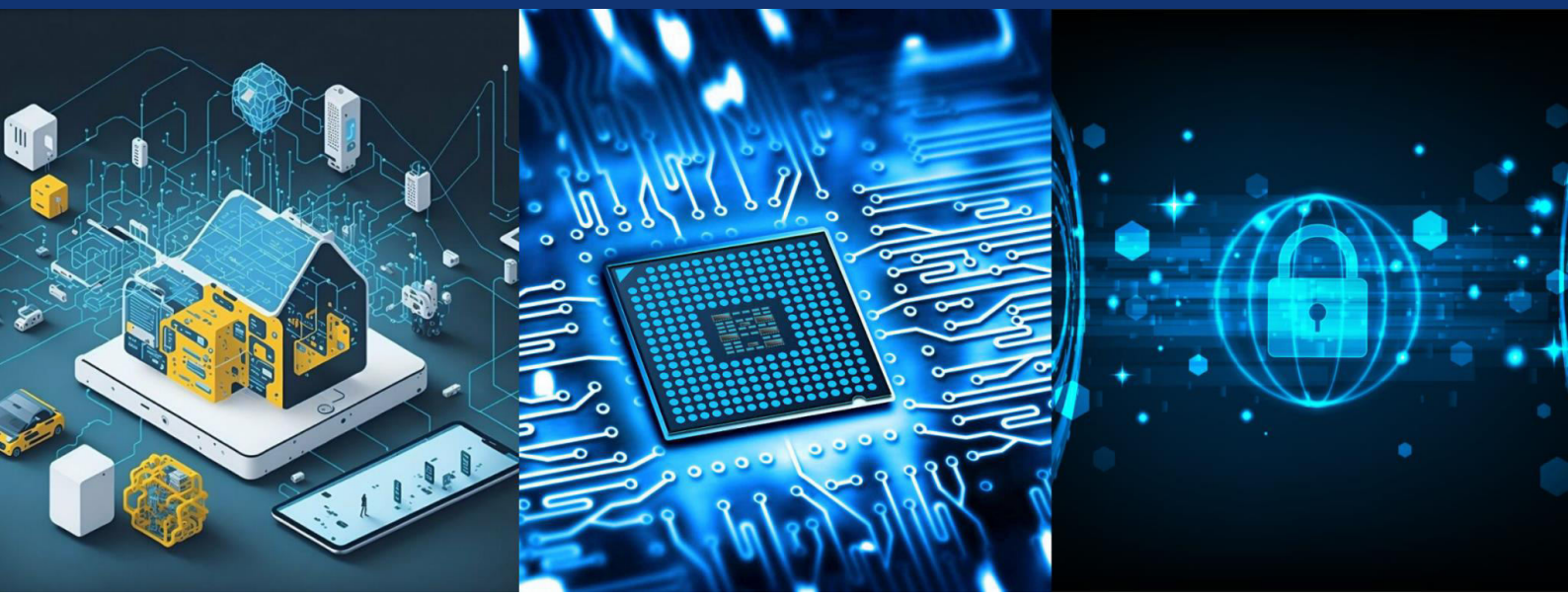
IJIRCCE

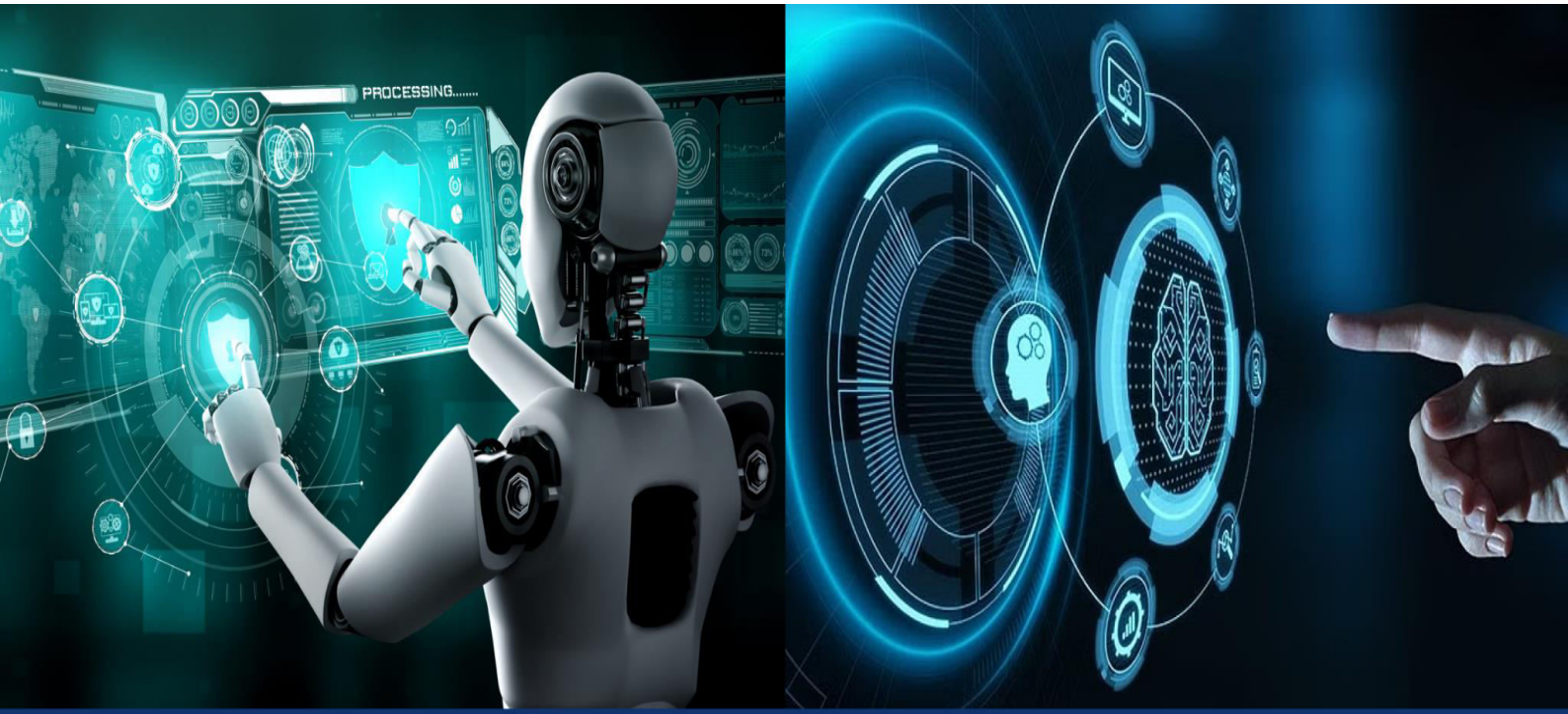
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

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



Impact Factor: 8.625

Volume 13, Issue 1, January 2025

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301165

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

Comprehensive Audit Data Pipeline Architecture - Strategies for Modern Banking Audit, Compliance and Risk Management

Mohan Kumar Sonne Gowda

Senior Audit Manager, HSBC Bank N.A., USA

ABSTRACT: The Institution Bank, which has over $2 trillion in assets, is one of the largest Bank & Financial Services Organizations in the world, classified as one of the largest Global Systemically Important Banks (GSIBs). Strong auditing capabilities are critical for managing an organization's risks and ensuring compliance with regulations and operating effectively. In this session, we will describe a holistic audit data pipeline that combines Audit Data Pipeline Architecture, Audit Data Analytics (using Python and Alteryx), and the overall direction of the IIA standards as specified by the Institute of Internal Auditors. The architecture incorporates machine learning for predictive analytics, multi-source data intake, and transformation through ETL and the identification of the conflicts of interest. Performance metrics metrics such as throughput, latency, error rates, and data quality are considered to improve the performance of the pipeline. Visualizations and example datasets demonstrate effective audit monitoring workflows. The structured Audit Data Pipeline Architecture provides the audit function a comprehensive structure to find control deficiencies and meet continuous monitoring expectations within banking environments while meeting regulatory expectations of G-SIBs. Recommendations for future improvement of the pipeline to improve controls amidst the changing financial landscape, include real-time streaming, advanced anomaly detection techniques, explainable AI Models, and blockchain-based audit trails.

KEYWORDS: Global Systemically Important Banks, Risk Management, Operational Resilience, Python, Alteryx, Audit Data Pipeline, Anomaly Detection Techniques, Real-Time Streaming, AI Models

I. INTRODUCTION

The Bank is at the forefront of international banking/finance and plays an important stabilising role with respect to the international financial system's health. The Bank is also ranked as one of the top Global Systemically Important Banks (G-SIBs) in the World according to the Basel Committee on Banking Supervision (BCBS) and the Financial Stability Board (FSB). This ranking highlights the Bank's strong financial position as well as its compliance with the high international regulatory standards imposed on all G-SIBs. The Bank's total Assets are more than $2+ trillion, providing a good indication of the Bank's scale and size [1].

To be classified as a G-SIB, five key factors must be considered: Complexity; Interconnectivity; Scale; Cross-Jurisdictional Activity; and Substitutability. These five factors determine the degree of Systemic Risk that the Bank presents to the financial system as well as the Capital Buffers necessary to avoid the Bank's Collapse (failure).

1. Complexity is the degree of Difficulty an entity encounters when dealing with the Bank's Financial Instruments.
2. Interconnectivity is the Bank's ongoing relationships with other financial institutions.
3. Scale is the Bank's Total Volume of Business Transactions.
4. Cross-Jurisdictional Activity refers to the Bank's Operating Environment across Multiple National and International Regulatory Frameworks.
5. Substitutability is how easily the Bank could be replaced by another Financial Institution.

This is essential because the Collapse of a G-SIB will create Significant Disruptions to the Global Economy and Financial Systems resulting in Regulatory Reform designed to Enhance Trust and Resilience to Adverse Market Events [2].

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

As a result of the above, the methodology for categorising Systemically Important Financial Institutions (SIFIs) has been revised, creating three new criteria for classifying SIFIs: Market Relevance; Expected Risks; and Interdependence. The Criteria of Market Relevance considers the institution's share of the Market and the potential impact of Termination of the institution on its Stakeholders and the Total Market.Potential Loss determines the likelihood of a financial institution encountering losses resulting from various causes including the failure to meet liquidity requirements, financial market breakdowns, the spread of disturbances through interconnectedness and financial system participants losing faith in the stability of a financial institution. Using these criteria assists regulatory authorities with identifying potential lenders for regulatory oversight and developing supervisory programs, such as minimum capital requirements or other types of financial resources to protect against losses, for the purpose of maintaining the soundness of the financial system and monitoring systemic risks [3].

It is essential that the Bank continue to have a detailed risk management system in place since it falls under the "systemically important financial institution" (SIFI) category due to its assets and potential losses. The Bank's Investment Banking Division maintains a Control Room (CR) to serve as a conduit for all communications between various departments and the Office of the Chief Compliance Officer. The CR works to minimize the possibility of conflicts of interest between investment banking activities, equity research and other trading activities. Through the maintenance of strict information walls, the CR can maintain compliance with current industry standards on conflicts of interest, information control, equity research and provide investment banking/equity research that is free from the influence of other departments [4].

The Governance Structure of the CR is integral in ensuring that decision-making and operations are independent and effective in managing risk. Senior executives of the Bank's multiple business units form an Oversight Committee to establish policies and protocols for risk management for the CR, while the CR leadership manages all daily operations and communicates regularly with other business units, maintains compliance and discloses results to Senior Risk Officers and Committees. Dedicated teams at the CR monitor transaction risk related to multiple entities and any possible conflicts of interest, while Legal and Compliance representatives ensure the CR remains compliant with both governance and regulatory requirements. The global Control Room works across major regulatory frameworks to achieve full compliance and support their comprehensive governance of established processes on behalf of all stakeholders. Currently, the Bank is conducting a review of the global Control Room's effectiveness in relation to its governance and risk management activities. As part of this assessment, the audit verifies compliance with all applicable regulatory frameworks to ensure adherence to these regulations [5] while also building a strategic audit data pipeline architecture.

The purpose of the FSB is to establish and promote global standards for the governance of Financial Stability Board (FSB) member institutions. The International Financial Reporting Standards include Fixed-income Issuers and Investors (FII) and the Loan to Value (LTV) Regulations set minimum Capital Requirements (BC) based on risk-weighted assets; the Dodd-Frank Act and MiFID II set specific requirements for the governance of derivatives markets and protect investors. The Sarbanes-Oxley Act (SOX) provisions for governance of the accuracy of the bank's financial reports further illustrates a comprehensive framework of Balancing Governance and Risk Management Practices.

Currently, the FSB has put forth their operational guidelines regarding the governance of Systemically Important Financial Institutions (SIFIs), while the Bank Control Room acts as a framework for the Bank to bring together the major global regulatory frameworks in order to optimise governance, compliance, operational resilience and reporting processes. In summary, the Bank Control Room supports EXCEL in managing enterprise risk and when the various global regulatory frameworks are used effectively, they will elevate the Bank to the highest levels of TRUST AND CONFIDENCE from its customers and stakeholders [6].

The Bank is currently working to enhance its capabilities to comply with 'Best Practices' for governance and risk management; therefore, the Bank will assess its current management practices as it relates to enterprise risk management. For example, as part of this assessment, the Bank will highlight practical management techniques for avoiding conflicts of interest in investment banking. The Bank will also perform a comprehensive analysis of the data used to support its operational controls. The purpose of this assessment is to provide the Bank with the tools it needs to improve processes within its EXCEL enterprise risk management systems, correct processes already in place, protect clients and ensure compliance with all regulatory requirements. All these objectives are critical to developing and maintaining a high degree of TRUST AND CONFIDENCE between clients and stakeholders globally [7].

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

II. RELATED WORK

Peer-reviewed academic articles related to banking compliance and risk management use various research methods, such as empirical analyses, case studies, qualitative studies, evaluations of the impact of regulatory changes, and systematic literature reviews. Such research methods encompass many aspects of the complexity inherent to meeting global compliance obligations related to banking, specifically Basel III (the current global framework for capital adequacy), anti-money laundering and know your customer compliance, the Sarbanes-Oxley Act's regulations on corporate accountability and transparency in accounting, the European Union's General Data Protection Regulation (GDPR), and larger financial institutions' compliance with operational risk laws. Most empirical research studies have focused on providing quantitative measurements, such as capital adequacy ratios, transaction monitoring accuracy, and breach incidence rates, to evaluate the effectiveness of an institution's compliance efforts using econometric models for determining the impact of regulatory reforms (e.g., Dodd-Frank Act) and new investment regulations (i.e. MiFID II) on institutions. The limitations related to these studies include data privacy considerations, the presence of multicollinearity caused by macroeconomic factors, and issues related to causality when quantifying the regulatory impact of mitigating risks such as reduced non-compliance penalties and increased liquidity coverage ratios (LCR) [8]. Qualitative research adds to the body of knowledge regarding quantitative studies, and, as suggested by the Federal Reserve in its supervisory guidance with respect to institutions that have $50 billion in total consolidated assets (SR 08-8), such research is often conducted using case study approaches that seek to identify the root cause(s) of an institution's noted compliance deficiencies and successes. By examining firm-wide risk management frameworks, internal control systems and governance models, qualitative analyses reveal valuable insights about how an institutional entity behaves. Similar to using case study methods to validate/highWhile self-reported biases and difficulties with extrapolating results across different regulatory jurisdictions (for example, comparing between U.S. Office of the Comptroller of the Currency OCC and European Union European Banking Authority EBA) are impediments to drawing conclusions from this research, the results contained in interviews with compliance officers and regulators show that there are cultural barriers when it comes to responsibility for taking on risk and also how effective training programmes are within the context of this research [9].

Regulatory and policy review studies are essential to systematically evaluating issues such as Basel III's capital buffer, BCBS 239's principles for risk data aggregation, and application of RegTech for automated compliance. These studies provide a means for tracing the evolution of the integration of governance models into an integrated governance approach, merging the functions of compliance and enterprise risk management ERM by consolidating supervisory reports, enforcement actions and outcome of stress tests into a single view of an organisation's risk management process that includes market, credit, operational, and compliance risks. These methodologies support the growing literature on the broadening of risk-based approaches by placing emphasis on the risks associated with major areas of risk, such as AML transactional scrutiny, and therefore increasing organisational resilience while raising concerns regarding fragmented information systems, disparate regulatory enforcement, limited resources to scale controls, and the need for advanced analytical capabilities for real-time monitoring. Finally, from a practitioner and survey-based methodology perspective, it is possible to gain insights into the challenges of implementing effective compliance procedures.

An event study approach to estimating compliance violation fines (for example under the General Data Protection Regulation (GDPR) or Foreign Account Tax Compliance Act (FATCA)) provides valuable insight, and surveys of risk committees and compliance departments outline the challenges they experience in their firmwide compliance initiatives (e.g. difficulties in merged affiliate transaction monitoring with fair lending evaluations). Recent research methodologies take into consideration technological advancements, including the evaluation of AI anomaly detection, automated reporting under Sarbanes-Oxley Act SOX 404, and BCBS 239 dashboards [10]. However, even with these research methodologies' advantages, there are still barriers that need to be addressed; these include self-reported governance performance bias, difficulty separating compliance consequences from market effects, variations between jurisdictions, and limitations on access to internally private risk data.

Nevertheless, the research agrees that there are best practices when considering RegTech implementation, strong training protocols, and the development of structured processes for identifying and monitoring operational risks; it advocates for an integrated, technology-enabled compliance process that encompasses all operational risk domains, including SOX internal control automation, AML transaction monitoring, and liquidity reporting to assist banks in navigating the complexities of regulation and enhance confidence from stakeholders and promote systemic stability.

© 2025 IJIRCCE | Volume 13, Issue 1, January 2025| DOI: 10.15680/IJIRCCE.2025.1301165

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

III. SYSTEM ARCHITECTURE

Audit utilized multiple traditional and advanced data-driven methods per the IIA's International Professional Practices Framework for improving impact and identifying risk; The audit was performed by employing a logical, risk-based method and completing significant planning, sampling/testing of controls, evaluation of controls and development of quality reporting in order to use multiple auditing methods including but not limited to: substantive testing; walk-throughs; control testing; and analytical review, to assess the governance/risk/control environment for governance/risk/control (GRC) and data was collected and processed/analysed with various platforms/tools including Alteryx/Python to enhance the efficiency/accuracy of audit processes. Subsequently, an ETL (extract, transform, load) pipeline was built using a combination of existing software APIs and custom build scripts using Python programming language to automate data collection and processing for all loan and transaction activities from many different sources which allows for improved data quality and consistency due to transformation (E/T/L pipeline). Also, custom script created in Python will automate data quality checking and identify anomalies based on historical trends observed through interactive dashboards and predictive analytics/machine learning dashboards being used for more proactive GRC forecasting/and decision making/developing business rules for managing risk.

Audits were managed throughout their lifecycle: from planning, execution through to issues tracking, change management and reporting while working collaboratively with teams in other locations. Task assignments were considered based on team member's skills to balance workload and produce higher quality outcomes. Key indicators were monitored to maintain alignment on project goals and timelines. Proper collaboration with senior leadership ensured alignment on audit priorities and needed technology while building relationships through ongoing communication with stakeholders. During the audit process, audit leadership sought to support and develop continuous training of team members in data analytics and best practices for ongoing performance improvement. This broad-spectrum monitoring and team training supported the audit staff's consideration and improvements of control deficiencies and data vulnerabilities, when the models and tools were later published as continued use outside of periodic audits to improve controls and data deficiencies, aligned with the IIA competence framework audit activities for supporting risk auditing and stakeholder management [12].

The audit activity may be seen as a multi-layer flow chart is depicted in below Figure 1, with arrows to depict the order and phases associated with data's transportation and processing. The figure depicts distinct channels (i.e. processes for each category) to capture dates inception, transformed data, analytic data and reporting. This framework is mindful of best practices associated to conducting audits, ensuring that other key factors are prioritized into the architecture such scalability, data quality, auditability and stakeholder access. Therefore, this system will not only allow for future growth but provide for continued rigor in accuracy and transparency for handling data throughout the processes in shown in below Figure 1:

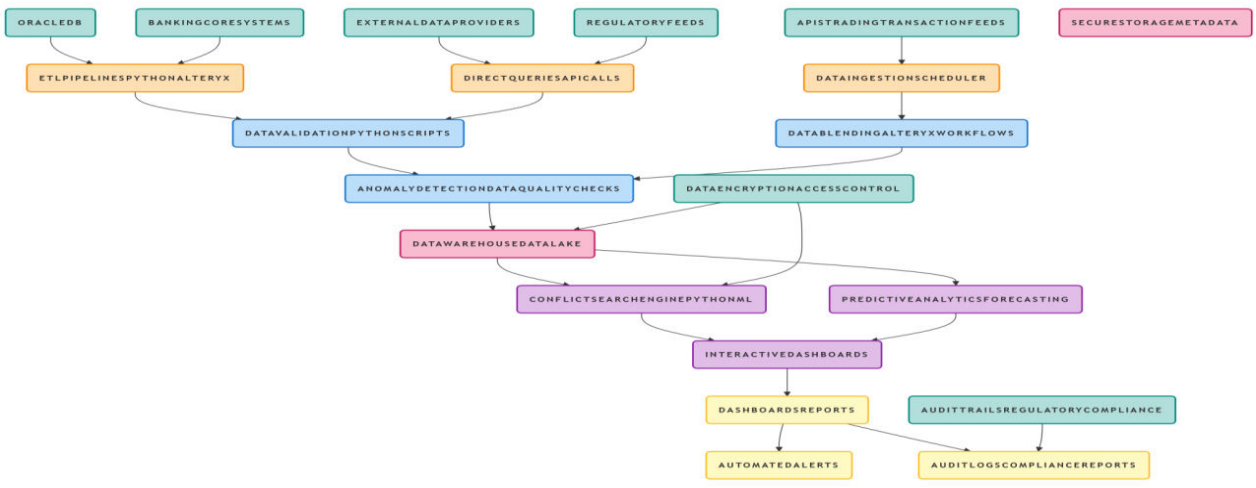


Figure 1: Audit Data Pipeline Architecture

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

1. **Layer of Data Sources:**
- A diverse set of data sources such as Oracle databases and internal financial systems.
- Data extraction performed via database commands and/or APIs.
2. Layer of Data Extraction:
- A pipeline for extracting, transforming, and loading data.
- Using Python or Alteryx for the extract routines.
- The data extraction can be trip triggered or scheduled with error handling and logging.
3. **Layer of Data Transformation and Cleaning:**
- Normalizations and cleaning using Python for data enrichment and anomaly detection.
- The Alteryx for data merging and preparation.
- It will clean up inconsistent, duplicate, or missing data from all sources.
4. **Layer of Data Storage:**
- Central storage of data, likely an analytic database or data warehouse.
- Organized for analytical inquiries with data governance rules and audit trails.
5. **Layer of Analytics and Testing:**
- Audit testing methods using Python for sampling and conflict testing.
- Forecasting and predictive analytics will use machine learning.
- The use of a dashboard to follow audit indicators and report on risk.
6. **Layer of Reporting and Monitoring:**
- Accessible dashboards for audit and business companions.
- Periodic and real-time reporting on audit results and data quality.
- Automated alerts for major violations with role-based access control.
7. **Layer of Cross-cutting Governance and Security:**
- The enforcement of data security rules, including restrictions and encryption.
- Compliance with internal auditing and regularity procedures.
- Extensive audit trail recording including data pipeline versioning.

Audit Data Pipeline Architecture diagrammatically depicts the components used to transform unsorted (raw) data into useful information for audit purposes. The Data Sources Layer collects data from several locations, including regulatory feeds, APIs, external suppliers, core banking platforms, and an Oracle database. Once this information has been collected by the Data Sources Layer, it will flow into the Data Extraction Layer. Both Alteryx and Python provide Data Extraction through pipelines (scheduled processes and direct queries) and ensure reliability using logging and error-handling techniques during extraction.

In the Data Transformation & Cleansing Layer, Data Validation and Enhancement will be performed using Alteryx and Python. Data Validation consists of performing Anomaly Detection and Quality Assurance checks to ensure the data's consistency is maintained before cleaning the data, while Cleaning involves removing duplicate or incorrect entries in the data set. Once the above tasks are completed, the Cleaned Data is stored within a Centralised Data Storage Layer designed to enable Analytics and Reporting. This example highlights data integrity controls as well as Access Management to assist in providing Audit reporting and ensuring that no one can access the Central Data Storage Layer without completing either security or access assessments.

Data Analytics and Testing will be performed in the Analytics & Testing Layer via Interactive Dashboards and Machine Learning Models to derive knowledge and predictions from the data. Reporting and Monitoring Layer will distribute results to stakeholders through the use of dashboards and Automated Alerts for any Data Anomalies identified. Lastly, Cross-cutting Governance & Security measures will include Encryption and Access Control over the entire pipeline for security and to meet regulatory requirements. Overall, the Modular Design of this Audit Data Pipeline Architecture incorporates Best Practices by Integrating Checks for Data Quality and Establishing Governance of Multi-source Data to allow for Effective Risk Identification and Continuous Audit Monitoring [13].

The schema relationships and tools of the audit data pipeline illustrate the Organizational Structure of the Customers, Loans, Transactions, and Audit Control table(s); the Customers table uses Customer_ID as the Primary Key and has a One to Many relationship with Loans, where a Customer may have Multiple Loans; the Loans table stores Loan-

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

specific information, has Loan_ID as the Primary Key, and uses Customer_ID as the Foreign Key to link to the corresponding row in the Customers table; Transaction table uses Transaction_ID as its Primary Key and has a Foreign Key to refer to the Customers via Account_ID stored with the Transaction Metadata; Audit Control (optional) references both Transactions and Loans and stores Audit-related Data [14].

The different technologies needed to implement these schemas include relational databases like SQL Server and PostgreSQL, which have robust indexing and support complex queries, and analytic databases like BigQuery and Snowflake, which are useful for high-volume data and analytics. Data extraction, cleaning, and loading will use ETL/ELT tools like Alteryx and Apache NiFi. Python and Pandas will be used for model creation and data validation on new machine learning models. Overall, this schema structure provides accurate representations of data and clear internally reference-able links between data, all built in a scalable environment that will meet the demands of the audit data pipeline is shown in below figure 2:

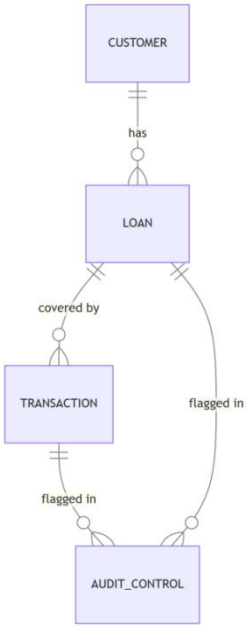


Figure 2: Schema Relationship Diagram for the Audit Data Model

Performance indicators for the Audit Data Pipeline Architecture are measurements that evaluate actions. Included in the measurements are throughput, which measures the efficiency of processing data, and data latency, which is the pace data travels for the analytics layer, which may then accelerate the speed of decision-making. The error rate is a measurement of the errors made from the processing of data; the lower the error rate, the better the data quality and pipeline stability. Data quality is an indicator of the accuracy, completeness, consistency, and freshness of the audit data that are necessary for reliable results. The Audit Data Pipeline Architecture defines the necessary components, performance indicators, and quality controls at the data quality through tables. Moreover, the tables define the operational standards and technical design of the architecture for effective, timely, and compliant processes of audit data, so that design can be understood quickly, performance can be checked, and quality assurance is performed while continuously monitoring and improving a process according to business and regulatory needs. Not only can the table verify the performance indicators, it is also a comprehensive reference guide allowing any user to evaluate and understand the overall architecture for maintaining the overall health of the pipeline and effective data governance for a globally significant bank as shown in below Table 1:

Metric Name	Sample Value	Description
Throughput	1500/sec	Records processed per second
Latency	12 sec	Time from intake to report

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

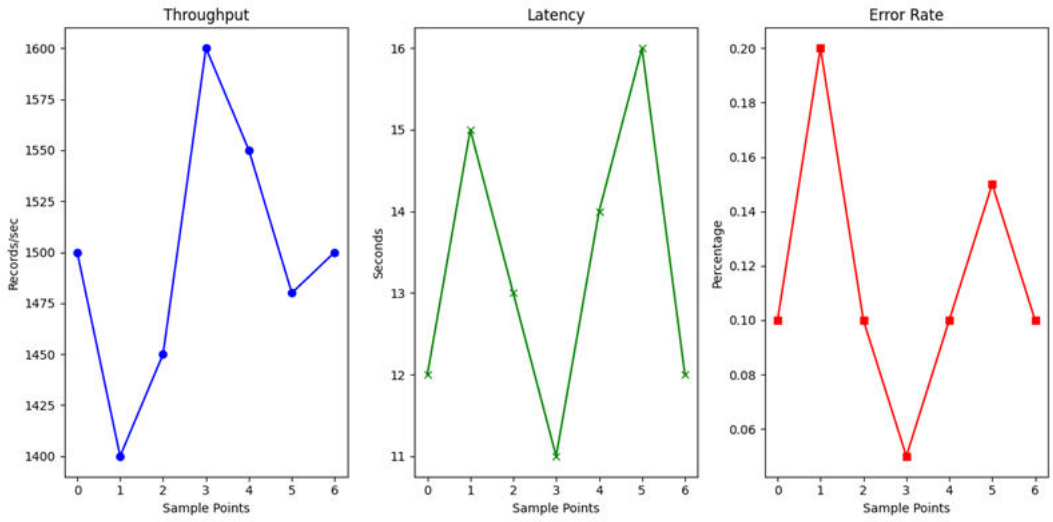
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Error Rate	0.1%	Processing errors
Data Quality	98%	Clean & accurate data
Uptime	99.9%	Availability during operations
Recovery Time	30 sec	After interruptions

Table 1: Audit Pipeline Performance Metrics (Sample Data)

System health is measured by the performance of the infrastructure to ensure potential bottlenecks do not occur, while Availability or 'uptime' is the measure to determine the pipeline is functional. Failure recovery time measures how soon automated data processing resumes to ensure the completeness of data processed within the audit data pipeline. Backlog indicates that data has not been processed, and any backlog made to the audit data pipeline may indicate various delays of the pipeline. Data drift detection provides information on how data distributions have changed which may indicate data quality issues. Last but not least, completeness of the audit trail indicates if full transparency has been made available for compliance purposes. Regularly monitoring and alerting using something like Prometheus and Grafana can allow enteprise to be proactive, and to consistently improve the audit data pipeline to meet the quality, compliance, and performance objectives.

End-to-end latency is defined as the length it takes for raw data to travel through an audit data pipeline from ingestion at the source to when it is ready to show audited insight or report. In order to measure this delay appropriately, it is necessary to have timestamps at the appropriate intervals. For example, consider tracking the moment data is ingested as well as timestamps preceding then following notable processing such as data cleansing, transformation, storage, analytics, and reporting. Once timings for data availability and ingestion are determined, the difference between them can be found to create an overall measure of the latency, while considering the latency at other stage of the processing steps in the process as well. Correlation IDs and metadata can help to find timestamps through the different components effectively. In addition, having automated monitoring and alerting can help to track latency and process issues once setup. It is also important to consider the effect of external items such as source system latencies and network delays. Putting into place and comprehensive logging with timestamps and correlations will allow organizations assess, monitor, and optimize end-to-end latency of audit data pipelines and ensure timely audited insights, as shown in below Figure 3:



IV. CONCLUSION

The architecture explains the ways to create robust audit testing protocols to align with the underlying data analytics capabilities available to auditors through the use of cloud-based and data analytic software - in particular Alteryx and Python. The architecture is designed for financial data in which extracting, transforming, cleansing and storing, and machine learning is used to identify conflicts and predict future outcomes should be systematic. Key performance

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

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

indicators (KPIs) are particularly emphasized - such as throughput, latency, error rates, and data quality, to become the metrics used to measure the success of the pipeline. The architecture provides the reader with sample data sets and visualization scripts so that they can not only monitor their data, but identify and resolve bottlenecks that can delay the completion of audits. The audit data pipeline strategy is expected to improve the effectiveness of the quality of audits and detection of risks as well as assist with providing enhanced compliance evaluations. As time goes on and as the audit pipeline grows, the ability to use both real-time data and event-driven methodologies is increased in obtaining quicker audit findings. It is possible that as analytics improve in the future, there may be even more sophisticated ways to detect risks through self-learning machine-based models, automated techniques, and the use of smart contracts based on blockchain technology to ensure compliance. Stakeholders may also be provided with an artificial intelligence-based dashboard to enable them the ability to make informed, timely decisions while correctly responding to the present banking compliance and risk-management environment.

REFERENCES

1. "2024 List of Global Systemically Important Banks (G-SIBs)", 26 November 2024, FSB, https://www.fsb.org/uploads/P261124.pdf.
2. "How to Define a Systemically Important Financial Institution – A New Perspective", Volker Brühl, 2017, https://www.intereconomics.eu/contents/year/2017/number/2/article/how-to-define-a-systemically-important-financial-institution-a-new-perspective.html.
3. "Global systemically important banks: assessment methodology and the additional loss absorbency requirement", 26 November 2024, https://www.bis.org/bcbs/gsib/index.htm.
4. "How to Implement Control Testing Programs to Mitigate Risks in Banks", Shahzad Merchant, https://www.anaptyss.com/blog/implement-control-testing-programs-banks-mitigate-risks/.
5. "Control Frameworks: A significant step towards compliance with the EU's new DORA regulations", Bradley Rees, Kevin Davies, 20 February, 2024, https://www.cognizant.com/dk/en/insights/blog/articles/control-frameworks-a-significant-step-towards-compliance-with-the-eus-new-dora-regulations.
6. "The Impact of Enhanced Liquidity Regulations on G-Sibs' Default Risk", Simon Cottrell, Jinghua Lei, Yihong Ma, Sarath Delpachitra, Natan Colombo, Dec 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5074202.
7. "Conflicts of Interest in Investment and Wholesale Banking", Daniela Strebel, Neil Cowie, 16 Oct 2024, https://www.deloitte.com/uk/en/services/consulting-risk/blogs/2024/conflicts-of-interest-in-investment-and-wholesale-banking.html.
8. "Sound and effective Compliance Risk Management in Banks", https://www.metricstream.com/insights/effective-compliance-risk-management-banks.html.
9. "A best-practice model for bank compliance", Piotr Kaminski, Kate Robu, January 2016, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/A%20best%20practice%20model%20for%20bank%20compliance/A_best_practice_model_for_bank_compliance_2.pdf.
10. "Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles", October 16, 2008, https://www.federalreserve.gov/supervisionreg/srletters/SR0808.htm.
11. "INTERNAL AUDIT COMPETENCY FRAMEWORK", 2020, https://www.iia.org.pl/sites/default/files/internal-audit-competency-framework.pdf.
12. "What is data pipeline architecture? Definition and overview", Arkadiusz Kordos, Jan 10, 2024, https://codilime.com/blog/data-pipeline-architecture-explained/.
13. "Understanding Data Pipeline Architecture", Chen Cuello, SEP 13, 2024, https://rivery.io/data-learning-center/data-pipeline-architecture/.
14. "What is a data pipeline? Best practices and use cases", Danika Rockett, https://www.rudderstack.com/blog/data-pipeline/.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details