stratpoint
FAST FORWARD TO THE FUTURE

Strategic QA in Financial Services:

Enhancing Reliability and Compliance

Mastering QA to build trust and resilience in Banking and Finance



Table of Contents

3 **Executive Summary**

4 Why a Strategic QA Framework Matters in Banking and Financial Services

6 Unique Challenges of QA in Banking and Financial Applications

8 Building a Robust QA Framework

12 Transitioning to a QA Testing Center of Excellence (TCOE)

14 Optimizing QA Investment

18 Future Trends in QA for Banking and Financial Services

19 Stratpoint's Approach to QA

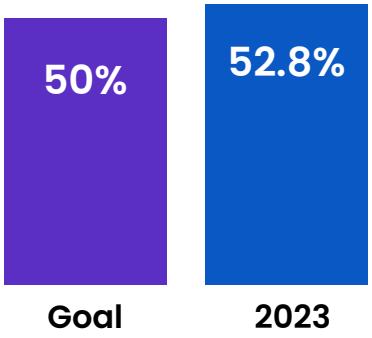
23 Quality at the Core

Executive Summary

The banking and financial services industry in the Philippines is undergoing rapid digital transformation, driven by the growing adoption of online banking, mobile payments, and fintech solutions.

According to the *Bangko Sentral ng Pilipinas* (BSP), digital payment transactions accounted for 52.8% of monthly retail payments in the country by the end of 2023, surpassing the government's target of 50% digital payment adoption. With this increasing reliance on digital financial services, ensuring the quality, security, and reliability of banking and fintech applications has never been more critical.

Digital Payment Adoption in PH



Based on the Digital Payments Transformation Roadmap 2018-2023

Quality assurance (QA) in banking and fintech applications is crucial for maintaining trust, preventing financial losses, and ensuring compliance with stringent regulatory requirements. In an environment where even a minor software defect can lead to fraudulent transactions, security breaches, or operational failures, robust QA practices are essential. The customers' demand for seamless digital experiences further underscores the need for reliable and high-performing applications.



Why a Strategic QA Framework Matters in Banking and Financial Services

Despite advancements in software development and testing methodologies, financial institutions in the Philippines face several QA challenges:



Legacy vs. Modern Platforms

Many financial institutions still rely on legacy systems that require integration with modern fintech applications, increasing the complexity of testing. Legacy applications often lack compatibility with newer technologies, making it necessary to adopt robust testing methodologies to ensure smooth interoperability between traditional core banking systems and new-age digital services.

Customer Expectations

The demand for 24/7 access to banking services means that financial applications must be resilient, high-performing, and free of defects. A single software failure can lead to significant customer dissatisfaction, loss of revenue, and reputational damage, underscoring the importance of a strong QA framework.

Rapid Digital Adoption and Scalability

The exponential growth of digital transactions requires systems to handle massive volumes of data and transactions without compromising performance. Scalability testing and performance testing are crucial yet challenging to execute effectively.

Talent Gap

Finding and retaining skilled QA professionals with expertise in financial services is a challenge. The rapid pace of technological change necessitates continuous learning and upskilling.

Regulatory Compliance

Banks and financial institutions must adhere to local and international standards such as BSP Circular No. 808 (Information Technology Risk Management for All Banks and Other BSP Supervised Institutions), the Data Privacy Act of 2012, PCI DSS (Payment Card Industry Data Security Standard), and AMLA (Anti-Money Laundering Act). Ensuring compliance requires adherence to these regulations and ongoing monitoring and updates to security protocols to keep pace with evolving legal requirements.

Security Vulnerabilities

The rise of cyber threats, such as phishing and data breaches, makes security testing an indispensable component of QA strategies. With digital transactions on the rise, the risk of financial fraud and cyberattacks has escalated, putting pressure on banks and financial services firms to continuously refine their security measures through rigorous QA testing.

A well-structured QA framework ensures that financial applications are rigorously tested across multiple dimensions, including security, functionality, performance, and regulatory compliance. This framework should encompass:

- **Automated and manual testing** for comprehensive coverage. Automated testing enhances speed and efficiency, while manual testing ensures critical edge cases are identified and resolved.
- **Agile and DevOps integration** to enable faster, more efficient testing and release cycles. Continuous integration and continuous delivery (CI/CD) frameworks can significantly reduce the time-to-market for financial applications without compromising quality.
- **Regulatory-driven QA practices** to ensure continuous compliance with evolving financial laws. Regular audits and compliance checks should be integrated into QA workflows to maintain adherence to industry standards.
- **Security-first testing** approaches to identify and mitigate vulnerabilities before deployment. Proactive security testing safeguards sensitive customer data and minimizes exposure to cyber risks.

A structured QA framework helps financial institutions mitigate risks and reduce costs from software defects by preventing prolonged development cycles, costly post-release fixes, and operational risks through shift-left testing. It also enhances customer trust by ensuring smooth and reliable digital experiences. Additionally, financial organizations prioritizing QA gain a competitive advantage by delivering seamless, secure, and efficient digital banking and financial services that meet modern customer demands.



Unique Challenges of QA in Banking and Financial Applications

High Stakes of Software Defects in Financial Services

The financial sector is one of the most heavily regulated industries due to the sensitive nature of transactions and customer data. Even minor software defects can result in catastrophic consequences:

- **Transaction failures:** System errors in fund transfers, mobile payments, or ATM transactions can lead to financial losses and damage institutional credibility. Even a short period of downtime can impact thousands of transactions, causing frustration among users and potential revenue loss for banks and financial institutions.

- **Compliance violations:** Failure to meet regulatory requirements, such as the National Privacy Commission (NPC)'s advisories and guidelines to protect personal data, can result in penalties, legal repercussions, and reputational damage. Failing an audit can also lead to increased scrutiny from financial regulators, slowing down future product rollouts and innovation.

- **Data breaches:** In 2023, the Philippines recorded the highest number of financial-related phishing attempts on business devices in the Southeast Asian region. A security loophole in a banking application could expose millions of customers' personal and financial data.

Complex IT Ecosystems

Many banks in the Philippines still operate on legacy core banking systems while integrating modern digital services. The coexistence of outdated systems and new fintech solutions creates significant QA challenges:

- **Compatibility issues** between old and new technologies. Ensuring seamless data migration and interoperability requires thorough regression testing and validation.
- **Ensuring seamless data synchronization** across multiple platforms. Data consistency and accuracy must be verified through end-to-end testing strategies.
- **Testing APIs and third-party integrations**, such as digital wallets and remittance services. A minor defect in API connectivity could disrupt multiple services and transactions.

Evolving Customer Expectations

Filipino consumers are increasingly demanding seamless digital experiences and 24/7 availability of financial services. A report by Visa showed that card payment usage (swipe, online, tap, and contactless) was at 70% while mobile wallet usage was at 87% among Filipino consumers in 2023, emphasizing the need for banking applications to be reliable and always accessible. QA teams must ensure:

- **Minimal downtime for mobile and online banking platforms**
- **High transaction speeds and optimized performance**
- **Intuitive and bug-free user experiences**

Increased Adoption of AI and Cloud in Financial Applications

Many Philippine banks invest in artificial intelligence (AI) and Cloud-based solutions to enhance digital banking services. While these technologies bring efficiency and scalability, they also introduce new QA challenges:

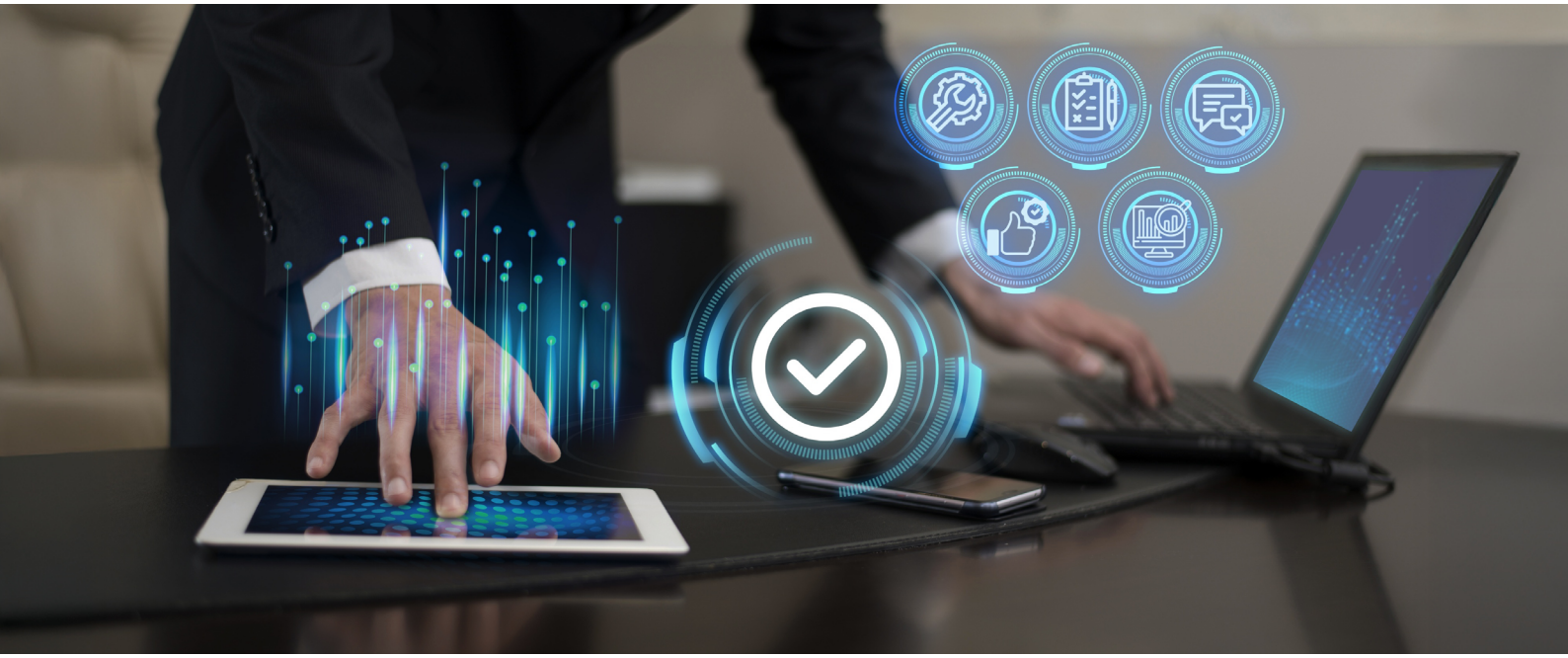
- **AI-driven risk assessment models must be tested for accuracy and fairness.**
- **Cloud-based applications require rigorous performance and security testing to prevent vulnerabilities.**
- **AI-powered chatbots and virtual assistants must be tested for reliability in handling customer queries.**

Regulatory Landscape

Regulatory compliance is a top priority for financial institutions. Philippine banks and financial institutions must adhere to certain requirements, including:

- **BSP Circular No. 808:** Mandates an information security management system to protect against cyber threats.
- **Data Privacy Act of 2012:** Requires secure handling of customer data, similar to the EU's General Data Protection Regulation (GDPR).
- **PCI DSS:** Ensures secure payment transactions to prevent fraud.
- **Anti-Money Laundering Act (AMLA):** Requires robust monitoring and reporting mechanisms for suspicious transactions.

By addressing these challenges through a structured QA approach, banks and financial services firms can enhance service reliability, improve compliance, and maintain customer trust in an increasingly digital landscape.



Building a Robust QA Framework

Banks and financial institutions must ensure their applications meet the highest standards of security, performance, and compliance while delivering seamless experiences to customers. A well-structured QA framework reduces software defects, enhances trust, minimizes operational risks, and ensures regulatory adherence. By incorporating robust testing strategies and shifting toward proactive quality management, banks and financial service providers can future-proof their digital platforms and maintain a competitive edge in an evolving financial landscape.

Key Pillars of a Strong QA Framework

To construct a resilient and effective QA framework tailored for the complexities of the financial sector in the Philippines, institutions must solidify their approach with foundational pillars. These pillars ensure not only the functionality and security of applications but also their ability to adapt to the dynamic regulatory and technological environment.

Balancing Automated and Manual Testing

Effective QA in banking and financial applications requires a balance between automated and manual testing for efficiency and accuracy. Automated testing accelerates release cycles and improves software quality by handling repetitive, high-volume tasks. Implementing data-driven testing and integrating automation into CI/CD pipelines further enhance test efficiency. On the other hand, manual testing is essential for exploratory testing, usability assessments, and validating complex edge cases. A well-rounded QA approach leverages automation for scalability while using manual testing to ensure intuitive, accessible, and high-quality user experiences.

Performance and Load Testing

As digital transactions surge, ensuring applications can handle peak loads and maintain optimal performance is critical for customer satisfaction and business continuity. Performance and load testing validates system stability under high transaction volumes to prevent outages and ensure seamless customer experiences. It also includes performing stress testing to evaluate the system's behavior under extreme conditions and using performance monitoring tools to identify bottlenecks and optimize performance.

Functional and Regression Testing

To guarantee a consistent and reliable user experience, meticulous functional and regression testing is essential to prevent defects and ensure stability. It ensures that new releases do not introduce defects and that all functionalities perform as expected.

- Implement test case management tools to organize and track test cases.
- Conduct thorough regression testing after each code change to ensure that existing functionality is not affected.
- Utilize test data management strategies to ensure that test data is realistic and representative.

Compliance Testing

The Philippine financial landscape is governed by a complex web of regulations, demanding a rigorous approach to compliance testing to avoid penalties and maintain trust. Develop a compliance test suite that covers all relevant regulations, including the Data Privacy Act, PCI DSS, AMLA, KYC, and BSP circulars. Maintain a comprehensive audit trail of all compliance testing activities.

Security Testing

In an era where cyber threats are increasingly sophisticated, safeguarding financial applications requires a proactive and multifaceted security testing strategy. Proactively identifying vulnerabilities helps prevent cyber threats, data breaches, and financial fraud. Adopt a shift-left security testing approach, integrating security testing earlier in the development lifecycle.

- Conduct static application testing (SAST) and dynamic application security testing (DAST) to identify vulnerabilities.
- Implement interactive application security testing (IAST) for real-time vulnerability detection.
- Perform security code reviews to identify potential weaknesses in the code.
- Conduct regular penetration testing to simulate real-world attacks.



Shifting from Reactive to Proactive QA

To excel in today's fast-paced fintech landscape, Philippine banks and financial institutions must transition from a reactive posture to a proactive QA strategy, anticipating and mitigating risks before they materialize.

Continuous Testing in DevOps and Agile

Embedding QA within CI/CD pipelines ensures early defect detection and faster release cycles. A continuous integration (CI) server automates the build and test process, and continuous delivery (CD) pipelines automate the deployment of new releases. By embedding testing seamlessly within the development pipeline, organizations can accelerate delivery while upholding stringent quality standar ds. Using containerization technologies ensures consistent environments across development, testing, and production.

AI and Machine Learning-Driven Predictive QA

Harnessing the power of AI and machine learning allows for the identification of potential defects before they impact users, transforming QA from a reactive to a predictive function. Leverage machine learning algorithms to analyze historical defect data and predict potential defects and AI-powered test case prioritization to focus on high-risk areas.

Risk-Based Testing

In a landscape of limited resources, a risk-based testing approach ensures that efforts are concentrated on the most critical areas, maximizing efficiency and min-imizing potential impact. Prioritizing test efforts based on risk assessment ensures that critical functionalities receive the highest level of scrutiny. Risk-based metrics track testing progress and identify areas that require additional attention.

By integrating these elements into their QA framework, banks and financial ser-vice firms can achieve greater efficiency, security, and compliance in their digital transformation journey.

Transitioning to a QA Testing Center of Excellence (TCOE)

As banks and financial institutions continue to scale their digital operations, the need for a standardized, scalable, and efficient QA approach becomes more pressing. Establishing a TCOE allows organizations to consolidate QA efforts, streamline processes, and implement best practices across the enterprise. A QA TCOE centralizes testing strategies, ensuring consistency, compliance, and efficiency while optimizing resources and reducing costs.

Benefits of TCOE

A QA TCOE serves as a centralized hub for QA expertise, resources, and best practices. By consolidating QA functions, financial institutions in the Philippines can reap numerous benefits.



Improved test quality

A centralized QA framework enhances testing accuracy and consistency. A TCOE establishes standardized QA processes, methodologies, and tools across the organization, ensuring consistency and reducing inconsistencies arising from disparate QA practices.



Improved efficiency

A TCOE eliminates redundant efforts, streamlines workflows, and optimizes resource allocation, leading to significant cost savings and faster time-to-market without compromising quality.



Scalability and agility

It easily adapts to new technologies, methodologies, and business requirements. A TCOE enables organizations to respond more quickly to changing business requirements and market demands, supporting agile development methodologies and accelerating the delivery of new features and functionalities.



Regulatory alignment

A TCOE establishes clear QA governance structures, processes, and metrics, enabling better risk management and ensuring compliance with regulatory requirements.

Key Components of TCOE

A successful QA TCOE comprises several key components that work together to achieve its objectives.

1. **Centralized governance for QA across the enterprise:** A dedicated TCOE Standardized processes also facilitate knowledge sharing and collaboration among QA professionals. This includes defining QA roles and responsibilities, establishing QA processes and standards, and implementing QA metrics and reporting mechanisms. Centralized governance ensures consistency, accountability, and transparency in QA practices across the organization.

2. **Standardized QA processes and frameworks:** By implementing industry-recognized testing methodologies such as the International Testing Qualifications Board (ISTQB), ISO, and Six Sigma, banks can maintain high QA standards and reduce defects. This ensures that QA activities are conducted in a consistent and repeatable manner, reducing errors and improving efficiency. Standardized processes also facilitate knowledge sharing and collaboration among QA professionals.

3. **Upskilling and training programs for QA teams:** A TCOE invests in upskilling and training programs to develop the skills and expertise of QA professionals. This includes providing training on new testing methodologies, tools, and technologies, as well as fostering a culture of continuous learning. Upskilling programs ensure that QA teams stay abreast of the latest trends and technologies, enabling them to test complex financial applications effectively.

A well-implemented QA TCOE helps financial institutions drive quality, reduce risks, and ensure robust software performance, ultimately enhancing customer satisfaction and regulatory compliance.

Optimizing QA Investment

As banks and financial organizations navigate the complexities of digital transformation, they must strike a balance between cost efficiency and QA. Investing in a structured and strategic QA approach ensures that these companies minimize risks while maximizing value from their tech investments.

Balancing Cost vs. Value

Investing in a robust QA framework may require upfront costs, but it yields significant long-term benefits. By preventing defects early in the development lifecycle, organizations can avoid costly rework, reduce time-to-market, and minimize the risk of production failures.

ROI of Robust QA Frameworks vs. Cost of Failures

The cost of software failures in the financial sector can be substantial, including financial losses, reputational damage, regulatory penalties, and customer churn. The average cost of a data breach in 2024 was $4.88 million globally, and financial enterprises spent 22% more at $6.08 million. The cost of fixing defects post-production can be up to 30 times higher to fix than those identified during early testing phases. Financial organizations should perform detailed cost-benefit analyses – quantifying savings from early defect detection, reduced downtime, and minimized security incidents. Leveraging analytics from tools or open-source platforms can help quantify these benefits.

Total Cost of Ownership (TCO) Reduction

Evaluate the long-term savings achieved by reducing rework, downtime, and regulatory penalties. By mapping out the TCO of current QA practices versus a more mature, integrated QA approach, decision-makers can quantitatively assess potential savings.

Strategic Vendor Selection

Choosing a QA partner should go beyond cost considerations. Banks and financial service providers must evaluate expertise, compliance, knowledge, technological capabilities, and the ability to meet the organization's specific needs to ensure long-term success.

- **Alignment with business goals**
  Do they understand your challenges and objectives?
- **Tailored solutions**
  Are the solutions customized to fit your business industry?
- **Strategic approach**
  Can they provide a technology roadmap with measurable outcomes?
- **Proven experience**
  Do they have a track record of delivering successful transformation projects?
- **Domain expertise**
  Can they match their solutions to your specific business needs?
- **Communication and collaboration**
  Are there effective communication channels and collaborative tools?
- **Long-term commitment**
  Are they invested in building a lasting partnership?
- **Global and local capabilities**
  Can they scale solutions for both local and global enterprises?
- **Agile methodologies**
  Do they adopt agile practices to ensure flexibility and rapid delivery?
- **Scalability**
  Can they adapt to your changing needs and scale as your business grows?

Learn more about selecting the right tech partner for your digital transformation journey.

Best Practices for Financial Institutions

To fully optimize QA investments, consider adopting a mix of internal best practices and external partnerships.

Implementing a Risk-Based Testing Approach

- **Risk prioritization:** Start with a thorough risk assessment to identify critical banking functionalities that, if compromised, would have severe financial or reputational consequences. Use techniques such as Failure Mode and Effects Analysis (FMEA) to prioritize testing efforts.

- **Focused testing resources:** Allocate more rigorous testing protocols to high-risk areas while automating lower-risk functionalities to optimize resource allocation. This targeted approach can reduce unnecessary testing overhead and improve overall efficiency.

Aligning QA Strategy with Digital Transformation Goals

- **Cross-functional collaboration:** Encourage collaboration between development, QA, and business teams to ensure that quality goals align with broader digital transformation objectives. For example, aligning QA efforts with customer experience goals can help in reducing churn and enhancing satisfaction.

- **Centralized QA governance:** Create a centralized QA oversight function that works closely with IT, operations, compliance, and business units. A dedicated governance model helps align QA initiatives with broader business objectives, ensuring that quality measures support both operational excellence and strategic growth. Regular review sessions and transparent reporting of QA metrics can foster continuous improvement.

Benefits of an Outsourcing QA Model

Cost efficiency without compromising quality

Outsourcing QA can significantly reduce the fixed overhead associated with building and maintaining an in-house QA team. This approach allows companies to convert fixed costs into variable costs, paying for quality on an as-needed basis.

Access to specialized QA expertise

Engaging with external QA partners offers access to highly skilled professionals, often certified through frameworks such as International Software Testing Qualifications Board (ISTQB). These experts bring the latest methodologies, ensuring that the QA processes remain current with industry best practices.

Scalability and flexibility

Outsourced QA services provide the agility to scale testing efforts up or down based on project demands. During periods of high release frequency or regulatory audits, external teams can quickly bolster testing capacity.



Future Trends in QA for Banking and Financial Services

The landscape of QA in banking and financial services is constantly evolving, driven by rapid technological advancements, changing customer expectations, and increasing regulatory scrutiny. To stay ahead of the curve, financial institutions in the Philippines must anticipate and adapt to emerging trends in QA. This involves embracing new technologies, methodologies, and approaches that can enhance the efficiency, effectiveness, and agility of their QA processes.

The Rise of AI-Driven Automation

According to Gartner, 30% of enterprises will incorporate an AI-augmented testing strategy into their operations by 2025. AI is revolutionizing QA processes by introducing automation that enhances efficiency and accuracy. This automation accelerates testing cycles and reduces human error, leading to more robust software applications. AI-powered tools can automate various aspects of testing, including test case generation, test data management, and defect detection.

> **The Commonwealth Bank of Australia has invested heavily in AI technologies, resulting in a 40% reduction in call center wait times and a 50% decrease in scam losses.**

Shift-Left Testing

The shift-left approach involves integrating testing early in the software development lifecycle, allowing for the identification and mitigation of vulnerabilities before they escalate. In financial services, this proactive strategy reduces remediation costs and enhances security posture. Implementing shift-left practices has enabled organizations to align security and engineering teams early, reducing delays and improving collaboration.

The Impact of Cloud-Native Applications on QA Strategies

The adoption of Cloud-native applications transforms QA strategies in banking and financial services. Cloud-native architectures facilitate scalability, flexibility, and rapid deployment, necessitating QA approaches that can keep pace. CI/CD pipelines are essential in this context, enabling seamless testing and deployment processes. Financial institutions are leveraging Cloud-native solutions to enhance their digital banking experiences, with AI-driven QA ensuring compliance and quality in these dynamic environments.

Continuous Testing and Hyper-Automation in DevOps Pipelines

Continuous testing, integrated within DevOps pipelines, ensures that software is consistently validated at every stage of development. Hyper-automation combines AI and machine learning to further streamline as many aspects of the testing process as possible, including test case generation, test data management, and test execution. This integration allows for real-time feedback and rapid issue resolution, essential for maintaining the agility required in modern banking services.



Stratpoint's Approach to QA

As digital banking becomes increasingly complex and regulated, Stratpoint's approach to QA is designed to deliver scalable, secure, and high-performance testing solutions that meet the rigorous demands of the financial services industry. Stratpoint leverages modern QA strategies and industry-recognized frameworks to drive efficiency and deliver measurable improvements in software quality.

Delivering Scalable and Secure QA Solutions

Stratpoint's QA methodology is built around modern practices that streamline testing processes while maintaining the highest standards of security.

Modern QA Strategies to Drive Efficiency

Stratpoint utilizes both automated and manual testing processes to ensure comprehensive coverage across critical applications. Leveraging modern QA methodologies, such as agile and DevOps, to accelerate testing cycles, improve collaboration, and ensure continuous delivery of high-quality software, Stratpoint helps banks and financial institutions reduce the time-to-market while ensuring that each release meets stringent quality standards.

Strategic QA Playbook Development and Implementation

To ensure consistency and efficiency in QA processes, Stratpoint emphasizes the development and implementation of a strategic QA Playbook. This playbook serves as a blueprint for testing methodologies, best practices, and governance structures tailored to every organization's unique needs, as no two companies operate the same way. This customized approach ensures that each organization's specific workflows, regulatory requirements, and technological environments are accounted for. By implementing a bespoke QA playbook, banks and financial institutions can achieve higher QA efficiency, improved defect prevention, and a stronger alignment between testing practices and business objectives.

Ensuring Performance and Reliability

Stratpoint implements performance testing to ensure banking and financial applications operate efficiently under high transaction loads. Through rigorous load and stress testing, Stratpoint helps financial institutions identify bottlenecks, optimize system responsiveness, and prevent downtime. This ensures that applications deliver seamless, high-speed digital experiences, even during peak usage periods.

Scalable QA Services

Recognizing that each financial services firm has unique needs, Stratpoints offers a suite of scalable QA services tailored to address different stages of the software development lifecycle.



QA Conditioning
Training

Start with comprehensive training programs to enhance your team's skills, knowledge, methodologies, and practices.



QA Coaching
Consulting

Recognize gaps at any point of your QA journey and elevate software quality.



QA Crew
Staff Augmentation

Onboard skilled and experienced QA professionals to ensure the success of your products from day 1.



QA Pitstop
Managed QA

Scale up and down with a dedicated QA team to oversee and manage your QA process from end to end.



QA Quick Fix
Testing as a Service

Leverage innovative testing tools and proven frameworks to achieve the best testing outcomes.



Seamless QA Resource Consolidation via TCOE

The establishment of a Testing Center of Excellence (TCOE) facilitates standardized processes and centralized oversight. Stratpoint's TCOE model streamlines vendor management, reduces duplication of efforts, and ensures that best practices are uniformly applied across all projects. This approach not only drives operational efficiency but also leads to more predictable outcomes and easier scalability during periods of rapid digital transformation.

Industry-Recognized Expertise

Stratpoint differentiates itself by building its QA methodologies on globally recognized standards and leveraging cutting-edge technology.

Stratpoint's QA solutions are anchored in frameworks that comply with the International Software Testing Qualifications Board (ISTB) standards as an ISTQB Gold Partner. By maintaining these standards, Stratpoint ensures that its testing methodologies are not only robust but also continuously updated to reflect the latest industry trends.

Strategic Use of Test Automation and AI-Driven Testing Solutions

> Embracing automation is at the core of Stratpoint's approach. The use of AI-driven testing tools enables predictive analysis, risk-based testing, and enhanced defect detection. Essilor Shared Services Philippines Incorporated (ESSPI), a shared services company providing solutions and support services to Essilor Group, improved software quality and efficiency by introducing automated test scripts, reducing testing execution time by 90%, and enhancing overall QA processes.



Quality at the Core

Banks and financial institutions in the Philippines face increasing challenges – from evolving cyber threats and stringent regulatory requirements to heightened customer expectations for seamless digital experiences. Addressing these challenges requires a proactive, well-structured QA framework, so banks and financial institutions can achieve:

- **Enhanced risk mitigation** by identifying and resolving vulnerabilities before they escalate.
- **Operational efficiency** via test automation, reducing manual efforts and expediting release cycles.
- **Customer trust and retention** through seamless, high-performing digital banking experiences.
- **Regulatory compliance** through continuous adherence to financial security standards.

With increasing reliance on digital banking and fintech solutions, ensuring software quality is a strategic enabler of business growth. Organizations that invest in maturing their QA capabilities position themselves ahead of competitors, delivering secure, resilient, and scalable financial services in an ever-evolving market.

Take the Next Step in Assessing Your QA Maturity

Where does your organization stand in its QA maturity? Whether your institution is transitioning from traditional QA models or looking to scale its automation and AI-driven testing capabilities, now is the time to take action. Assess your current QA framework and explore how a strategic partnership with industry leaders can help optimize your investment in quality.

Stratpoint's proven expertise in QA equips banks and financial enterprises with the tools, frameworks, and automation strategies needed to drive efficiency and compliance. If your organization is ready to enhance its QA processes, optimize testing investments, and consolidate resources through a Testing Center of Excellence (TCOE), our team is here to help.

Schedule a discovery call now and explore how we can boost your QA strategy for the future of digital banking.

References

1. **Anti-Money Laundering Council**. (2015). *Republic Act No. 9160. Anti-Money Laundering Act of 2001*. http://www.amlc.gov.ph/laws/money-laundering/2015-10-16-02-50-56/republic-act-9160
2. **American Society for Quality**. (n.d.). *Failure Mode and Effects Analysis (FMEA)*. https://asq.org/quality-resources/fmea
3. **Balbix**. (2025). *SAST, DAST, IAST: Application Security (AppSec) Testing Tools*. https://www.balbix.com/insights/sast-dast-iast-application-security-appsec-testing-tools/
4. **Bangko Sentral ng Pilipinas**. (2023). *2023 Status of Digital Payments in the Philippines*. https://www.bsp.gov.ph/PaymentAndSettlement/2023_Report_on_E-payments_Measurement.pdf
5. **Bangko Sentral ng Pilipinas**. (2013). *BSP Circular No. 808: Information Technology Risk Management for All Banks and Other BSP Supervised Institutions*. https://www.bsp.gov.ph/Regulations/Issuances/2013/c808.pdf
6. **Bangko Sentral ng Pilipinas**. (2024). *BSP: Use Security Features for Online Transactions*. https://www.bsp.gov.ph/SitePages/MediaAndResearch/MediaDisp.aspx?ItemId=6238
7. **Bangko Sentral ng Pilipinas**. (2024). *Philippines Hits Target of Digitalizing 50 Percent of Retail Payments*. https://www.bsp.gov.ph/SitePages/MediaAndResearch/MediaDisp.aspx?ItemId=7182
8. **BDCC Global**. (2023). *Things to Know About CI/CD Pipelines and the Latest Open-Source CI/CD Tools*. https://www.bdccglobal.com/blog/things-you-should-know-about-ci-cd-pipelines-and-its-latest-tools/
9. **BusinessWorld Online**. (2024). *Banks ramp up spending on cybersecurity as attacks rise*. https://www.bworldonline.com/banking-finance/2024/05/31/598619/banks-ramp-up-spending-on-cybersecurity-as-attacks-rise/
10. **Commonwealth Bank of Australia**. (2024). *Customer safety, convenience and recognition boosted by early implementation of Gen AI*. https://www.commbank.com.au/articles/newsroom/2024/11/reimagining-banking-nov24.html
11. **CrowdStrike**. (2024). *What is Shift Left Security?* https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/shift-left-security/
12. **DigitalOcean**. (n.d.). *10 AI Testing Tools to Streamline Your QA Process in 2025*. https://www.digitalocean.com/resources/articles/ai-testing-tools
13. **Docker**. (n.d.). *Use containers to Build, Share and Run your applications*. https://www.docker.com/resources/what-container/
14. **Empaxis**. (2024). *Outsourcing Quality Assurance Testing - Why Investment Management Software Companies Need 3rd Party Experts*. https://www.empaxis.com/blog/outsourcing-quality-assurance-testing
15. **Fintech News Philippines**. (2024). *Philippines Recorded Highest Numbers for Phishing Attacks*. https://fintechnews.ph/64749/fintech/philippines-recorded-highest-numbers-for-phishing-attacks/
16. **Gartner**. (n.d.). *Gartner Experts Answer the Top Generative AI Questions for Your Enterprise*. https://www.gartner.com/en/topics/generative-ai
17. **Imperva**. (n.d.). *Financial Services Cybersecurity*. https://www.imperva.com/learn/data-security/financial-services-cybersecurity/
18. **Infotek Solutions**. (n.d.). *What is the Cost of Defects in Software Testing*? https://www.qaonlinetraining.com/what-is-the-cost-of-defects-in-software-testing/
19. **International Software Testing Qualifications Board**. (n.d.). *ISTQB Website*. https://www.istqb.org/
20. **Intersoft Consulting**. (n.d.). *GDPR Information Portal*. https://gdpr-info.eu/
21. **ISO**. (n.d.). *ISO Standards*. https://www.iso.org/standards.html
22. **Albattah W., Alzahrani M**. (2024). *Software Defect Prediction Based on Machine Learning and Deep Learning Techniques: An Empirical Approach*. https://www.mdpi.com/2673-2688/5/4/86
23. **MihuPai**. (2024). *How AI Automation Simplifies Banking Compliance and QA Processes*. https://mihup.ai/ai-automation-simplifies-banking-compliance-and-qa-processes/
24. **National Privacy Commission**. (2024). *NPC Issues Circulars to Strengthen Personal Data Protection in PH*. https://privacy.gov.ph/npc-issues-circulars-to-strengthen-personal-data-protection-in-ph/
25. **National Privacy Commission**. (n.d.). *Republic Act 10173: Data Privacy Act of 2012*. https://privacy.gov.ph/data-privacy-act/
26. **PCI Security Standards Council**. (2018). *PCI DSS Quick Reference Guide*. https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf
27. **Philippine Institute for Development Studies**. (2024). *AI in Philippine Banking: Embracing Innovation Amid Challenges*. https://www.pids.gov.ph/details/news/in-the-news/ai-in-philippine-banking-embracing-innovation-amid-challenges
28. **Scrut Automation**. (2024). *The Necessity of a Risk-Based Approach in Modern Compliance*. https://www.scrut.io/post/the-necessity-of-a-risk-based-approach-in-modern-compliance
29. **Securiti.ai**. (2024). *Data Regulations in the Financial Sector of the Philippines*. https://securiti.ai/data-regulations-in-the-financial-sector-of-the-philippines/
30. **Security Intelligence**. (2024). *Cost of a Data Breach 2024: Financial Industry*. https://securityintelligence.com/articles/cost-of-a-data-breach-2024-financial-industry/

31. **Six Sigma Online**. (n.d.). *Implementing Lean Six Sigma In Software Development.* https://www.sixsigmaonline.org/six-sigma-for-software-development/
32. **Stratpoint**. (2025). *Stratpoint Advances QA Excellence with ISTQB Gold Partnership.* https://stratpoint.com/2025/01/13/stratpoint-advances-qa-excellence-with-istqb-gold-partnership/
33. **The Council for Six Sigma Certification**. (2018). *Six Sigma: A Complete Step-by-Step Guide.* https://www.sixsigmacouncil.org/wp-content/uploads/2018/08/Six-Sigma-A-Complete-Step-by-Step-Guide.pdf
34. **Visa**. (2024). *Annual Visa Consumer Payment Attitudes Study Reveals Significant Decline in Cash Payments Amid Rise in Cashless Transactions.* https://www.visa.com.ph/about-visa/newsroom/press-releases/annual-visa-consumer-payment-attitudes-study-reveals-significant-decline-in-cash-payments-amid-rise-in-cashless-transactions.html
35. **Visa**. (2024). *New Horizons for Payments in Our Hyper-Digital Age: Consumer Payments Attitudes Study.* https://www.visa.com.vn/content/dam/VCOM/regional/ap/singapore/global-elements/documents/visa-cpa-2023-report-ipvmc-final.pdf
36. **West Monroe**. (2023). *A look inside the process: How to 'shift left' security and compliance in financial services.* https://www.westmonroe.com/insights/how-to-shift-left-in-financial-services

stratpoint
FAST FORWARD TO THE FUTURE

About Stratpoint

Stratpoint is the digital acceleration partner for companies ready to transform. With expertise in agile software development, quality assurance, Cloud, data, and AI, it empowers businesses to boost efficiency, improve decision-making, and gain a competitive advantage in today's digital economy.

www.stratpoint.com hello@stratpoint.com Stratpoint Technologies

