Operational resilience

Testing considerations

January 2021

The fundamental importance of Operational Resilience is understood by businesses that have faced crisis situations, whether they were major IT outages, cyber-attacks, geo-political incidents or any number of physical events such as severe weather, fire or floods. Almost overnight, COVID-19 has become the single greatest threat to the continuity and existence of many businesses. The maturity of an organisation's operational resilience now has the very real potential to dictate whether an organisation will survive.

The Bank of England's aim for Operational Resilience is to **"Improve the ability of the financial services sector to absorb the impact of an unexpected event while continuing to perform its most important activities for the UK economy".**
Charlotte Gerken, Director, Bank of England, June 2017

The Bank's Prudential Regulation Committee and Financial Market Infrastructure (FMI) Board focus on the operational resilience of the firms and FMIs they regulate.

The operational resilience strategy consists of three key element:

Targeting the right things

Building resilience

Response and exercising

Operational threat	Overview
Cyber attacks	Malicious attempt to damage or disrupt a computer network or system, for example DDOS (distributed denial of service).
Customer events	Specific days and times when applications are overloaded, increasing the potential for system outages.
IT change	A system change can impact the resilience of key organisational processes.
Third party	The failure of a third party vendor in providing IT services, such as cloud platforms can lead to disruption.
Natural hazards	COVID-19 has highlighted the need for organisations to focus on resilience against threats from naturally occurring events.

Technology considerations

As companies continue to embrace digital transformation, they need to effectively manage the technology implications to be operationally resilient.

Cyber attacks	**Service availability**	**Cyber security**	**Infrastructure management**	**Disaster recovery**
IT changes	**Service availability**	**System reliability**	**Infrastructure management**	
Natural hazards	**Disaster recovery**			
Third party	**Cyber security**			
Customer events	**Disaster recovery**			

Service availability
Understand the impact Recovery Time Objectives (RTO) based on planned and unplanned events.

Cyber security
Use of "Cbest" to measure the levels of cyber resilience an organisation has achieved.

Infrastructure management
"On/off premise" infrastructure architecture strategy built on quality and security principles.

Disaster recovery
Cloud based architectural redundancy can avoid service failure impacting key customer journey processes.

System reliability
Reduce recovery lead time and positively influence the solution's uptime through improvements in monitoring, alerting and root cause analytics.

Testing considerations

Technology considerations	Testing considerations
System availability	– Create and implement test strategies which implement and measure the success of formal Failure Mode and Effects Analysis (FMEA) and Fault-Tree Analysis (FTA) processes. – Implement test frameworks to effectively identify and prioritise tests that simulate the ways a system can fail based on FMEA and FTA analysis.
System reliability	– Utilise reliability testing frameworks to follow the Modelling, Measurement and Improvement methodology. – Organisations will need to utilise load testing along with traditional feature and regression testing to fully analyse the ability of a system to meet its reliability requirements.
Cyber security	– Organisations need a complete cyber security strategy, to enable SME staff members to prevent or minimise impacts of cyber attack. – Considerations towards penetration testing, security scanning, ethical hacking, and risk assessment will form the forefront of a cyber security strategy.
Infrastructure management	– Ensure testing of existing and new procedures in suitable/ representative pre-prod environments is included within the release plan and is therefore integral to the definition of a shippable solution. – An organisation will need to test at scale the ability to roll out upgrades to software, through aligned domains and standardised packaging scripts.
Disaster recovery	– Consider using chaos testing and black swan scenarios to measure and increase levels of resilience. – Consider what inputs from testing can be made available to inform the definition of "operational steady states" in production to allow proactive alerting on threshold breaches.

Testing challenges

Challenges	The KPMG way
Lack of due diligence towards cyber security testing may lead to application security vulnerabilities.	– Implement a cyber security test strategy within the organisation. This should include having a cyber security team handling security related threats.
System performance can be compromised during seasonal intensity, particularly those applications connected to management.	– Performance by design, through the use of Continuous Integration (CI) / Continuous Delivery (CD) pipelines should be integral to architectural design and application development practises. – Implementing advanced monitoring and alerting solutions (APM) to increase the breadth and depth of performance insight.
Business as usual processes can cause disruptions through system upgrades, patch installations and modifications.	– Subject matter analysis of domain knowledge and testing expertise to provide seamless services for our customers. – Cloud enablement services for managing and testing solutions.
Digital change and transformation to the IoT solution framework will cause risk to existing standalone platforms.	– Assess, quantify and implement a testing approach for new and unmitigated risks that the transformation programme exposes the organisations to. – Develop a top down framework of resilience embedded across the organisation.
Third party vendor disruption can lead to storage/ hosting downtime.	– Test assurance and health check services to evaluate quality of third party service delivery and to compare to industry standards with a prioritised list of recommended service optimisations.

KPMG's unique mix of testing specialists, industry SMEs and our 'Accelerated Testing' framework can reduce the cost of change by up to 25%. **For more information on how KPMG can help with your Operational Resilience initiatives, please get in touch.**

kpmg.com/uk

Daryl Elfield
Testing Partner
T: +44 (0) 20 7311 6330
E: daryl.elfield@kpmg.co.uk

Andrew Husband
Partner, Operational Resilience Lead
T: +44 (0) 7771 337960
E: andrew.husband@kpmg.co.uk