KPMG

Ensuring Enterprise Resilience

The changing profile of operational risk and methods to ensure enterprise-wide resilience

—

May 2020

Ensuring Enterprise Resilience

Even organisations with an existing focus on resilience can be impacted when a Black Swan event occurs. The effects of major disruption are felt throughout the organisation, and technology estates can be put under new and pronounced strain.

Maintaining resilience in these circumstances means taking an organisation-wide view across three pillars –financial, operational and commercial.

Turbulent situations call for a rapid response, frequently requiring the introduction of critical IT change. This is particularly true of the **quality and operational** (a.k.a. non-functional) aspects of technology which, when delivered correctly, will ensure operational "stable states" persist, even in volatile times.

Testing can and should play a prominent role in ensuring these non-functional aspects are validated.
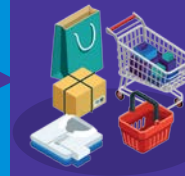
KPMG Enterprise Resilience Framework

Operational resilience
- Operational crisis management
- People
- Supply chain
- Technology and data
- Premises and property
- Cyber and fraud risk

Financial resilience
- Financial stress testing and forecasting
- Financial crisis response and contingency planning
- Liquidity and financing

Commercial resilience
- Markets, products and services
- Customer experience and behaviours

Click here for our guide to maintaining enterprise resilience

Enterprise Resilience - Testing Considerations

As organisations respond to the challenges of the current situation, new imperatives drive the focus of activities. The graphic below considers the short and medium term focus for testing.

Business Focus

Testing Focus

	Business Focus	Short Term	Medium Term
New change	Development and delivery of time critical change for:- — existing critical systems — newly critical systems Tactical acquisition and integration of SaaS products	— Non-functional testing practices must align to Agile/DevOps ways of working — Accurate modelling and testing of new workload patterns — Increased automated test coverage for new change and new systems brought online	— Implementation of Continuous Testing pipelines — Extend automation across all elements of NFT to increase efficiency, coverage and level of test insight — Use operational intelligence analytics to maintain an accurate view of platform usage patterns and reflect into test scenarios
Architectural Resilience	Carrying out capacity reviews and infrastructure scaling for:- — increases (and decreases) in traffic volumes — increased use of remote working technologies — network traffic and routing / prioritisation	— Build and execute test scenarios to inform capacity management and scalability decisions — Testing new architectural redundancy for fault tolerance — Regression testing for segregation of co-hosted applications — Review 3rd party service quality assurance plan	— Implement infrastructure monitoring, logging and alerting solution to inform capacity reviews — Regular capacity management reviews to allow cost efficiencies from accurate platform scaling and to support future traffic growth
Production Incidents	Responding to production incidents:- — first line service call volumes — tactical service recovery activities — Project-led remediation	— Analysis of production monitoring data for new change — Dev, Test and Operations collaboration working groups — Fix verification testing — Review, test and refine recovery procedures	— Implement failure testing and use learnings to enhance DR playbooks to allow rapid recovery of business critical processes — Implement solution monitoring and alerting solution to expedite issue identification and resolution

Document Classification: KPMG Public

Non-functional testing focus in the current climate

Performance

Evaluate impacts in the following areas:-
— New functionality exposed on essential systems
— Critical 3rd party integrations
— Application configuration changes
— Increased system traffic and user concurrency
— Geographic locations
— Performance during component failure
— Data Centre 'Edges'
— Infrastructure Capacity and Scalability

Reliability

The following are the considerations for failure and recovery:-
— Understanding the impact to a solution's uptime requirement of planned and unplanned activity e.g. system failure and recovery, lead time for deployment, failed deployment remediation and BAU house-keeping tasks
— Implement additional architectural redundancy to increase fault resilience
— Review and refine existing disaster recovery processes and ensure new change is reflected in recovery playbooks

Security

Increased and sustained levels of remote working, potentially increases attack surfaces and can affect an organisation's overall security posture. Amongst the increased risks that must be tested are:
— Increased volume of password resets and account creation / reactivation
— Ability to share documents and sensitive data offline
— Impact to functionality and performance of software / hardware security patching
— Use of personal devices

Usability

The focus on rapid deployment of new functionality must also ensure delivery of:-
— Usable change - familiar, intuitive and engaging experiences
— Accessible change to ensure the CX is protected

Testing practices must support verifications for the quality of new change, from the customer perspective, at pace.

Maintainability

The following items consider the extent to which solutions can be observed and maintained:-
— Observability:-
  - Solution should allow deviations from "stable states" to be tracked and alerted on
  - Ensure monitoring covers all new change
  - Testing routines must evaluate accuracy of operational dashboards
— Maintainability:-
  - To enable digital channels to support new operations, design and development principles must be evaluated and improved

Portability

Increased reliance on the availability and stability of solutions requires that, in the event of an outage:-
— Solutions should be proven to be able to be transferred to alternative platforms quickly
— Maintenance of standard operating procedures and the extent to which validated IaC (infrastructure as code) is in place should be assessed

Compatibility

New change introduced must not affect the congruent nature of the technology estate
— As previously non-core systems now become essential, assessments are required against architectural design decisions relating to system co-hosting
— Carry out assessments of the business impacts of failure and need for segregation of co-hosted systems to protect the integrity of the altered live operation

Summary

The following details the operational areas that should be validated to ensure Enterprise Resilience during the current crisis

Agility is key: to respond to the dynamic nature of the situation, Testing Practises must evolve quickly to support **the safe introduction of change** and to provide effective support for production incidents

Review **maximum concurrent licences** for business critical systems and ensure new peak requirements can be supported

To build a consolidated view of resilience across the operation, **3rd party resilience** must be evidenced to ensure the integrity of critical system integrations

Understanding and protecting the **critical business processes** and the technologies that support them, will ensure business continuity during failure scenarios

Place specific emphasis on testing **the remote working "technology-set"** (e.g. VPN, communication, document management and cloud compute) has the size and scale to support the uplift in traffic and maintain productivity

Recovery procedures must be tested, refined and maintained to keep them in line with the functional and architectural changes applied

Testing **the "edges" of the data centre** (VPNs and end points) is particularly important to ensure they have the scale to support new and increased stresses on entry points

Monitoring is key to understanding the **current health of the service** & to allow accurate projections for new operational modes

Capacity Management must be a primary area of focus to ensure headroom exists for systems that are now required to support significantly altered usage patterns

KPMG Non-Functional Testing Services

KPMG Non-Functional Testing Services enable our customers to achieve operational resilience by assuring the accessibility, performance, security and rapid recovery of their IT change.

NFT Strategy Services

Provides guidance to our customers when navigating the significant challenges of defining and evaluating a solution's non-functional requirements. The service offers periodic service quality assessments and independent delivery assurance throughout programmes of change.

— Non-Functional Requirements Advisory

— Delivery Assurance

— Service Quality Assessment

— Performance Engineering

— Performance Testing

— Capacity Planning

Performance Assurance Services

Spans the entire lifecycle of IT change – we analyse designs, help to define solution requirements and extensively measure and optimise performance from the component level across the entire solution architecture.

Operational Resilience

Customer Experience Services

Combine testing expertise and analytics solutions. We use high-value customer insight to inform and scope customer-centric testing; this drives inclusion, retention and growth to ensure the delivery of intuitive, personalised and accessible customer experiences.

— Customer Intelligence Analytics

— Accessibility Assessment

— Usability Testing

— Recovery Testing

— Failure Testing

— Application Security Testing

Resilience Services

Deliver testing expertise to accelerate the speed of recovery by evaluating and enhancing application security, failure and disaster recovery procedures.

KPMG Testing Services

What do we do?

We can help improve your QA and testing capability, to enable successful business outcomes

We can reduce the delivery risk of complex transformation programmes by managing or delivering the testing components

Why use KPMG Testing Services?

Our cross-sector expertise – we bring the whole of KPMG to an engagement, leveraging deep industry expertise across multiple sectors to enhance the technical skills of our testing specialists

Our investment in innovation – we believe in the value of innovation over large off-shore body shops. As a result, we have created a series of high value propositions that help our clients to accelerate business change

Our award winning team – named Leading Software Testing Vendor in 2019 and winners of the 2018 Test Management Team of the Year at the European Software Test Awards

How do we do it?

Our key services lines enable us to:

Assess the effectiveness of your testing

Optimise your testing capability, including application of our *Accelerated Testing* automation framework

Manage your testing projects, to help successful delivery

Deliver test services directly, including test design and execution

Daryl Elfield
Testing Partner
daryl.elfield@kpmg.co.uk
+44(0)20 731 6330

Xavier McGlynn
Senior Manager
xavier.mcglynn@kpmg.co.uk
+44 (0)7786 125755