UKAuthority Briefing Note

October 2020

In partnership with

rackspace technology & vmware

A new dimension for business continuity

How the Covid-19 pandemic has affected the demands on disaster recovery and business continuity planning in the public sector

Contents

1. Introduction

The covid-19 pandemic has changed perceptions of business continuity (BC) – in the public sector as much as anywhere. As the lockdown began it became clear that the major disaster recovery (DR) priority of the past, to provide an alternative working space when people could not get to their desks, did not apply. Instead it threw the emphasis onto home and remote working – and continuity: ensuring that people could continue to access networks and applications and do their jobs when any communal workspace was out of bounds.

This has accelerated a shift in the balance of thinking about both DR and BC, away from buildings and towards people, and that has deep implications for infrastructure, strategies, the assessment of cost against risk and the testing of plans. It has also highlighted the importance of cloud services and scalability in BC planning, forcing organisations to look carefully at whether they are well prepared to quickly adapt to an emergency scenario in which many staff are logging into systems remotely.

While the earlier concerns and the need for DR plans cannot be ignored, the possibility of further lockdowns and a long-term reduction in office working is creating the need for new approaches to ensure BC in the first instance. And there is a growing awareness of the need to embed it more deeply within organisations, making the case for 'BC by design' within each element of operations.

This paper addresses the key factors and identifies priorities for the public sector as it faces up to the long-term effects of the pandemic on its technology infrastructure.

2. A different type of infrastructure

Developments in technology have had an effect on BC plans since befowre the pandemic, as the steady emergence of the 'bring you own device' (BYOD) approach to hardware, the increasing resilience of mobile networks and growth of cloud services have all provided new options. Plenty of organisations have taken the scope for all this into account, but often on the assumption that it will apply to a minority of their staff at any one time. The pandemic, however, has created a situation where it has become the default – at least for office based employees – and demanded a massive scaling up of the use of in-house applications through private networks and cloud services accessed through the internet.

This has come with a shift in assessing the value of data centres. Traditionally, organisations have often run a dedicated data centre with a second in place or an arrangement with a third party, as a back-up data centre, with the replication of its data as a DR measure. This laid the ground for the continuity of service in the event of disruption, but at a high cost, requiring an investment in infrastructure for a facility that would seldom, if ever, be used.

New horizons delivered by cloud

New options have emerged with the possibility to use cloud platforms such as AWS and Azure as the secondary repository of data. This can match the flexibility of a secondary data centre in making it possible to quickly resume disrupted services, while reducing the need for up-front investment and taking out some of the associated costs. The latter includes the management of the secondary facility, testing its capabilities, physical security operations and the provision of an uninterruptable power supply – all resource-intensive features.

There is also the possibility of running down the primary data centre and relying completely on cloud services, with the cloud provider taking prime responsibility for the factors above. But this needs a new element of management and a significant effort in ensuring that the arrangements align with the organisation's BC plan. This adds to the need to optimise the use of cloud services, requiring skills that many public authorities are still trying to develop, and often turning to a third party to provide.

Options have increased further with the growth of hyperscalers – the major companies that run hundreds of thousands of services and provide infrastructure, platform, public and private hosted cloud services – and make it easier to spread the load between different clusters of servers in different locations. This reduces the risk of a single point of failure in an organisation's IT infrastructure, and removes the redundant capacity in the two data centre model. Both clusters are used simultaneously for different purposes but can take over from each other in event of a disruption, thereby cutting wastage in computing costs. It effectively combines BC planning with a more cost-effective operational model.

Hybrid flexibiilty

It has also raised questions about the right balance between using public and private cloud applications, with the former involving the unwelcome possibility of processing capacity being affected by a surge in demand from other tenants.

A wholesale shift to private cloud could prove to be an expensive approach, and the situation has been further complicated as some public authorities have moved applications back on-premise from the public cloud, believing it gives them tighter cost control and a better view of how to optimise their digital operations.

There is scope for a solution in using platforms that make it possible to connect and manage applications on any cloud – public, private, on-premise - depending on their technical and business requirements, and to move them between these clouds as needs dictate. This makes it possible to manage a hybrid cloud infrastructure from a single platform, monitoring changes in processing activity and the performance of applications, and adapting them to respond to changes in traffic from a remote workforce. It is the ability to change that reinforces the continuity of a service, making it possible to switch to an environment that can handle a big increase in remote access.

It does not have to ensure maximum availability for any application, as BC planning involves judgements on the criticality of different operations, but it provides the scope to design around ensuring those that are priorities are prioritised, and guaranteed to be continuously available. The important thing is that it involves clouds with the capacity to handle a burst in activity without a significant delay.

3. Devices and connectivity

Another increasingly important element of the infrastructure element of BC is the provision of appropriate devices, and connection protocols, to ensure that staff can work securely from home – or wherever needed. For some organisations, one part of their response to the pandemic was quickly having to source large numbers of laptops or tablet computers with the right operating systems and sufficient processing power to access and use all the usual applications – but with mass global demand this caused supply issues. While some are happy to allow staff to use their own devices, they cannot take for granted that everybody will have a suitable device; and there are cases in which IT teams have to check that the security applications are in place and working properly.

BYOD and mobile working must be embedded

This has been done as an emergency response, but the pandemic has highlighted the need to embed this into core BC planning. There are risks and benefits, including cost, on either making hardware available to all staff or enabling BYOD.

Regardless of device, there is a critical need for robust log-in processes, either to enter a virtual private network or applications running in the cloud. Entering a password can be sufficient when working on-premise, but remote working can demand more stringent measures such as multi-factor authentication or the use of biometric log-ins.

Along with this is the need to ensure that people have adequate connectivity at home to continue working. This is a more difficult problem to deal with and, in the event of identifying some people who live in areas where there are still problems with broadband connections, the planning may have to include the reassignment of roles during a disruption.

4. Targeted support

Architecting for continuity is a complex business and an expert partner can be a big asset in managing these issues – one that can provide the 'glue' between the organisation and its cloud suppliers to provide the resilience in infrastructure, including the ability to scale up capacity on demand – and down again when no longer needed.

Rackspace Technology has specialised in this, working with cloud suppliers to understand the capabilities of different services and how this can provide resilience around the application layer for public sector bodies. It can outline costs and how to optimise the use of a cloud infrastructure to support applications, effectively providing a 'one stop shop' to bring it all together.

This can take the form of shifting data in applications between servers from different suppliers at different locations, using a complex network to distribute the load in a way that prevents any denial of service. It can ensure that if one service fails another can automatically take over, providing a key element of BC planning.

This not always easy, but it is achievable, and such partnership support can play a crucial role in ensuring that services remain continually available.

5. In action: Harnessing cloud as lockdown hit

Rackspace Technology helped develop and implement solutions for a number of public sector customers as lockdown shocked the nation in March.

NHS trust moves 2,000 staff to home working via cloud

In one case it worked with an NHS trust in the early stages of the pandemic to ensure that it had the IT capacity to support home working for up to 2,000 workers.

This involved a three-node cluster of VMWare Cloud on AWS running a VMWare Horizon virtual desktop infrastructure (VDI) application integrated with a native AWS virtual private cloud (VPC). The cluster has a hybrid connection to the trust's existing hosted data centre and virtual private network (VPN) to allow access to applications.

The company worked with VMware and AWS solution architects to finalise the design and architecture, and completed the build to deploy the VMware Cloud and AWS environments. It then completed the VDI provisioning under a combined statement of work within the contract. It is now providing a fully managed service, including monitoring and incident management across all the components in the solution.

This was done within a tight timescale as the trust had an urgent need for a minimum viable product to support its staff as lockdown measures came into play.

MoD harnesses cloud and internet facing services for continuity

The rapid shift to home working in the Covid-19 pandemic imposed a new demand on digital services at the Ministry of Defence, where around half of its staff did not have the appropriate devices for home access to its MoDNet secure network and the applications and services it provides.

It responded with a major shift to internet facing services, partly through the use of a Joint Server Farm operated by Rackspace Technology, which made it possible to scale up its requirement and maintain access to Defence Gateway Services for 300,000 users. It also developed a 'vanilla' service on Office 365 with limited functions and extra security requirements. Although separate to MoDNet, this has made it possible for users to look up and communicate with people on the network.

One consequence of this has been that military personnel have now been able to access administrative tools through mobile devices rather than having to queue at kiosks for access to MoDNet. It has also accelerated thinking in the Ministry about how to make more of mobile technology and cloud services, with a perception that it will maintain a significant level of home and remote working even as the pandemic eases.

This is part of a shift in thinking away from disaster recovery and towards business continuity.

6. The human element

While DR and BC planning has traditionally focused on technology, the pandemic has highlighted the human element. People need more than the right equipment and access to systems to do their jobs, and organisations have to think about how to support them through the disruption.

One of the most common observations has been that people have done better in responding when they are using familiar technology. When a cloud infrastructure helps to facilitate the easy transfer of applications it does a lot to ensure that employees can work with them as usual, rather than having to follow different paths for a process and work with unfamiliar interfaces. The shift to using remote technology can sometimes make changes necessary, especially if it involves using smartphones or tablets, but if systems are designed to provide a similar user experience it should minimise the disruption.

Similarly, moving from an in-house system, accessed through a VPN, to a cloud-based platform can necessitate some change. If this is the case, there has to be a plan for rapid training and peer support to get the best out of the users.

The widespread shift to video conferencing has also required elements of people management. Not only have people needed to learn how to use the systems – which should not be a major demand – but there are cultural factors in how they behave during an online meeting.

Many digital leaders have commented that people have become a lot more ready to show themselves onscreen than before the pandemic, and it may be necessary to encourage any laggards to follow as part of ensuring that everybody makes a full contribution.

Along with this there have been plenty of observations about mental health issues among some staff when they are isolated during lockdown. This is increasingly being seen as part of the BC dynamic, and if, as many expect, there is a long term shift towards home working there will be a need for closer relationships between BC planners and HR teams to pre-empt any problems.

7. Cost versus risk

The pandemic has also thrown a thresh light on the cost versus risk dynamic that underpins BC planning. Organisations should identify the potential for disruption in every area and for any eventuality. They must lay plans following stringent assessment of the possibilities of any specific problem arising; the effect it could have on the organisation; what steps are necessary to mitigate against it; and the cost of putting these plans into effect.

There is bound to be a point at which it becomes necessary to live with the risk on the understanding there is a remote chance of it happening. There is also a need to assess the likely level of disruption and whether it would still be possible to maintain operations to an acceptable standard. This requires looking at different processes, assessing how critical they are to services and the cost of keeping them running in different scenarios. Costs have to be evaluated against risks to different elements of the business, and it can be difficult to measure the risk of an application not being available.

There is complexity in the detail and measuring such 'unknowns' is currently an underdeveloped science, with an absence of any standardised scoring mechanism. But there should be an effort to identify the major issues and major costs and take these to board level in an organisation. They can be seen in a more holistic context and any decisions taken in line with the broad priorities of the organisation.

With this in mind, it is worth noting that the shift to cloud and the ability to optimise the costs of using the services provides for a more dynamic, and potentially expensive approach to BC, which can shift the balance towards meeting costs and reducing acceptable levels of risk.

8. Testing the tests

The pandemic has also highlighted the need to widen the scope of testing for BC plans. Traditionally tests have focused on the issues identified as potential points of failure, largely power supplies, availability of IT networks and applications, and the closedown of buildings. Synthetic monitoring has been applied, using emulations or scripts of transactions using the applications, to identify any weak points in performance, following which corrective action can be taken. With the right process for remediation this could ensure the next round of tests showed the weaknesses had been rectified.

It has never been a silver bullet, has sometimes suffered from deals with vendors that do not provide for any changes once a product has been delivered, and can lead to extra, unanticipated costs. But it has made a significant contribution to strengthening DR plans for many organisations.

Now Covid-19 has introduced this new element in which the option of an alternative central workplace is not sufficient and thrown the emphasis onto home working. This has created an even more complex set of demands for testing that will have to be confronted as new plans are developed.

Efforts will have to take in those factors that have emerged from the big increase in home working, and there are more variables around individual members of staff. Much will depend on whether they have the capability and connectivity to continue their work from home, and it could lead to a requirement for an audit of every employee's circumstances to identify weak points and assess overall capacity.

This will be a big ask, even for large organisations, especially as a robust BC plan calls for routine, not just one-off testing. It will ultimately lead back to the cost versus risk question and a decision on acceptable risk.

9. Metrics and outcomes

Imposing metrics upon BC planning is a complex task, and their accuracy would only be fully tested in the unwelcome event of a disruption. But there is scope for applying them to some areas, identifying the elements of an organisation's operations and priorities and how much would be lost in the event of a breakdown.

There are three factors where the potential stands out:

1. **The resilience of service delivery dependencies** – If one stage of operations cannot be carried out or is severely

reduced, what is the extent of the knock-on effects to other stages?

2. **Continuity of delivery of service to end users and citizens** – How long would a service be unavailable? Or by how much would it be reduced if running at a restricted level? How many citizens depended on a service would be affected by this?

3. **Continuity of delivery of corporate objectives** – How far would a disruption reduce an organisation's scope to meet its strategic objectives or by how long would it slow down the delivery?

Along with this there are factors for which, while it is not always possible to attach metrics, it is possible to make measured judgements on how strong the elements are across an organisation:

1. **Integrated resilience as a cultural norm,** in which everybody involved in planning and managing services is always paying attention to any possible risks to BC.

2. **The provision of flexible and adaptable response, recovery and restoration procedures,** within the realm of traditional DR but extending to the areas that have emerged as significant during the pandemic.

3. **Integrated DR strategies for corporate IT**

An important element of this is to recognise that the conditions, and potential risks, will always be changing. BC planning is not a one-off, and for it to be successful there is a need to identify the changes and adapt the plans to ensure resilience. This approach should be deeply ingrained throughout the organisation to maintain its operations status through any time of crisis.

10. A role within transformation

A handful of lessons have begun to emerge from the pandemic, one of which will have become apparent to those who need to know. BC has to be a boardroom issue, if not for every detail, at least for the major elements of an organisation's plan and how these relate to its major objectives. Organisations that have suffered some service disruption due to Covid-19 should be ready to acknowledge any shortcomings and be ready to charge a senior official with the task of setting them right.

There also has to be clear ownership of BC planning and monitoring of how it is being maintained. There is a view that it is often dispersed between different individuals or teams in an organisation, which leaves the risk of factors being neglected or contractions between different elements. It needs a senior responsible owner for BC with a clear line of authority to coordinate any plans.

In addition, BC planning will be most effective in the long term when it is intrinsic to digital thinking and aligned with transformation plans. Transformation entails change, which will impact factors around resilience and risk, and they all need to be taken into account with every investment and service redesign. Plans to use new applications should make use of the BC facilities within a digital infrastructure, and feed into any thinking about where there may be potential points of failure. And it should all be revisited and revitalised as the digital structure evolves, coming back to the key point that as risks change, so the planning needs to change.

Overall, BC has become a more complex business in the trail of the pandemic and demands fresh thinking in any public sector organisation. It is clear that cloud services are now more important than ever and should play a key role in an updated approach.

11. Further information

Further reports in this series:

1. Smart sourcing insight

Read more about smart sourcing as an approach to best of breed procurement by downloading UKAuthority & Rackspace Technology's report: 'Smart Sourcing Insight - Finding the right balance in outsourcing, insourcing and cloud procurement'.

Produced in association with Rackspace Technology, this report looks at how the public sector can approach the sourcing of modern technologies in a cloud enabled world.
Download 'Smart Sourcing Insight' here

2. Managing digital complexity

Read more about how orgnisations harnessed the hybrid cloud in the immediate response to Covid-19 whilst keeping their horizons open in terms of long term resilience. Again produced by UKAuthority in partnership with Rackspace Technology, you can ***download the report 'Managing Digital Complexity in a Pandemic' here.***

Rackspace Technology

Rackspace Technology is the multicloud solutions expert. We combine our expertise with the world's leading technologies — across applications, data and security — to deliver end-to-end solutions. We have a proven record of advising customers based on their challenges, designing solutions that scale, building and managing those solutions, and optimising returns into the future.

As a global, multicloud technology services pioneer, we deliver innovative capabilities of the cloud to help customers build new revenue streams, increase efficiency and create incredible experiences.

Named a best place to work, year after year according to Fortune, Forbes, and Glassdoor, we attract and develop world-class talent to deliver the best expertise to our customers. Everything we do is wrapped in our obsession with our customers' success — our Fanatical Experience™ — so they can work faster, smarter and stay ahead of what's next.

UKAuthority

UKAuthority champions the use of technology, digital and data by central and local government, police, fire, health and housing, to improve services for the public they serve.

Visit UKAuthority.com to keep up with news and developments in govtech, digital & data for the public good.

UKAuthority hosts regular virtual events exploring best practice and innovation in the public sector.
Visit the UKAuthority events schedule here

UKA Live: Do we need to rethink Disaster Recovery post-Covid?

The contents of this document formed the focus of a recent UKA Live discussion hosted by Helen Olsen Bedford, featuring:

- Colonel M C Cornell, Assistant Head - Information Application Services, British Army
- Carol Williams, Head of ICT and SIRO, Walsall Council / Chair of Socitm West Midlands Region
- Owen Powell, Chief Information Officer, Central and North West London NHS Foundation Trust
- Sppencer Sutton, Solution Architect, Rackspace Technology

You can watch the full discussion here

UKA Live

Do we need to rethink Disaster Recovery post-Covid?

Programme supported by rackspace technology vmware

Guests

Carol Williams
Walsall Council / Socitm

Owen Powell
CNWL NHS

Col M C Cornell
British Army

Spencer Sutton
Rackspace Technologies

HOST
Helen Olsen Bedford
UKAuthority

This briefing note has been researched, written and published by UKAuthority thanks to support from Rackspace Technology.

Authors: Mark Say & Helen Olsen Bedford, UKAuthority

For further information on the contents of this Briefing Note please contact:

- Helen Olsen Bedford, Research Director, UKAuthority: helen@ukauthority.co.uk
- Spencer Sutton, Cloud Solution Architect, Rackspace Technology: Spencer.Sutton@rackspace.co.uk