Assuring AI in the Banking Industry

A Cognizant QE&A POV

Impact and adoption of AI in Banking industry: ‘Hype’ to ‘value-driven use cases’

It is an exciting time to be involved in the AI space, as we are witnessing a surge in innovation and creativity. The advancements in AI, especially with tools like **CoPilot, ChatGPT**, etc., have truly revolutionized the way we perceive and interact with technology. The projected growth rate of 28.46% **CAGR** from 2024 to 2030, leading to a market volume of **US$ 826.7 billion by 2030**, is a testament to the immense potential and widespread adoption of AI across various sectors *(Reference: AI Statistics: 500+ Facts Driving Global Innovation)*.

The **McKinsey Global Institute** (MGI) estimates that Generative AI (Gen AI) could add between $200 billion and $340 billion in value annually to the global banking industry. This represents 2.8% to 4.7% of total industry revenues, primarily driven by increased productivity.

Generative AI is poised to become a significant catalyst for productivity gains in the banking industry. It is expected to enhance **customer experience**, improve **risk management**, and optimize **operational efficiencies**. Banks are rapidly moving from the hype phase to experimenting with value-driven use cases, such as enabling autonomous decision-making, automated compliance procedures, AI-driven customer service bots, enhanced fraud detection through real-time anomaly spotting, and speeding up time-consuming tasks like developing code.

While the potential of AI in the banking sector is immense, the journey from fragmented pilots to a fully integrated AI ecosystem comes with its own set of challenges and risks. To truly harness the power of AI, banks need to address several key issues:

- **Generation of false or wrong information:** AI models can sometimes produce inaccurate or misleading information, which can have serious implications in the banking sector.
- **Intellectual property infringement:** AI models often use internet-based data, which can lead to copyright violations and plagiarism incidents.
- **Impaired fairness:** AI models may exhibit biases against certain groups of users, leading to unfair outcomes.
- **Privacy concerns:** There is a risk of unauthorized disclosure of personal or sensitive information.
- **Security threats:** AI systems can have vulnerabilities that may be exploited by malicious actors.
- **Performance and explainability risks:** High performance in AI systems is undoubtedly important, but without proper explainability, we risk facing a lack of trust from users, potential biases, and even security vulnerabilities. On the other hand, prioritizing explainability might sometimes come at the expense of performance, which can hinder the effectiveness of solutions.

Managing the risks associated with Gen AI is crucial as adoption scales from pilots to enterprise-wide implementation. Establishing proper guardrails and risk mitigation strategies is essential to unlock the potential value of Gen AI while avoiding serious complications such as financial, reputational, legal, and operational risks. According to a **Harvard Business Review** article, organizations need to develop capabilities to detect, identify, and prevent the spread of potentially misleading Gen AI content. This involves strict access controls, improving privacy and data protection systems, establishing proper model governance and tracking, and investing in AI ethical and security training. By institutionalizing these strategies, companies can mitigate the risks associated with Gen AI and ensure their successful and responsible adoption.their successful and responsible adoption.

Re-imagining Assurance for Gen AI

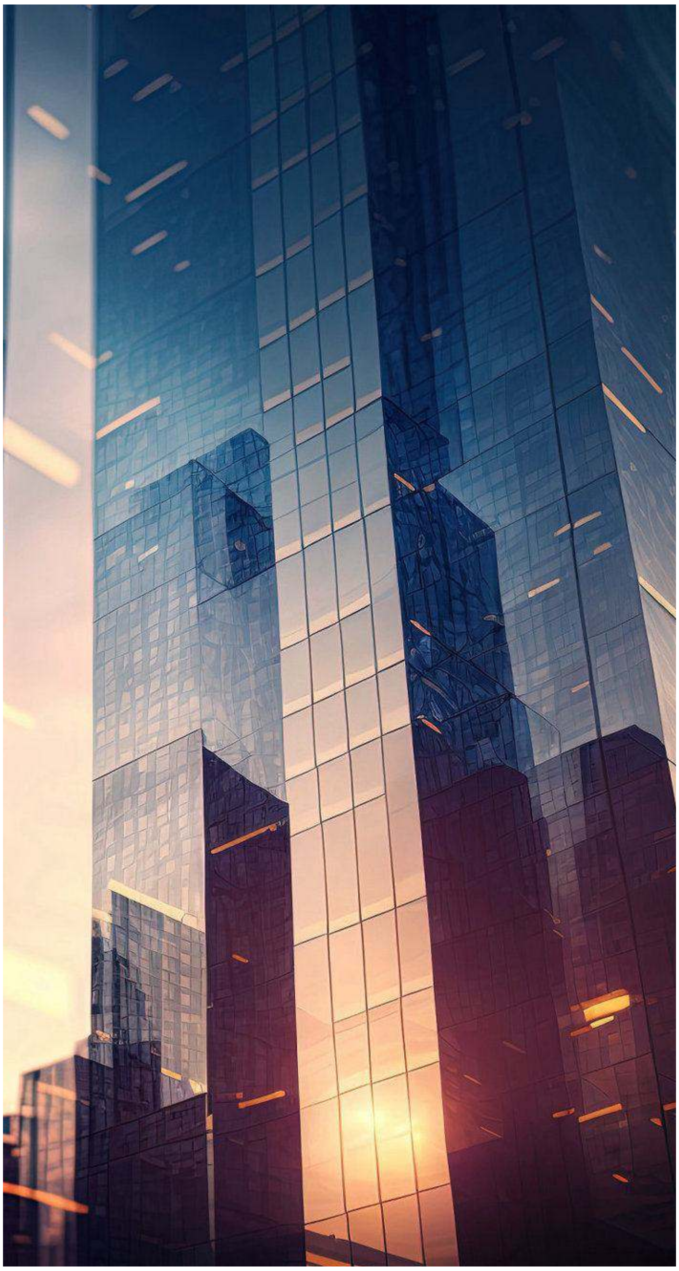
Testing of AI models will be significantly different from testing traditional applications.

Cognizant Quality Engineering and Assurance (QE&A) practice helps enterprise organizations succeed in the connected world with quality and speed. As a global thought-leader in QA with global partnerships and more than 1,000 clients across industries, we bring first-time-right quality and proven next-generation QE solutions to your business' most important initiatives.

At **Cognizant QE&A**, the **AI Assurance Strategy** plays a pivotal role in mitigating AI adoption-related risks. Banking industry being a highly regulatory industry, building this strategy around the Responsible AI (RAI) principles ensures that the AI systems are fair, inclusive, safe, secure, transparent, explainable and accountable. The RAI principles at Cognizant are designed to uphold the standards set out in the company's Code of Ethics and are built upon guidelines established in relevant legislation, best practices, and frameworks. This approach not only helps in managing risks but also fosters trust and reliability in AI systems.

Testing Gen AI models presents unique challenges due to their unpredictable outputs, complex learning processes, and potential for bias or hallucinations, requiring specialized strategies and tools. Moreover, the inherent complexities of these models introduce various quality concerns.

We often encounter issues like latency, errors, and the challenge of explaining the AI's decision-making processes. These factors necessitate a thoughtful and comprehensive approach to constructing our testing steps and plans.



Lack of clarity on what expected result is

Traditionally, testing is based on comparing versus actual outcomes. However, in the case of AI based systems, it is next to impossible to predict an expected outcome with precision.

Non-deterministic output result

Normally testers can predict the expected results for a traditional application. However, LLM-based applications can provide different responses, even with the same input. The unpredictable outcomes make traditional testing approaches, especially test automation, extremely difficult.

Sustained testing vs change driven testing

For AI models it is necessary to continuously retain the existing AI model, including to prevent AI degradation, and to adjust software to new data and inputs. Testing helps assess how well the model can work with new, unseen data. Therefore, the need to retest AI apps exists sustainably.

Test execution cost impact

Running regression tests exploratory testing, or simple sanity checks multiple times doesn't significantly affect the cost. However, every time the LLM is hit even fot Testing purposes, there is a significant cost component attached which must be taken into account from RoI perspective.

Non-functional testing

Large scale implementation of AI based systems puts AI algorithm under heavy load where they have to process large volume of data or perform complex computations. For such scenarios, rigorous stress testing of the algorithms to verify their robustness and efficiency becomes critical.

From hallucinations and unpredictable behavior to latency, errors, and the intricacies of explainability and prompt engineering, ensuring the quality and reliability of AI-powered features requires a well-planned strategy with clear focus on identifying & mitigating bias, ensuring non-deterministic reliability, assessing ethical concerns, validating outputs for accuracy and correctness, enhancing data security and ensuring conformance to NFRs (non-functional requirements). By addressing these unique challenges and leveraging specialized strategies and tools, organizations can ensure the reliability and effectiveness of their GenAI models.

Our approach of assuring AI and mitigating the risk of AI

Our framework for AI Assurance looks to test Gen AI models from four different perspectives to ensure comprehensiveness in testing:

1. **Data Quality Assurance:** Validating training and testing data for Coverage, Drift, Bias, Validity and Consistency
2. **Model Quality Assurance:** Validating model performance against benchmark measurement criteria for Prompt Performance, Model Decay, Hallucinations, Aggregated & Disaggregated Error Analysis
3. **Trustworthy AI Assurance:** Understanding the inner workings of the model under test and performing reliability checks for gauging Fairness, Explainability, Privacy and Regulatory Compliance
4. **Performance & Security Assurance:** Conducting Load & Stress tests with complex chained prompts to identify and remediate performance issues like memory leaks or inefficiencies that cause higher CPU usage. Carrying out Security Tests by using a wide variety of adversarial data and penetration tests.

Key Tenets of AI Assurance:

Pillars of Cognizant's comprehensive AI assurance strategy

Data quality assurance

Carry out tests assure training and testing data against the benchmark metrics for Data Consistency, Data Validity, Data Distribution, Bias Detection, Data Sensitivity, Data Coverage, Drift Scores and Bias Mitigations etc.

Model quality assurance

Leverage statistical and formula driven evaluation methods to compute metrics like Hallucination Degree Coefficient, Summarization, Answer Relevancy, BLEU score, Guideline Adherence, Coherence, Source Authenticity Score, Chunking Attribution, Contradiction Score, Contextual Recall, Prompt Perplexity etc.

Trustworthy AI assurance

Evaluate inner workings of the model under test by determining key metrics such as Jailbreak Deflection Score, PII Exposure Detector, Toxicity, Tonality, Ethical Compliance Rate, Fairness Score, Robustness Index, Criminality & Misogyny etc.

Performance & security assurance

Conduct load and stress tests to evaluate metrics like Prompt Injection Deflection Score, Load Resilience, Response Time, Memory Leakage. Security Testing must be carried out to identify and mitigate threats like Data poisoning, Prompt injection or Unintended cross tenant access.

Given the sheer scale and complexity involved, conducting the testing of AI models manually is simply out of question. It would be incredibly time-consuming and labor-intensive. To achieve the scale and speed of efficiencies we need, Cognizant recommends adopting a hybrid test execution approach. Harnessing **AI for AI Assurance**, using open-source LLM evaluation frameworks and coupling it with the power of test automation, we can maximize our results. This hybrid approach allows us to efficiently manage the complexity and scale of our projects while ensuring thorough and accurate testing.

Helping a Banking client assure their AI implementation

A large bank wanted to roll out an enterprise-wide AI platform aimed at democratizing the usage of AI and gain a clear market differentiation by establishing itself as the leader in AI space, accelerating engineering productivity gains and leveraging insights to benefit its customers. Cognizant partnered with the bank to provide assurance solutions for the enterprise AI platform.

We built an **Automated Natural Language Processing (NLP) powered AI Assurance Framework**. This innovative solution was designed to ensure the responsible and ethical development and deployment of AI models. Our framework emphasized key aspects such as fairness, transparency, and accountability, while also addressing potential risks and biases that may arise during AI model development.

Outcomes Delivered:

- **20+** AI models have been tested and signed off for production deployment
- **300+** issues identified across model output quality, UI & Functionality issues, API defects and Performance issues
- Significant time and cost savings

In Summary

Risk Management & Responsible AI implementation is one of the top two critical success factors reported by Gen AI high performers across the industry verticals when it comes to capturing the maximum value from this nascent technology. The importance of AI Assurance is even heightened in Banking industry due to elevated regulatory scrutiny, financial, reputational and legal risks.

As we continue to navigate the ever-evolving landscape of AI, it is becoming increasingly clear that a robust and comprehensive AI Assurance strategy and its implementation are crucial for long-term success. In fact, it's these well-crafted strategies that will in future ultimately distinguish the true industry leaders from the also-rans.

Cognizant's QE&A practice, with its deep expertise in delivering Best-in-class services to the global clients, has a well-defined and thorough AI Assurance strategy. This strategy can be customized for the client's needs, domain essence and help implement a risk mitigation strategy for the client's AI implementation strategy.

Accelerate your AI journey with confidence. Book your tailored AI Assurance assessment with Cognizant QE&A at QualityAssurance@cognizant.com —and turn responsible innovation into measurable impact.

cognizant®