



Digital Systems & Technology

Automation Assurance Framework to Validate Cloud Readiness

Our automation-driven approach to assuring continuity and quality before and after migrating operations to the cloud will safeguard your organization's data, applications and servers.

Executive Summary

Migrating to the cloud has proven to be a transformative step for many organizations, but it is complex and entails risks to applications unless proper end-to-end, cloud-specific testing is performed. We have seen that many organizations limit their testing strategy to application-level regression analysis, which is insufficient to ensure that the applications, data and servers are fully functional and safe post migration. In light of the many ways cloud leveraging has evolved, a comprehensive assurance

strategy to bring in cloud-centric validation techniques is required.

For instance, application performance issues can often surface on the cloud if the servers are not correctly sized, if there are network latency issues that were not tested in isolation or if there are dependencies with other applications that were not tested end to end on the cloud. Consequently, businesses moving to the cloud without a comprehensive cloud testing strategy can

Traditional testing covers validation of functional and nonfunctional aspects of applications, databases and servers. But in addition to those tenets, cloud testing needs to include validation of all cloud attributes including availability, scalability, multitenancy, interoperability and security.

Traditional vs. cloud testing

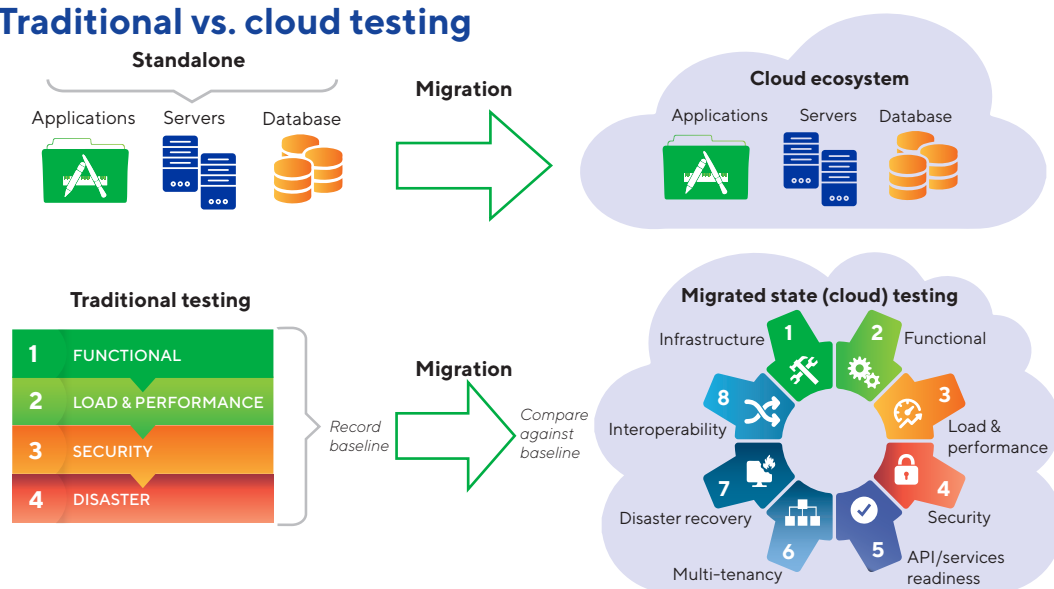


Figure 1

expose their applications to potential risks leading to server breakdown issues and application crashes.

To help enterprises get the best out of the cloud, we have devised a strategy that encompasses all key cloud-readiness attributes – not merely

functionality, performance, security and user experience. This white paper will provide insights into a proven cloud migration assurance framework that we have implemented in our successful cloud migration programs.

How traditional and cloud testing differ

Cloud testing differs greatly from conventional application and/or system testing (see Figure 1). Traditional testing covers validation of functional and nonfunctional aspects of applications, databases and servers. But in addition to those tenets, cloud testing needs to include validation of

all cloud attributes including availability, scalability, multitenancy, interoperability and security. It is also important to note that the approach to testing will differ based on migration methods – namely re-host, re-platform, re-factor and re-architect (see Phase 2 section below).



Our cloud migration assurance framework

We devised an all-inclusive framework that offers IT teams a structured approach to validate business readiness post cloud migration but before going live. The framework focuses on three key migration phases (see Figure 2):

- Phase 1: Assessment:** A checklist and assessment questionnaire help determine an application's readiness and suitability for cloud migration.
- Phase 2: Planning:** A strategy that will customize the migration methodology depending on the type of application and the cloud architecture.

- Phase 3: Migration and validation:** Configure applications, databases and servers on cloud. Conduct pre- and post-migration tests and determine go/no-go decision criteria.

Phase 1: Assessment

During this phase, applications, databases and servers are qualified based on their technical attributes, business criticality and priority to determine potential candidates for migration. The deployment and service models can vary based on the following criteria:

- Application type (in-house; COTS; custom-developed).

QA framework for cloud assessment, planning & implementation

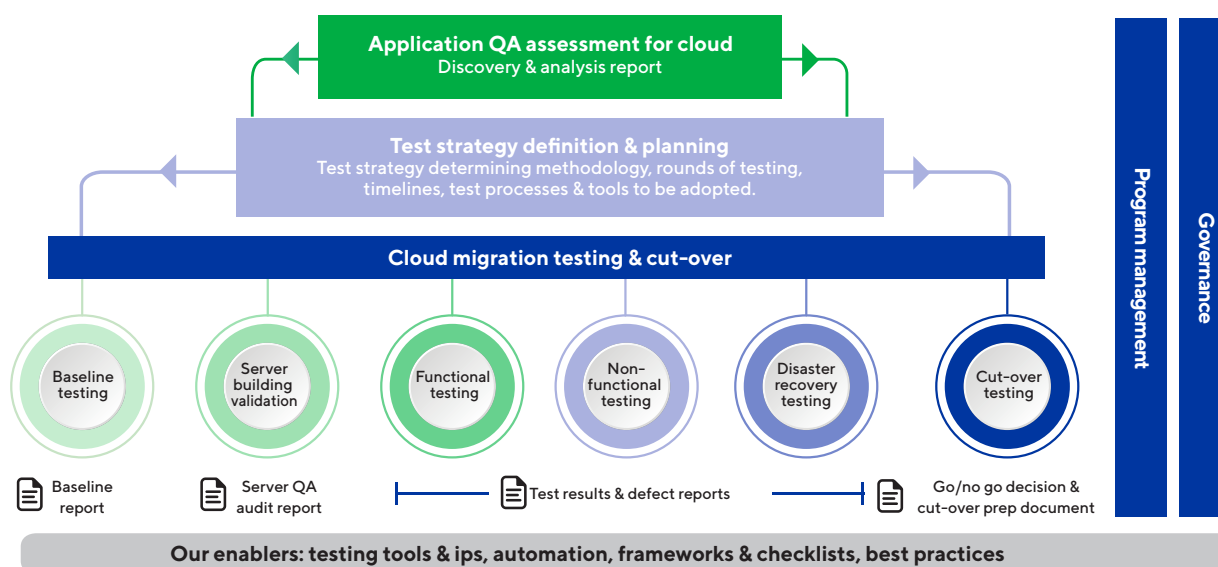


Figure 2

- Upstream/downstream dependencies.
- Availability zones.
- Security and compliance requirements.
- Costs and licensing.

Our assessment approach comprises two key steps: (1) discovering the current state of applications including databases, servers, OS, user load patterns and network behavior, and (2) analyzing such gathered information to derive functional and nonfunctional test requirements and to finalize the testing scope.

Our quantitative, scoring-based assessment framework provides a consistent method toward application profiling across multiple parameters and results in a cumulative score to determine the fitment for cloud.

Phase 2: Test strategy & planning

The different server and application migration

methodologies call for specific test approaches and strategies. These are the four different migration methodologies:

- **Re-host/lift and shift:** No technology changes required; migrate workload as is to cloud.
- **Re-platform:** Needs OS/DB changes; reinstall applications so they work on cloud platform.
- **Re-factor:** Requires code remediation, middleware changes, decoupling, etc. related to cloudification.
- **Re-architect:** Requires application architecture changes to leverage microservices and cloud-native functionalities.

Based on our experience in large-scale migrations involving different methodologies, we provide a sample guideline in Figure 3 to determine the optimal test strategy, based on the relative importance of the various testing types. For example, a simple web application already built on

Test strategy recommendations for different migration methodologies

Testing types	Re-host—lift & shift	Re-platform	Re-factor	Re-architect
Baseline testing	High	High	Medium	Medium
Functional regression	Medium	High	High	High
Performance testing load/latency	Medium	High	High	High
Stress testing	Low (critical for apps w/ varying user loads)	Low (critical for apps w/ varying user loads)	High	High
Security testing	High (critical for external facing apps)	High (critical for external facing apps)	High	High
Database testing	Low	High	High	High
Interoperability testing	Determined based on application integration & platform dependencies			
Disaster recovery & fail over	Determined based on DR scope (RPO/RTO requirements)			

Figure 3

The goal is to achieve maximum possible automation to accelerate the migration process and ensure comprehensive test coverage for applications to work seamlessly on the cloud. Our reusable automation framework is platform-agnostic and leverages the cloud APIs to enable early testing.

the latest technology and which does not need any OS/DB changes can be moved to the cloud using the re-host methodology, whereas a legacy app that needs changes to the OS or underlying architecture before it can be moved to cloud would fall under the re-factor or re-architect categories.

Phase 3: Cloud migration testing & cut-over

As part of cloud migration assurance, we recommend a minimum of three rounds of testing to ensure comprehensive coverage:

- I Round 1: Pre-migration testing** includes baseline testing in the existing premises and recording benchmarks for application/server performance.
- I Round 2: Post-migration testing** includes validating the server configuration against the architecture and conducting end-to-end tests – functional, web services, integration, performance, security, regression, DR and fail-over – against the applications on the cloud.
- I Round 3: Cut-over & go-live certification** includes cut-over planning and go-live testing and monitoring in the production environment, plus validating the environment decommissioning.

The goal is to achieve maximum possible automation to accelerate the migration process and ensure comprehensive test coverage for applications to work seamlessly on the cloud. Our reusable automation framework is platform-agnostic and leverages the cloud APIs to enable early testing.

To ensure optimal performance and security, it is critical to conduct nonfunctional testing as part of the cloud certification process. Performance testing is conducted to ensure scalability, measure latency, simulate peak user load and monitor the server performance. The results are compared against the baseline metrics and feedback is provided for performance tuning as needed. Security testing involves validating regulatory compliance (including SOX, PII, PCI, etc.) and also ensuring the security rules for authentication and authorization.

As the testing progresses, it is imperative to provide real-time information and reporting on the metrics to monitor the status and take corrective actions as needed. We have instrumented an overall release health dashboard that integrates build, deploy, test and release metrics. This tool enables business stakeholders to make go/no-go decisions.

Quick Take

Steering a Media Major to the Cloud

We assisted a leading media and publishing company to consolidate and migrate into the public cloud its infrastructure and applications which were distributed across over 18 data centers in the U.S., UK and Canada. In this project, we helped assess over 500 applications, of which over 100 were successfully migrated to AWS cloud. To do so, we employed Agile methodology, which enabled faster deployments, and we adopted our cloud migration assurance framework to define quality gates at each stage of migration and provide end-to-end test coverage for this migration.

The scope of assessment included baseline performance testing, server build validation on cloud, performance testing and monitoring, security testing, disaster recovery failover testing and go-live certification.

The project produced these key business benefits:

- Cloud deployment certification went 30% faster with QA automation framework.
- Parallel, in-sprint testing on cloud for accelerated releases and deployments.
- Increased resiliency and scalability with >30% improvement in application response times post migration to cloud.
- Shift left QA approach with automated cloud server validation framework enabled early defect detection.

Recap

Conventional testing methods are insufficient to ensure business readiness during cloud migration. Depending on the cloud migration methodology adopted, IT teams need to tailor their test strategy to ensure correct and complete validation. We

advocate a structured approach that will enable end-to-end validation which can be accelerated with effective use of tools and automation. Most IT teams are still just a few steps away from unlocking the true potential of the cloud, where the sky's the limit.

About the authors

Vikul Gupta

Lead, Digital Assurance Center of Excellence, Cognizant Quality Engineering & Assurance

Vikul Gupta leads the Digital Assurance Center of Excellence within Cognizant's Quality Engineering and Assurance business unit. He has 17 years of experience in product and service strategy formulation and delivery, with expertise in analytics, DevOps, cloud and data center automation. Vikul has helped several clients transform their QA organizations using analytics and cognitive-automation-based solutions that drive quality at speed. He holds a bachelor's degree in engineering from the National Institute of Technology, Surat, India. Vikul can be reached at Vikul.Gupta@cognizant.com | www.linkedin.com/in/vikul.

Anitha Srinivasan

Client Services Executive, Cognizant Quality Engineering & Assurance

Anitha Srinivasan leads the business development function within Cognizant for cloud assurance and quality engineering for the media and publishing industries. She has over 12 years of experience in quality consulting, business development and program delivery, and has been leading cloud assurance initiatives within Cognizant across industry domains. Anitha holds a master's degree in business analytics and intelligence from Indian Institute of Management, Bangalore, and a bachelor's degree in management from Birla Institute of Technology & Science, Pilani, India. She can be reached at Anitha.Srinivasan2@cognizant.com | www.linkedin.com/in/anitha-srini.

About Digital Assurance CoE

Digital Assurance Center of Excellence focuses on developing NextGen quality assurance solutions to help customers improve quality through Intelligent automation enabled by machine learning, artificial intelligence (AI) and conversational AI. The solutions developed by the Digital Assurance CoE support various areas of mobility, the Internet of Things, analytics, DevOps and cloud. AI-enabled BOTS provide predictive capabilities to identify defects and quality risks early in the lifecycle and help prevent application failures..

About Cognizant QE&A

Cognizant's Quality Engineering & Assurance (QE&A) is an independent business unit that addresses the end-to-end quality needs of today's digital enterprises. Cognizant's intelligent and automated approach to QA, driven by business-process-aligned test strategy and network-effect platforms, creates quality-led market differentiation. With more than 650 clients across industry verticals and a global footprint, Cognizant QE&A is a recognized thought leader in quality assurance.

About Cognizant

Cognizant (Nasdaq-100: CTSH) is one of the world's leading professional services companies, transforming clients' business, operating and technology models for the digital era. Our unique industry-based, consultative approach helps clients envision, build and run more innovative and efficient businesses. Headquartered in the U.S., Cognizant is ranked 193 on the Fortune 500 and is consistently listed among the most admired companies in the world. Learn how Cognizant helps clients lead with digital at www.cognizant.com or follow us [@Cognizant](https://twitter.com/Cognizant).

Cognizant

World Headquarters

500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters

1 Kingdom Street
Paddington Central
London W2 6BD England
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102

India Operations Headquarters

#5/535 Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060

APAC Headquarters

1 Changi Business Park Crescent,
Plaza 8@CBP # 07-04/05/06,
Tower A, Singapore 486025
Phone: + 65 6812 4051
Fax: + 65 6324 4051