

# Software testing in the Cloud

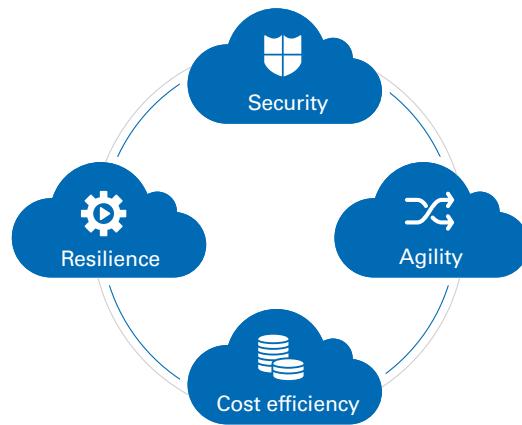
## KPMG Testing Services

The adoption of cloud services continues to accelerate, across all industries.

Cloud technology is no longer regarded as emerging; instead, its maturity is continuously growing and today there is no organisation that has not had contact with some sort of cloud service, whether consumed as IaaS, PaaS or SaaS.

Amongst the factors that lead businesses to adopt cloud services are the advantages it offers, primarily these are:

### Potential Cloud benefits



**However, realisation of these benefits is not guaranteed.** Fully engraining QA, at every stage of cloud adoption and operation, must be an overriding mandate. This means businesses must carry out robust QA planning and specification to ensure the Cloud business case is successfully delivered.

Furthermore, businesses must be acutely aware of the increasing levels of **regulatory scrutiny of Cloud**. Regulators expect to see proof that organisations have **fully formed and applied Public cloud strategies** for data, resilience and cloud exit. A key vehicle to provide the evidence regulators need is high quality cloud testing regimes and this is another reason **testing is high on the Cloud agenda**. Hyperscale cloud service providers acknowledge this, and understand that essential to accelerating the time to value, is successful navigation of industry challenges, aligning C-Suite strategies to business outcomes and accelerating business transformation through quality centric initiatives.

# Cloud computing risks

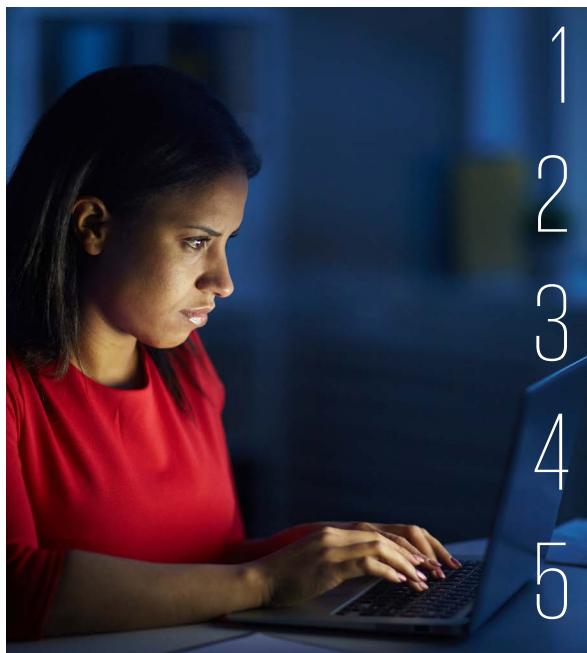
An in-depth understanding of the cloud risk profile will allow for robust mitigations to be put in place. This protects the platform from unwelcome sanctions, loss of revenue and reputational damage.

Testing plays a prominent role in ensuring risk can be effectively and efficiently mitigated and will be central to the realisation of an enterprise-wide resilience capability.

Cloud computing risks		Mitigation through testing
Business risks	Inadequate adjustments to Governance models to accommodate cloud factors introduces risks to the validity of policies and procedures and asset management.	Early engagement of testing expertise allows cloud governance models to be developed to include critical testing considerations.
Governance	Non-compliance for industry regulations – obligations include GDPR, availability and timely end of day reporting. This is applicable to an organisation's estate and its 3rd party integrations.	NFR elicitation and refinement ensures that cloud testing approaches fully address regulatory considerations in the context of Cloud.
Compliance	Unmitigated cyber risks leads to diminished customer confidence, penalties and loss of revenue. Examples of Cyber risk include: phishing, ransomware, malware and 3rd party data breaches.	Cyber threat modelling, security design assessments and testing expose and mitigate vulnerabilities associated to cloud technologies.
Cyber security	Uncontrolled cloud costs, examples include:- over provisioning, poor cloud resource management, inefficient/unoptimised applications and a lack of cloud cost tracking. In addition, vendor lock-in constrains the ease of course alterations to alternative and more cost efficient cloud platforms.	Performance and Resilience testing allows accurate capacity planning. Portability testing will mitigate technological restrictions on future re-platforming.
Cost management		
Technical risks		
Platform security	Undetected, unmitigated vulnerabilities across infrastructure, application & storage layers.	Early and continuous security testing across the cloud platform will ensure security frameworks eliminate vulnerabilities.
Resilience	Availability issues arising from instability, lack of fault tolerance & sub-optimal recovery procedures on the primary cloud platform and 3rd party integrations.	Failure testing increases fault resilience and ensures impacts are contained within specified tolerances. Testing also increases the efficacy of recovery processes and procedures.
Performance	Poor customer engagement arising from slow and unstable applications. Inability to leverage cloud elasticity to scale platforms for business growth.	Real-world, customer focused performance scenarios ensure equivalent performance levels irrespective of customer access methods and locations. Early performance profiling enables solutions to scale to support emerging throughput demands.
Control	Lack of control over and transparency of SaaS applications. Impacts of enforced version upgrades are not evaluated or evaluated too late.	Ensuring that testing practises neatly align to the selected cloud deployment will allow efficient and effective testing to be carried out.

# Cloud testing challenges and benefits

**Traditional approaches have been found to be misaligned to Cloud** and do not leverage all of the benefits to testing that it can offer. The challenges of testing Cloud must be overcome before full benefit realisation can be achieved. These challenges include:



**Developing a clear understanding of specific quality risks** associated to the Cloud Strategy and aligning the Test Strategy to mitigate those risks.

**Controlling the uptime and management costs** associated to parallel running of multiple test environments, often near or at production scale.

**Teams possessing non-functional testing skills** that understand how cloud compute, storage and networking differs from traditional architectures is crucial to ensure testing is effective.

**Integrating legacy estates and test practises** within hybrid cloud models. To fully maximise the testing benefits Cloud enables, legacy testing practises must also be optimised.

**Establishing a capability for continuous testing** is challenging to comprehensively implement but can deliver significant efficiency gains. The execution of mandatory manual test cases must be accommodated in the context of CI/CD.

## How Cloud Benefits Testing

Public cloud presents new opportunities to make testing more efficient, collaborative and drives greater cost efficiency. Cloud benefits testing in the following ways:



### Efficiency

- Rapid test infrastructure (de)/provisioning
- Automated test data generation
- Time to insight by leveraging native cloud monitoring & alerting
- Cloud is an enabler for Agile testing approaches



### Cost

- On-demand (SaaS) test tooling
- Rapid test environment configuration
- Reduced cost of defect fixes
- Management of production sized test environment uptime

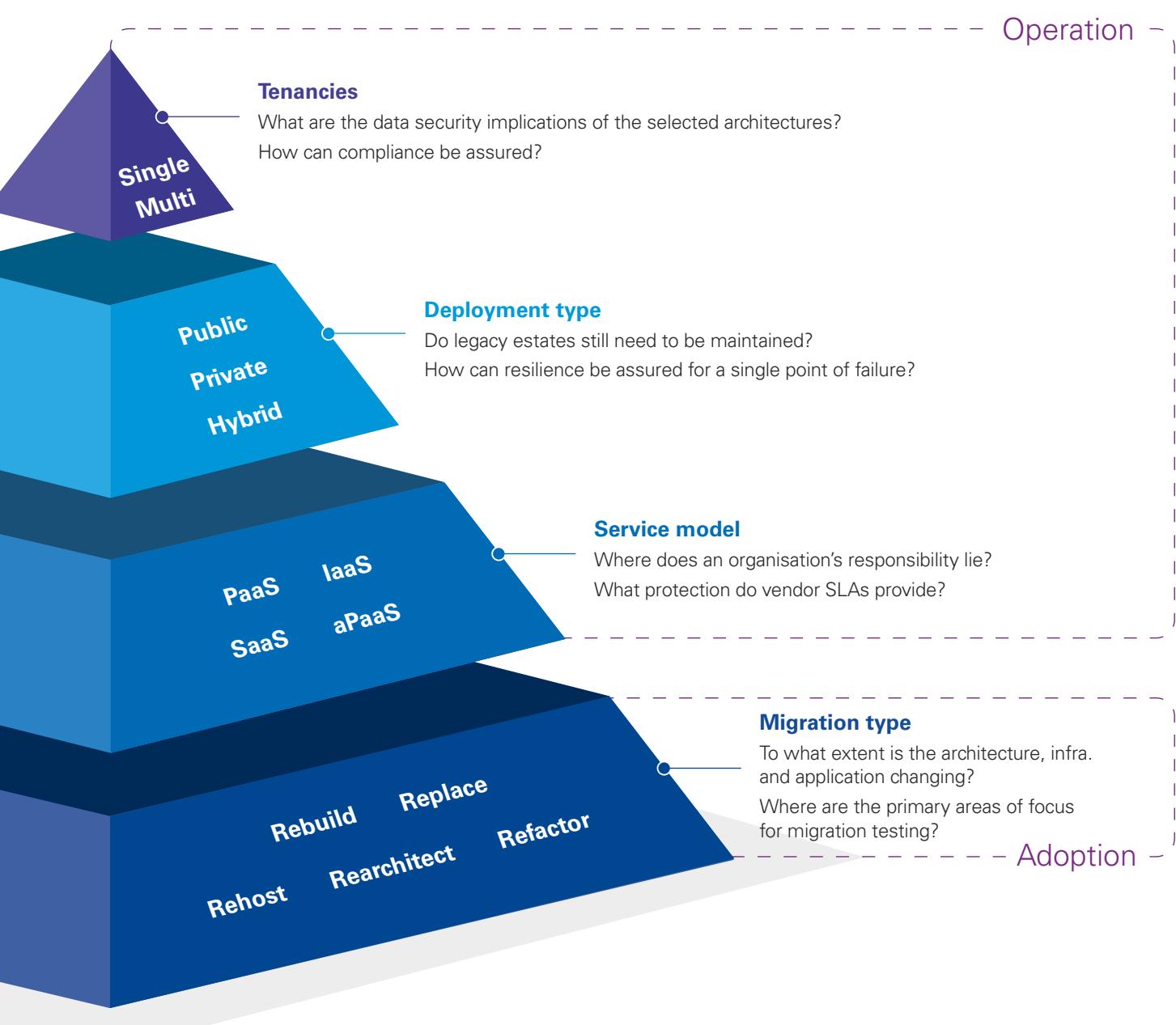


### Collaboration

- Shared assets
- Shared insight
- Transparency of progress and inhibitors
- DevOps aligned ways of working

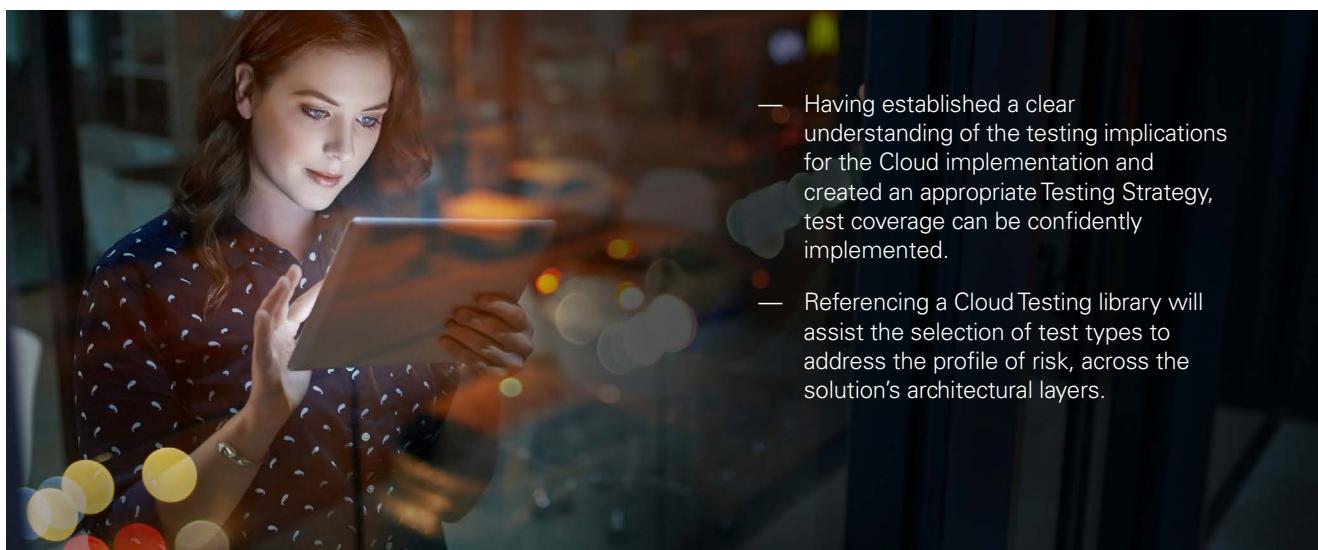
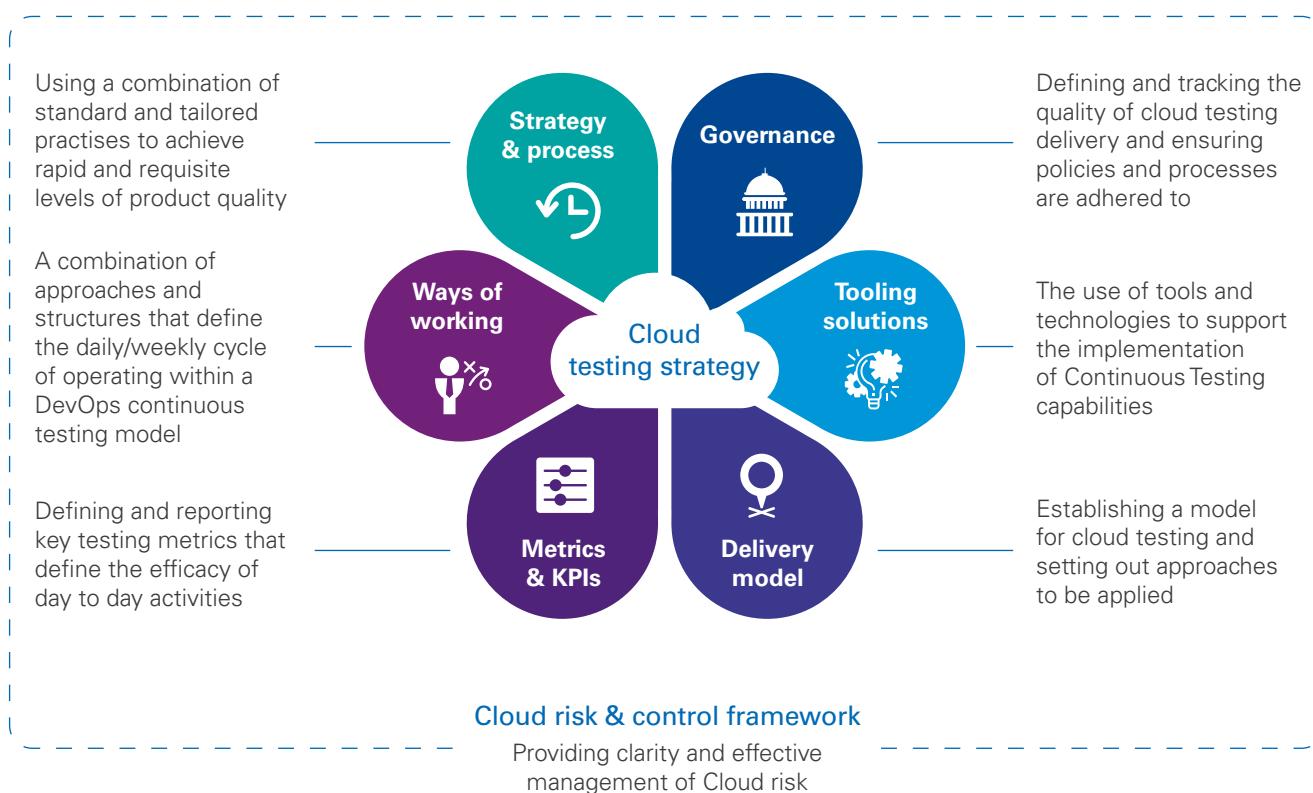
# Cloud implementation types and models

There are many options available to organisations that are adopting and operating cloud business services. The priority and focus for testing changes, based on each situation. To ensure that testing will address the right risks, the quality implications for cloud technology choices must be fully understood:



# Key inputs into the Cloud Test Strategy

To support the stable operation of the live service, the Cloud Testing Strategy must align to and leverage all aspects of the Cloud. This includes ensuring the following items are comprehensively addressed and represented in the strategy:



- Having established a clear understanding of the testing implications for the Cloud implementation and created an appropriate Testing Strategy, test coverage can be confidently implemented.
- Referencing a Cloud Testing library will assist the selection of test types to address the profile of risk, across the solution's architectural layers.

# Cloud test coverage

Appropriate cloud test coverage will take into account a host of factors. Upon selection of the right level of coverage, achieving optimal levels of automation is key to the efficiency of testing. A broad set of cloud testing types are detailed below:

## Cloud test catalogue

Infrastructure	Dynamic Build Test Coverage					
	Storage	Network	Compute			
Static Infrastructure Scanning	<ul style="list-style-type: none"><li>– Security</li><li>– Code quality</li><li>– Compliance</li><li>– Performance</li><li>– Cost efficiency</li><li>– Fault tolerance</li></ul>	<ul style="list-style-type: none"><li>– I/O latency</li><li>– Caching</li><li>– Replication, Back up, Archive</li><li>– Failure &amp; Recovery</li><li>– IAM</li><li>– Audit &amp; Logging</li></ul>	<ul style="list-style-type: none"><li>– Network latency</li><li>– Firewall rules</li><li>– Routing</li><li>– IAM</li><li>– Cluster Management</li><li>– Load Balancing</li></ul>	<ul style="list-style-type: none"><li>– Connectivity</li><li>– I/O latency</li><li>– O/S</li><li>– Failure &amp; Recovery</li><li>– Port scanning</li><li>– Elasticity &amp; Scalability</li></ul>		
Static Application Scanning	<ul style="list-style-type: none"><li>– SAST</li><li>– Code quality</li><li>– Accessibility scanning</li><li>– Software composition analysis</li></ul>	Dynamic Application Test Coverage	<ul style="list-style-type: none"><li>– API functionality</li><li>– Throughput</li></ul>	<ul style="list-style-type: none"><li>– SQL latency</li><li>– Volume</li><li>– Batch</li><li>– Availability</li><li>– Replication</li></ul>	<ul style="list-style-type: none"><li>– UX Under Load</li><li>– Accessibility</li><li>– Cross Browser</li><li>– Cross Device</li><li>– User Security Roles</li></ul>	<ul style="list-style-type: none"><li>– Release</li><li>– Recovery</li><li>– UAT</li></ul>

The areas where testing focus should be prioritised is important to ensure risks are addressed quickly and effectively. The fundamental consideration for testing coverage definition is the **Service model** that underpins the platform:

## Variations on testing focus

Service model	SaaS	PaaS	IaaS
	<ul style="list-style-type: none"><li>– SaaS app configurations</li><li>– Integration customisations</li><li>– Operational Acceptance Test</li><li>– Data security &amp; compliance</li><li>– Integration performance</li><li>– Usability</li></ul>	<ul style="list-style-type: none"><li>– Application Testing</li><li>– Integration customisations</li><li>– Data security &amp; compliance</li><li>– Infrastructure security</li><li>– Application security</li><li>– Integration performance</li><li>– Cloud elasticity</li></ul>	<ul style="list-style-type: none"><li>– Regression App. Testing</li><li>– Bespoke integration layer</li><li>– Legacy customisations</li><li>– Infrastructure security</li><li>– Multi-tenant data security</li><li>– Infra. performance</li><li>– Infrastructure sizing</li></ul>

# How we can help

KPMG addresses quality assurance for Cloud implementations by applying end to end and discreet services to ensure the right risks are optimally and extensively mitigated.



## Cloud Test Strategy

We produce tailored testing approaches to address general and specific cloud risks associated with the implementation. We recognise that **Continuous Testing** is a key enabler for the overall success of DevOps and have developed solutions, capabilities and methodologies that help our clients efficiently implement CT practices.



## Cloud Testing Capability Assessment

Our tiered Test Assessment Service evaluates programme testing maturity and capability against '**best in class**' **testing standards**. We use a combination of observations, stakeholder interviews and programme documentation/processes reviews to rapidly assess testing and delivery risks.



## Cloud Quality Engineering

We apply our extensive technical expertise to test and optimise cloud infrastructure and applications across all test disciplines including: **Functional, Performance, Security and Failure**.



## Cloud SaaS Testing

Using a combination of **powerful tools, applied methodology and technology accelerators**, we maintain and execute comprehensive, pre-built automated test libraries for SaaS CRM, Finance, HR and Procurement solutions to fully assure quality levels.



## Enterprise Cloud Testing Capability

# Our Cloud Testing service is connected across our firm

Our cloud testing service is solidified through deep integration with our connected KPMG value propositions:



## Cloud Technology Resilience

KPMG has developed an **enterprise-wide operational resilience** approach to enable firms to embed resilient practices. We apply our framework to inform testing priority and focus which assures resilience of critical cloud business services across the technology estate.



## KPMG Cloud Transformation

**A complete suite of Cloud services** that enables faster and safer journeys to the Cloud. Whilst quality is embedded throughout, testing leverages key service features to ensure high quality and compliant implementations.



## Cloud Risk and Control Framework

We apply our proven Cloud Risk & Controls Framework and transformation approach to help organisations understand, **mitigate and effectively manage risks through testing**. We establish new ways of working and help to embed quality assurance.



## Cloud DevSecOps Engineering

KPMG brings together our **industry leading risk, compliance, and security competencies** to enhance the infrastructure as code ecosystem for our clients' implementations



## KPMG Connected Cloud Customer

Our Connected Customer practice supports our clients to become customer-centric, digitally enabled organisations. A key areas of focus is **Customer Journey Transformation**. Testing supports the service through our UX Testing Services (usability, accessibility and front-end performance testing).



## Connected Cloud Capability

# Summary remarks



Cloud testing brings **unique challenges**, they must be acknowledged and overcome before the benefits Cloud can deliver to testing will be realised.



Multiple dimensions and complex situations call for a **deep understanding** of the correct emphasis of testing, this will deliver the clarity and confidence required to move into and operate within cloud environments.



On-premise estates have not reached their end of life, therefore **legacy testing practises** must be revisited to ensure they are aligned to the cloud testing strategy.



Testing on CI/CD pipelines will deliver significant **efficiency gains**, however certain testing e.g. Security, Accessibility, Exploratory must rightly remain partly a manual undertaking.



Quality is a shared responsibility – Cloud offers new opportunities to **increase collaboration** and engrain quality as a behaviour.



To remain credible and valuable in the context of Cloud, **quality engineering skill sets** must be developed to include multiple coding languages, architectural awareness and detailed understanding of the principles of the Cloud.



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



Cloud promises many **benefits over traditional platforms**, realising those benefits are not guaranteed however. Many factors must be considered – quality assurance has a significant role to play.

## Contact us



**Daryl Elfield**  
Testing Partner  
T: +44 (0)207 311 6330  
E: daryl.elfield@kpmg.co.uk



[kpmg.com/uk](http://kpmg.com/uk)



**Mark Corns**  
Director  
T: +44 (0)207 694 5901  
E: mark.corns@kpmg.co.uk



**Priya Raju**  
Director  
T: +44 (0)207 694 5189  
E: priya.raju@kpmg.co.uk

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2020 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation. CREATE | CRT129617