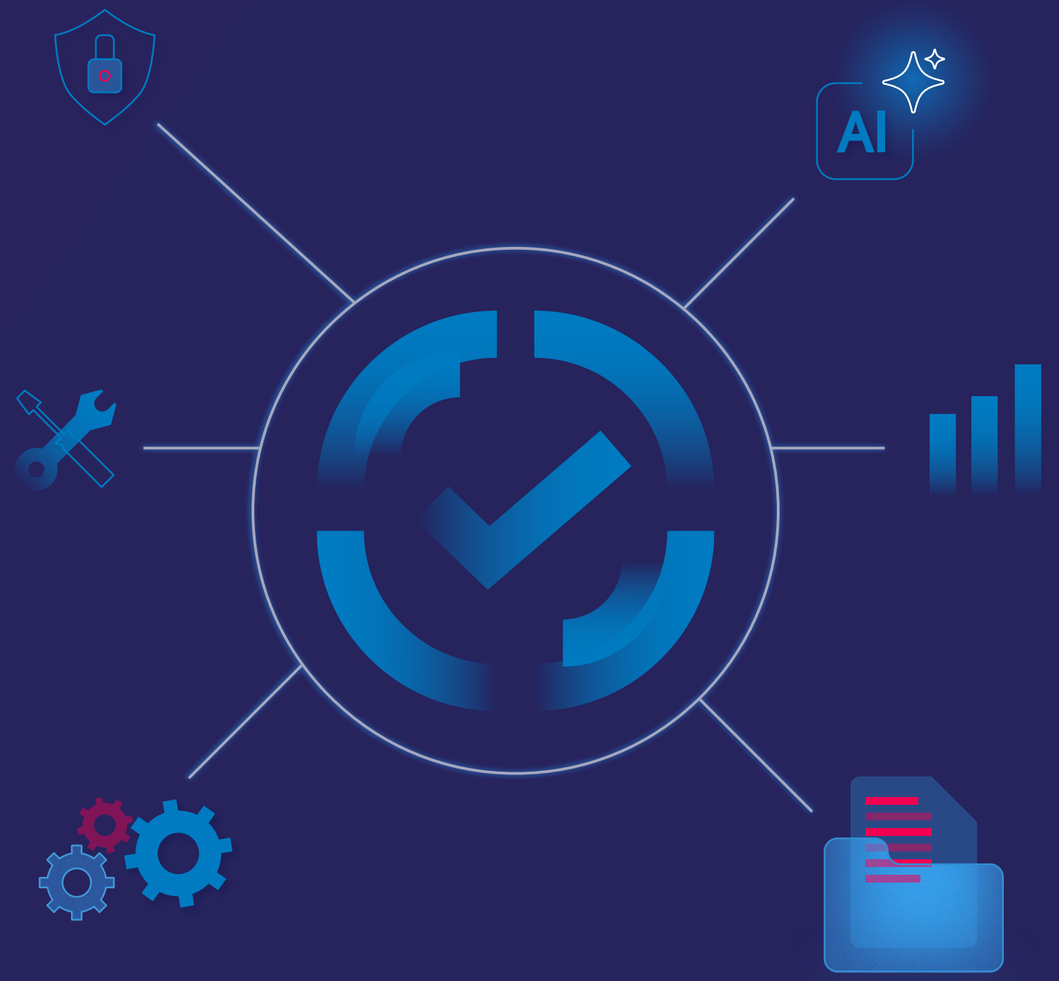
SUTHERLAND®

DIGITALIZING CORE CAPABILITIES

Accelerate and Scale Digital, Cloud, and AI Initiatives With Digital Quality Assurance



Modern enterprises operate in an **increasingly complex** connected ecosystem.

Digital services must perform across a wide range of platforms, channels, and geographies. And customers expect intuitive, omnichannel experiences with zero tolerance for failure.

But as AI-driven, cloud-enabled systems take center stage, there's a critical piece of the puzzle that often gets overlooked: when adoption scales and velocity increases, **how do you ensure every customer interaction is seamless, secure, and consistent?**

The truth is that enterprises are investing heavily in AI, cloud, and data-driven platforms to boost competitiveness and agility. But many transformation initiatives still underdeliver – not because the strategy is flawed, but because the execution is fragile.

As enterprises move fast to deploy new digital products and services as part of core capabilities that deliver measurable outcomes, quality can't afford to become an afterthought.

US businesses lost an estimated $2.08 billion in 2020 to poor software quality.[1] Fixing a bug can cost as little as $100 in the planning stage. But, if discovered during the production stage, that same bug can become a $10,000 headache.[2]

And it's not just about bugs. Inconsistent digital experiences, delayed product launches, fragile security postures, and unplanned downtime are all symptoms of frameworks that haven't kept up with the speed and scale of transformation. That's why organizations have embraced quality assurance as a strategic capability – one that spans platforms, teams, and customer journeys.

And yet, **88% of service leaders** say their existing QA processes are ineffective.[3]

[1] The Cost of Poor Software Quality in the US: A 2020 Report
[2] Costly Code: The Price Of Software Errors
[3] Customer Service Quality Assurance: Maximize the Value of Your Program

Digital quality assurance (DQA) is how enterprises flip that. No longer a back-end function, **DQA ensures new technologies live up to their promise.** It ensures innovation directly translates to tangible business outcomes – whether that's increasing revenue, cutting costs, enabling faster time-to-market, or beyond – **by protecting transformation investments** from unnecessary risk, disruption, and rework, as well as providing the agility to innovate with confidence.

It's no surprise, then, that more than half (52%) of enterprises are already prioritizing enhanced testing and validation protocols in AI-supported software development on the road to fully embracing DQA.[4] After all, in today's AI-accelerated world, **quality can't be the final checkpoint – it needs to be built in from the beginning.**

[4] How can organizations engineer quality software in the age of generative AI?

This POV will outline a strategic framework for digital quality assurance – one of the six essential steps in **digitalizing core capabilities.** We will explore:

The hidden threats that legacy QA models introduce into AI, cloud, and transformation efforts, and why these risks are increasing in modern ecosystems.

A strategic framework for a modern, AI-first, cloud-enabled digital assurance model powered by automation and continuous feedback.

Practical steps to embed digital assurance into your transformation roadmap, and to ensure your investments deliver measurable outcomes faster, more efficiently, and with greater resilience.

By connecting the business imperative to a clear digital assurance strategy, this framework provides leaders with **a roadmap to unlock the full potential of their core capabilities** and sustain a competitive advantage in a fast-changing digital economy.

Why Digital Transformation Success Demands Digital Assurance

Too often, businesses rely on outdated QA strategies that weren't designed for today's speed or complexity. Testing happens too late in the development cycle, lacks full coverage, or is disconnected from real-world conditions.

The result? Critical issues slip through the cracks – and the business pays the price. But the cost isn't just measured in bugs. It's measured in revenue lost, customer frustration, and transformation initiatives that stall before they deliver value or real business outcomes.

When quality assurance lags behind, businesses encounter **four recurring problems**.

ISSUE #1

Operational Nightmares
Escalated Digital and Financial Risks

Without integrated quality assurance, enterprises face a rising risk of unplanned outages, failed releases, and cascading technical debt. As digital, cloud, and AI systems become more interconnected, even minor defects can lead to major operational disruptions, from degraded performance to full-blown system downtime, with downtime costs hitting as high as $9,000 per minute for large organizations.[5]

This is especially true in Agile and DevOps environments where rapid deployment is the norm. When QA is reactive or disconnected from development, gaps surface late in the cycle, triggering urgent (and costly) remediation work. Engineering teams are pulled away from innovation to fix issues, while operations teams scramble to maintain service continuity.

A robust DQA framework embeds validation earlier in the development lifecycle. With AI-powered automation and continuous test coverage, defects are caught sooner, reducing the risk of service interruptions and lowering the cost of remediation. This ensures operational continuity and preserves development velocity.

ISSUE #2

Digital Headaches
Inconsistent Customer Experiences

Today's customers interact with brands across a wide range of touchpoints – web, mobile, kiosk, voice, and more. They expect a seamless, reliable, and responsive experience at every stage of the journey. But when quality isn't consistent, neither is the customer experience.

Minor glitches, variations in how features perform across devices, slow-loading interfaces, or broken functionality can be detrimental in eroding brand perception. For instance, as many as 88% of users are less likely to return to a website if they had a bad experience.[6] And because these issues are often only uncovered once users report them, the damage is already done.

The brand impact of broken experiences is profound, especially in competitive markets where user experience is a primary differentiator.

DQA brings a consistent, omnichannel validation strategy that evaluates user journeys across platforms and environments. With integrated feedback loops, real-device testing, and predictive analytics, enterprises can surface and resolve experience gaps before they reach the customer, building trust through reliability.

[5] The True Cost Of Downtime (And How To Avoid It)
[6] Know Your User: UX Statistics and Insights (With Infographic)

ISSUE #3

Innovation Bottlenecks

A Lack of Digital Agility and Delayed Time-To-Market

For enterprises to stay competitive, speed is everything. But traditional QA methods – manual testing, siloed review cycles, and delayed validation – are at odds with modern development timelines. And 58% of organizations that have automated software testing, have done so to increase deployment speed.[7]

If a robust assurance strategy isn't embedded into the heart of a digital transformation effort, enterprises can find themselves stuck in a cycle of reactive problem-solving. The result is a bottleneck: it slows deployment cycles, reduces agility, and makes it harder to react quickly to market changes. In essence, it stifles innovation.

DQA is built on agile development and continuous delivery practices, leveraging AI and automation to keep pace with rapid change. Test cases evolve in parallel with new code, reducing lag time and shortening feedback loops. This allows enterprises to ship faster – and with greater confidence – without compromising on quality.

ISSUE #4

Security Pitfalls

Increased Threats and Vulnerabilities

The more digital services an enterprise offers, the more surface area it exposes to potential threats. Every integration, update, or third-party plugin introduces new risks. Yet in many organizations, QA and security remain siloed – and vulnerabilities go undetected until after deployment.

This gap between development and security is increasingly expensive: the global average cost of a data breach reached $4.45 million in 2023, which is a 15% rise compared to 2020.[8] Whether it's customer data, proprietary systems, or compliance requirements, the stakes are high. A single vulnerability can lead to regulatory penalties, reputational damage, or loss of customer trust.

A modern DQA framework embeds security validation into every stage of development. Automated tests check for vulnerabilities in code, integrations, and user-facing features as part of the standard QA process. AI-powered anomaly detection flags suspicious patterns early, enabling proactive response before damage occurs. Security isn't left to the end – it's built in from the start.

[7] Automated Software Testing Adoption and Trends

[8] IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs

The Four Pillars of a Modern Digital Assurance Framework

For digital transformation to succeed, quality assurance must evolve.

It can no longer be a reactive, isolated activity performed at the end of the development cycle. Instead, **it must become an integrated, intelligent layer across the full digital value chain** – from planning and design through to deployment and continuous improvement.

This is particularly important as **enterprises adopt Agile and DevOps practices at scale**. Faster release cycles and decentralized teams demand a fundamentally new approach to quality – one that is proactive, automated, and built for interoperability. **This has accelerated the transition from traditional QA to digital QA and now onto AI-enabled QA**, which will enable near real-time, self-sustaining quality at scale.

In this context, **a modern digital assurance framework provides the foundation for delivering transformation with confidence, and for driving measurable business impact.** This framework is built upon **four interconnected pillars**. Together, they support high-performing, secure, and user-centric digital experiences without slowing innovation or increasing risk.

PILLAR #1

Adopt AI-Driven Test Automation

As development cycles accelerate and applications grow more complex, manual testing simply can't keep pace. Automation has now become the backbone of modern QA as a result, helping enterprises enhance both speed and coverage.

AI and ML-powered tools also go beyond traditional test automation by analyzing and learning from past data. This brings the advantage of autonomous test execution integrated with DevSecOps, self-healing scripts, predictive error detection, and adaptive learning, reducing the need to constantly rewrite test cases and allowing teams to focus on higher-value tasks.

Strategic investment into AI testing Centers of Excellence (CoEs) extends this further, and will be critical to long-term success. Acting as an R&D hub that can incubate and scale new automation capabilities and rapidly operationalize innovation, an AI testing CoE serves as the engine for enhancing accuracy, agility, and resilience in a structured and measurable way.

Practical steps

- **Partner with an intelligent automation specialist to build an AI testing Center of Excellence** that can drive innovation and guide enterprise-wide adoption.
- **Deploy a modular, AI-enabled test automation platform** that integrates with your existing toolchain. This ensures compatibility with CI/CD pipelines and supports scalable growth.
- **Use pre-built, domain-specific test libraries** to jumpstart coverage for common use cases, while customizing where needed for proprietary functionality.
- **Prioritize automation in areas with high regression risk or high user impact,** such as payment flows, onboarding journeys, and mobile UI. And apply automated defect classification and integration with existing issue identification systems.

If you're exploring where to begin, consider **Sutherland CloudTestr™** – an AI-powered test automation platform designed to accelerate delivery while enhancing reliability. Sutherland's AI Testing CoE also drives innovation in quality engineering through agent-led automation, NLP-based test generation, self-healing scripts, and predictive defect analysis. With tools like Claude AI and Playwright, and integration into DevSecOps pipelines, it enables intelligent, scalable, and resilient QA. The roadmap includes an Agentic Test Lab-as-a-Service (TaaS), advancing toward self-service, AI-driven test automation across the enterprise.

PILLAR #2

Emphasize Continuous Monitoring for Real-Time Quality Assurance

Digital experiences don't exist in a vacuum – they evolve in real time, shaped by shifting user behavior, unexpected usage patterns, and external dependencies. That's why quality assurance shouldn't end when code is released. In a modern QA framework, continuous monitoring is essential to ensure performance, usability, and system health are maintained post-deployment.

Real-time visibility into live environments enables teams to proactively detect issues, from API latency and frontend glitches to sudden drops in conversion rates. It also supports informed decision-making by offering empirical evidence of how users interact with digital products across channels and timeframes.

By closing the feedback loop between operations, development, and QA, continuous monitoring becomes a driver of resilience, innovation.

Practical steps

- **Implement AIOps tools** to track application behavior, user flows, and system performance across all environments: staging, production, and beyond.
- **Integrate anomaly detection algorithms** that flag deviations from baseline performance, helping teams act before incidents escalate into outages or support issues.
- **Establish cross-functional feedback loops** between end-users, DevOps, and business stakeholders, using shared dashboards and alerts to align priorities.
- **Use analytics from real-world usage** to refine test cases and guide future releases, turning monitoring data into continuous improvement. And use these insights to help further guide performance engineering practices, ensuring scalability under high traffic conditions to maintain an optimal user experience.

You don't need to build this from scratch. **Sutherland's application support** capabilities help teams scale monitoring, reduce MTTR, and surface actionable insights faster for shorter development cycles.

PILLAR #3

Shift to Security-First Validation Across the Lifecycle

From API exposure to misconfigured cloud environments, vulnerabilities can emerge anywhere. With threat surfaces expanding and regulations tightening, enterprises need proactive security testing that evolves alongside their codebase.

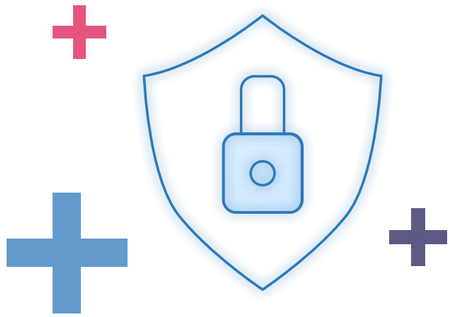
That's why a DQA strategy treats security validation as a core function that works in parallel with functionality and performance testing. By integrating security checks into CI/CD and test automation workflows, organizations can catch issues early, helping to reduce risk and build customer trust through secure-by-design systems.

Security is no longer the domain of a separate team at the end of the process. It must be embedded into every phase of digital development and delivery. This shift protects the enterprise while enabling faster, safer releases.

Practical steps

- **Embed static application security testing (SAST) and dynamic testing (DAST)** into automated pipelines, ensuring security validation happens on every commit. And include threat modeling in the early stages so it's fully integrated with QA workflows to ensure security considerations are proactive rather than reactive.
- **Use AI-powered anomaly detection** to flag suspicious behavior – such as unexpected data flows, access requests, or API usage patterns – before they can be exploited.
- **Validate encryption standards, authentication protocols, and secure coding practices** as part of functional test cycles – not in isolation.
- **Continuously monitor for compliance** with evolving regulations (GDPR, CCPA, HIPAA, etc) across regions and industries.

A **digital assurance partner** like Sutherland can help operationalize security-first testing, integrating compliance, threat modeling, and real-time validation into your QA workflows.



PILLAR
#4

Maintain Consistency
Across Digital Touchpoints with Omnichannel Validation

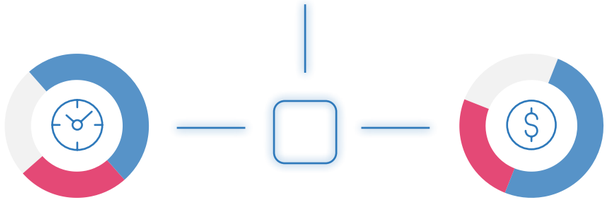
Customers engage with digital services in nonlinear, unpredictable ways, jumping from mobile to desktop, app to kiosk, chatbot to live agent. Yet many QA approaches still treat these channels in isolation, leading to inconsistent performance and fragmented experiences.

Omnichannel validation ensures that every digital touchpoint – regardless of device, channel, or context – aligns with brand standards, usability benchmarks, and customer expectations. This requires not only technical testing, but also an understanding of how real users move across platforms in real-world conditions.

Practical steps

- **Establish cross-platform testing strategies** that validate journeys across web, mobile apps, voice interfaces, and beyond – both individually and in sequence. And ensure test coverage includes varied device types, OS and browser combinations, and network conditions to reflect real-world environments.
- **Integrate UX testing into QA workflows** to capture usability insights alongside technical validations, ensuring both form and function meet expectations.
- **Leverage AI-based predictive analytics** to model user behavior, identify experience gaps, and prioritize enhancements based on actual usage data.
- **Include accessibility compliance** (e.g. WCAG standards) as a regular part of test coverage to ensure inclusivity across digital experiences.

Sutherland's digital assurance capabilities can help ensure consistency, functionality, and performance across every customer touchpoint, improving loyalty and conversion.



Conclusion

Across performance, operations, and customer experience, when new experiences are rushed to market without robust validation, the consequences are real: missed revenue, damaged brand trust, spiraling tech debt, and stalled innovation.

Enterprises don’t fail at transformation because they lack ambition. They fail because they underestimate risk. Digital Quality Assurance powered by AI and automation is how you de-risk digital transformation – embedding intelligence, consistency, and resilience into every system, experience, and service.

As organizations strive to modernize faster, deliver smarter, and operate securely, DQA has become the foundation for innovation. It’s the connective tissue that ensures your digital, cloud, and AI investments deliver measurable business outcomes, not just software releases – faster, more reliably, and at lower cost.

Let’s redefine quality. Learn how Sutherland can help you embed assurance into the heart of your digital, cloud, and AI transformation.

Learn More

Artificial Intelligence. Automation. Cloud Engineering. Advanced Analytics. For Enterprises, these are key factors of success. For us, they’re our core expertise.

We work with global iconic brands. We bring them a unique value proposition through market-leading technologies and business process excellence. At the heart of it all is Digital Engineering – the foundation that powers rapid innovation and scalable business transformation.

We’ve created over 200 unique inventions under several patents across AI and other emerging technologies. Leveraging our advanced products and platforms, we drive digital transformation at scale, optimize critical business operations, reinvent experiences and pioneer new solutions, all provided through a seamless “as-a-service” model.

For each company, we provide new keys for their businesses, the people they work with, and the customers they serve. With proven strategies and agile execution, we don’t just enable change – we engineer digital outcomes.

SUTHERLAND®
digital outcomes.

sutherlandglobal.com