifies the infrastructure complexity and encourages Financial Innovation within the Financial Ecosystem while continuing to maintain its Leadership and Competitive Edge within the Financial Services Sector.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

REFERENCES

1. "Building the Case for Project Risk Management: Advantages and Challenges", Kate Eby, June 8, 2022, https://www.smartsheet.com/content/project-risk-management-benefits.
2. "Financial institutions and nonfinancial risk: How corporates build resilience", Björn Nilsson, Thomas Poppensieker, Sebastian Schneider, Michael Thun, February 28, 2022, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/financial-institutions-and-nonfinancial-risk-how-corporates-build-resilience.
3. "Risk Management in Banking: Types & Best Practices for Mitigation", January 10, 2024, https://www.unit21.ai/blog/risk-management-in-banking.
4. "The value in digitally transforming credit risk management", July 2016, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20value%20in%20digitally%20transforming%20credit%20risk%20management/The-value-in-digitally-transforming-credit-risk-management.pdf.
5. "Impact of Artificial Intelligence on Fraud and Scams", December 2023, https://www.pwc.co.uk/forensic-services/assets/impact-of-ai-on-fraud-and-scams.pdf.
6. "Generative AI is expected to magnify the risk of deepfakes and other fraud in banking", Satish Lalchand, Val Srinivas, Brendan Maggiore, Joshua Henderson, 2017, https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html.
7. "What banking directors should ask about AI and machine learning risks", Vidhya Sekhar, Bill Hobbs, 19 Oct 2023, https://www.ey.com/en_us/board-matters/banking-risks-from-ai-and-machine-learning.
8. "AI Why AI is both a risk and a way to manage risk", Jeanne Boillet, 01 Apr 2018, https://www.ey.com/en_gl/insights/assurance/why-ai-is-both-a-risk-and-a-way-to-manage-risk.
9. "Modern Risk Management for AI Models", Rajosik Banerjee, Matthias Peter, 2022, https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2022/07/modern-risk-management-for-ai-models.pdf.
10. "AI-Powered Banking in Revolutionizing Fraud Detection: Enhancing Machine Learning to Secure Financial Transactions", Prem Kumar Sholapurapu, 2023, https://doi.org/10.70135/seejph.vi.6162.
11. "What banking directors should ask about AI and machine learning risks", Vidhya Sekhar, Bill Hobbs, 19 Oct 2023, https://www.ey.com/en_us/board-matters/banking-risks-from-ai-and-machine-learning.
12. "What are SLOs? How service-level objectives work with SLIs to deliver on SLAs", Saif Gunja, November 18, 2022, https://www.dynatrace.com/news/blog/what-are-slos/.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com