Yethi
Innovation for Quality

Continuous QA

The Key to Operational Resilience And Compliance in Modern Banking

Executive Summary

Today, regulatory requirements come with rapidly evolving governance and operating models to be more effective and efficient. Technology must demonstrate agility and scalability to meet these requirements and mandated deadlines/ processes. This evolving requirement has made QA, through continuous testing, a strategic enabler for growth and continuous compliance.

Within the realm of QA, automation has become the way to go for banks for enhanced efficiency and to meet continuous compliance requirements. Testing is no longer the last step, but rather the first line of regulatory defence

Table Of Contents

How Continuous QA Drives Operational Resilience and Competitive Advantage in Modern Banking

With the speed of technology often outpacing the speed of regulations, quality assurance has shifted from a process that was primarily focused on defect detection into a proactive, front line of regulatory defence. Legacy compliance frameworks that were built for periodic or at a point in time audits struggle to govern real-time evolving systems such as instant payments. This section establishes that a strategic focus on QA is the only mechanism to mitigate systemic risk, meet regulatory demands continuously, and build customer trust in a hyper-competitive marketplace.

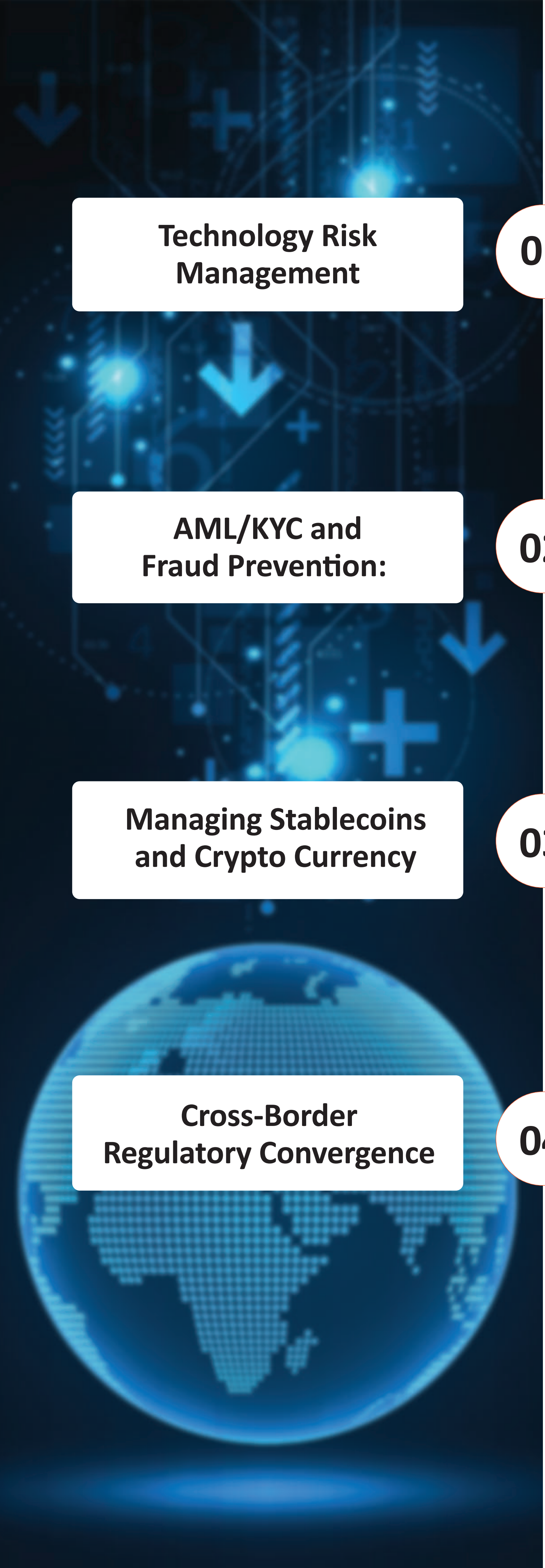
Regulatory Direction: Global Trends and Recent Changes

Today, every new regulation comes with an implicit technology assumption. Regulatory agencies are now tasked with assessing the actual technology systems and processes that enable modern day banking to exist. The Reserve Bank of India makes its position clear with a heavy focus on technology risk management, an establishment of a dedicated FinTech department, and detailed frameworks (RBI Master Direction on Information Technology Governance, Risk, Controls, and Assurance Practices) that put technology resilience at the forefront of compliance. This demonstrates how modern-day banking has reached a level where a separation from technology is not feasible.

Modern banking systems operate as interconnected ecosystems, where each financial institution and financial services provider is a 'node' of the wider system. Regulators are now looking at outcomes, resilience, and compliance not only from a system, but also at a node level. A single failure on a node such as a gateway network, fraud detection engine, or third-party integration, can have cascading outcomes that inhibit financial stability. This paradigm shift will require banks to consider different compliance strategies that consider testing the continual availability, security, and performance at the node level.

This growing emphasis is further evident with the RBI enforcing accessibility standards based on RPWD Act in 2024, or when Europeans regulators require instant payments (SEPA) to be completed in just **10 seconds**. This is direct evidence that **technology reliability is related to financial system stability.**

Notably, the shift toward a greater focus on technology **resilience is occurring across regulatory landscapes around the world.** Over the past three years, central and international regulatory bodies such as the Federal Reserve, European Central Bank, Monetary Authority of Singapore, and Hong Kong's HKMA have instituted substantial changes that affect practically every aspect of retail, corporate, and cross-border banking.



Some of the global focus areas include:

01 Technology Risk Management

Following incidents like **the 2024 CrowdStrike Falcon Sensor outage**, central banks have responded to market failures and shutdowns with stringent regulations on IT resilience, vendor management and business continuity planning.

02 AML/KYC and Fraud Prevention:

Banks globally must perform customer due diligence, screening, and suspicious activity reporting (e.g., HKMA's digital token policy, EU's AML package and US Bank Secrecy Act).

03 Managing Stablecoins and Crypto Currency

With cryptocurrency advancing to the realm of mainstream banking, many jurisdictions (e.g., HKMA, 2025; US GENIUS Act proposals; EU) have passed or proposed laws that require banks to deploy KYC and anti-fraud controls for crypto and digital assets.

04 Cross-Border Regulatory Convergence

Banks operating globally need to manage overlapping regulatory frameworks. Regulatory compliance measures (e.g., Basel III capital/liquidity regulations; EU's General Data Protection Regulation; Environmental, Social, Governance reporting requirements) constitute **overlapping and duplicative compliance** for the **modern multinational bank.**

These shifts bring a new challenge and opportunity for banking leaders. Compliance in 2025 for financial institutions is about demonstrating operational resilience, which is achieved through **comprehensive testing methodologies.** Every regulatory requirement, be it patch management, meeting performance standards, accessibility compliance, or business continuity, **depends on robust QA methodologies for successful implementation.** The institutions that thrive in this demanding environment will be those that recognize testing as mandatory for building trust with customers vis-à-vis the ones treating it like an afterthought.

The Impact on Compliance Mandates for Banks

The above regulatory trends produce tremendous demands for compliance across many fronts. Banks typically are asked to create more detailed compliance reports, real-time alerts, and/or may have to deliver compliance evidence to multiple **authorities on very short timelines**. As an example, KYC reviews on a time-sensitive basis for stablecoin holders or filing daily AML submissions can place pressure even on automated compliance systems. In parallel, the requirement for real-time monitoring (for payments, crypto flows, fraud triggers) could mean that compliance teams spend a significant portion of their daily time on monitoring systems. This places a massive burden on IT and analytics capacity from a time perspective.

Amidst all this, **compliance costs continue to be an increasing burden.** With AI adoption gradually increasing owing to its veritable contribution to higher efficiency levels, there is now an urgent need to integrate AI in compliance.

> ***Studies show that banks in the US could save over $23.4 billion in compliance costs by integrating AI compliance systems.***

However, **the upfront costs of setting up and implementing AI systems remains high.**

Lastly, compliance obligations are requiring banks to enhance data handling and integration capabilities around payment systems, customer data, transaction data, risk systems, etc. This creates new challenges around data fidelity testing and critical data security, which are essential to sustaining long-term regulatory compliance.

The Steps Banks Should Take: Addressing Regulatory Pressures

To successfully navigate the quickly changing regulatory environment, banks will need to take a strategic, proactive approach to compliance transformation.

01

With the industry moving toward instant payments and digital accounts for crypto, a key priority for banks is to **transition towards delivering real-time reporting, patching, and evidence.**

02

A strong QA and testing framework is the foundation for ensuring continuous compliance. Banks should invest in a continuous, comprehensive, functional, performance, security and compliance testing framework to confirm systems are meeting the regulatory obligations and working in a resilient manner. Testing **(Shift-left and Shift-Right)** enables teams to catch issues both in development and production, creating a trail of reliable evidence for audits.

03

Building internal expertise is critical. Banks must source and train compliance professionals for KYC, fraud and crypto regulations. New regulations in many jurisdictions (U.S., Hong Kong, E.U.) require institutions to certify employees on compliance technology, trends and latest developments.

04

With the rising compliance requirements, **adopting automation is a must**. The most successful banks now use automated evidence workflows to replace manual efforts, thereby increasing speed and remediating errors.

05

Banks must have plans for business continuity, backups, documentation, and disaster recovery processes. To truly stay compliant, banks should maintain **audit trails, logs, and documentation for any surprise audits.**

Continuous Compliance-as-Code: How Automated Testing Solves Modern Banking's Regulatory Challenges

The challenging expectations of modern banking across instant payments, real-time fraud monitoring, and patching have rendered the traditional sequential QA approach obsolete. Meeting the increasingly complex regulatory mandates around continuous resilience requires a technology-first approach. This section focuses on 'Continuous Compliance-as-Code (CCaC), which encompasses automated testing within the CI/CD pipeline. CCaC provides the necessary tactics to validate node level resilience and generate audit-ready proof such as logs and reports. Banks can demonstrate continuous resilience by embedding QA as a continuous automated discipline.

The Role of Testing in Ensuring Compliance

All the steps that banks must take; be it **maintaining technology reliability and continuity, ensuring data privacy, or preventing critical defects rely on effective testing**. If banks do not move their focus towards effective testing, they will not be able to ensure that their systems are reliable or ready for a surprise audit in the real world.

Performance Testing: Ensuring Payment System Compliance

Instant payments have fundamentally altered how banks think about risk. Traditional payment systems operated with fixed delays, which allowed for reconciliation and error correction. But with instant payments, there is no room for failure. A failure will result in an immediate breach of compliance, and the reputational damage will be significant and tough to repair.

This regulatory backdrop also enforces a framework of absolute network dependency among banks. There is no margin for downtime, no opportunity for manual intervention, and no tolerance for system failures that could cascade across the ecosystem.

As a result, performance testing must incorporate extensive full-scale ecosystem simulations in high stress scenarios now. And the regulatory implications go beyond technical compliance. With instant-payments, and interconnected banking, the regulatory test of resilience is applied not only at the level of the system, but also through the assessment of **the ongoing resiliency and availability at each node of the payments and compliance ecosystem**; be it a transaction node, a network node (APIs), or an integration point. The regulatory expectation is that no single node would become a point of failure, and therefore banks must test for and document resiliency at each connection. This is to ensure that all nodes can operate together in real time and are compliant across the entire system, particularly under peak exposure.

This is where performance testing is critical - particularly at individual connection points throughout the network. Performance testing must simulate actual operating conditions as closely as possible to be meaningful and demonstrate system behaviour during peak transaction volumes.

To demonstrate through performance testing that banking systems can maintain compliance even under stressful conditions, banks would require the following:

Real-time sanctions screening under extreme load conditions.

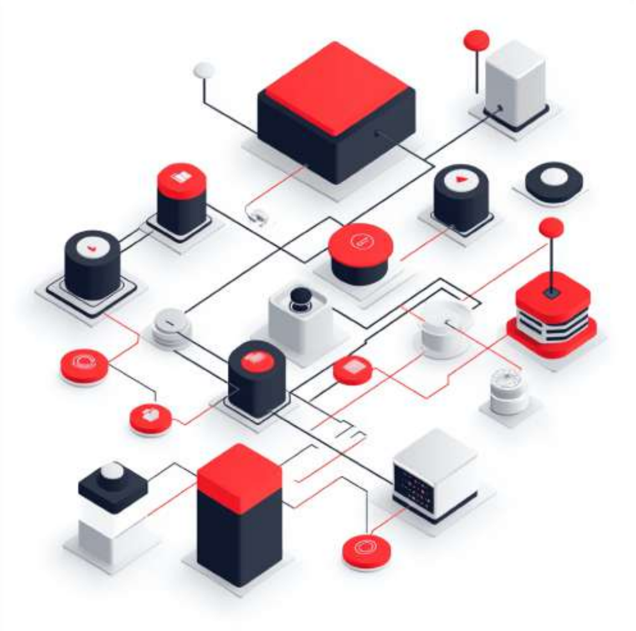
Fraud detection accuracy during high velocity transaction processing

System availability meeting regulatory uptime requirements (99.99%)

Data integrity throughout the entire payment lifecycle.

The Criticality of Patch Management and Automation

Modern banking functions with an overarching compliance paradigm. Regulatory updates are no longer rolled out in scheduled maintenance windows, but on a "real time" basis, which has profound implications for how banks manage patches and construct their testing environments. Simply put, systems that are not on the current **patches may not receive a vendor’s support;** it therefore creates a compliance risk well beyond cybersecurity, all the way to operational resilience.



Secondly, the interconnectedness of modern banking technology makes matters even more complicated, as new patches relate to and are dependent on previous patches; therefore, compliance means keeping the **complete technology stack up to date.**

Lastly, patch management in modern times is far more expansive as it extends to the entire ecosystem in which the organization is plugged in, **including the operating systems, networks, servers, databases, and antivirus system.** This creates a testing burden that simply cannot be done with a traditional patch management route.

Critical testing requirements for comprehensive patch management include:

- **Validating OS compatibility** across Windows, Linux, AIX, and Solaris environments.
- **Database Server Validation,** ensuring patch compatibility with Oracle, SQL Server, and other database platforms.
- **Network Infrastructure Testing**, validating firewall, router, and switch configurations after patch deployment.
- **Antivirus and Security Tool Validation**, confirming that security patches do not compromise protection capabilities.
- **Third Party Dependency Testing**: Validating that critical vendor services and systems maintain compliance standards and can support business continuity requirements. This includes testing backup service providers, data migration capabilities, and vendor failover procedures.

Automation serves as the only viable solution for continuous compliance. The expectation of real-time compliance capabilities drives the need for automated testing platforms that can validate regulatory adherence continuously without disrupting business operations.

The modern regulatory landscape demands **continuous patch validation through automated testing suites,** real-time compliance verification across interconnected systems, **automated evidence generation** for regulatory audit requirements, and integrated testing workflows that maintain business continuity during updates.

Automated testing platforms produce **logs, screenshots, and detailed execution records** that serve as proof during regulatory examinations. Regulators are increasingly recognising automated testing evidence because it largely eliminates human error and provides consistent, repeatable results.

In essence, automated testing platforms offer several advantages, including:

✓ *A **continuous monitoring** capability that provides real-time compliance status.*

✓ *Comprehensive **audit trails** with detailed execution logs and timestamps*

✓ *Standardised **reporting** that meets regulatory documentation requirements*

✓ ***Reduced manual effort** while improving accuracy and consistency.*

The Criticality of Security Testing

Through the process of thorough security testing, banks must show that they can mitigate unauthorised access, data breaches and/or financial fraud and comply with regulatory requirements. Newer cyber security regulations, such as PCI DSS, SOX, and banking specific security frameworks, require financial institutions to validate their security levels, which means undertaking rigorous testing methodologies.

Some important components of security testing methodologies related to regularity and compliance are:

Penetration testing, which simulates real-world cyberattacks, to identify vulnerabilities before malicious attacks exploit them.

Vulnerability assessments that systemically identify and categorise system weaknesses across the entire IT infrastructure.

Security code reviews that ensure applications meet regulatory standards and coding best practises.

API security testing for open banking and third-party integrations that meet regulatory requirements.

Network security validation that confirms firewall configurations, intrusion detection systems, and access controls function as designed.

Moreover, security testing must also encompass testing incident response procedures, breach notification systems, and recovery capabilities that meet regulatory timelines and documentation requirements.

Negative Testing is Crucial for Validating Compliance

Testing scenarios that ensure prohibited actions are blocked is critical. Negative tests provide not just the reassurance of validation to regulators that compliance controls are functioning properly, but validation to regulators that those controls function effectively even in negative situations. **This methodology demonstrates that institutions have implemented robust safeguards that prevent regulatory violations rather than merely detecting them after occurrence**. Negative test cases are relevant for scenarios like validating access controls and data privacy (**e.g., ensuring sensitive information is not accessed or moved appropriately)**, or fraud controls to validate that a suspicious transaction will trigger the proper compliance response.

Accessibility Testing

Digital accessibility is now a legal requirement. As a result of the implementation of the Rights of Persons with Disabilities Act in India, and mandated compliance with IS 17802 Digital accessibility standards, financial institutions providing digital banking services now have a binding responsibility to comply. With **1.3 billion** people with disabilities globally, compliance aligns business objectives with social responsibility, limiting legal liability.

Testing for compliance to accessibility is highly specialized:

01 **Automated accessibility scanning with WCAG compliant tools**

02 **Screen reader compatibility for users with visual impairment**

03 **Keyboard navigation for users with motor impairment**

04 **Colour contrast and resizing text to assist with complete accessibility**

Conclusion

The Strategic Takeaway for Banks

In 2025, the regulatory environment will favour banks that can display strong operational resilience via comprehensive testing practices. Mitigating the complexity of instant payments, ongoing regulatory changes, automated evidence requirements, and accessibility will fundamentally rest on testing as the basis of trust with regulators. Banks with strong testing practices will be afforded high-trust levels by regulators.

Banks that invest early in continuous automation testing at the ecosystem-level, automated audit-ready evidence, and resiliency validation at the node-level will establish confidence from regulators, partners, and customers. Conversely, banks that opt to treat testing as optional or secondary will expose themselves to not only compliance vulnerabilities, but a business interruption, reputational damage, and systemic degradation.

With Gen-AI utilization continually rising, QA will play a vital role in ensuring that the outputs are explainable. Testing will focus on identifying bias and ensure that AI models adhere to audit and transparency requirements. Banks must invest in continuous QA to build institutional trust and continue to grow through transformative technologies.

Testing is no longer the last step but is now the first line of regulatory defence.

Yethi
Innovation for Quality

About Yethi

Yethi Consulting Pvt Ltd is a leading provider of Quality Assurance, Test Automation, and Payments Modernization solutions for the global banking and financial services sector. Our mission is to ensure the reliability of financial applications, accelerating business success worldwide.

With over a decade of experience, Yethi combines deep domain expertise with a robust library of 1.2 million test cases covering 350+ financial applications. We've successfully delivered 700+ projects for 130+ customers across 30+ countries, offering a comprehensive suite of products, services, and solutions.

Disclaimer

©2025 Yethi Consulting. The content of this whitepaper is intended for informational and knowledge-sharing purposes only. Reproduction or distribution in any form is prohibited without the prior consent of the author. All external trademarks and copyrights mentioned herein remain the property of their respective owners and are duly acknowledged.