redstor

Top 7 considerations for choosing a

DATA ARCHIVING SOLUTION

A PAPER BY REDSTOR | APRIL 2018 | WWW.REDSTOR.COM

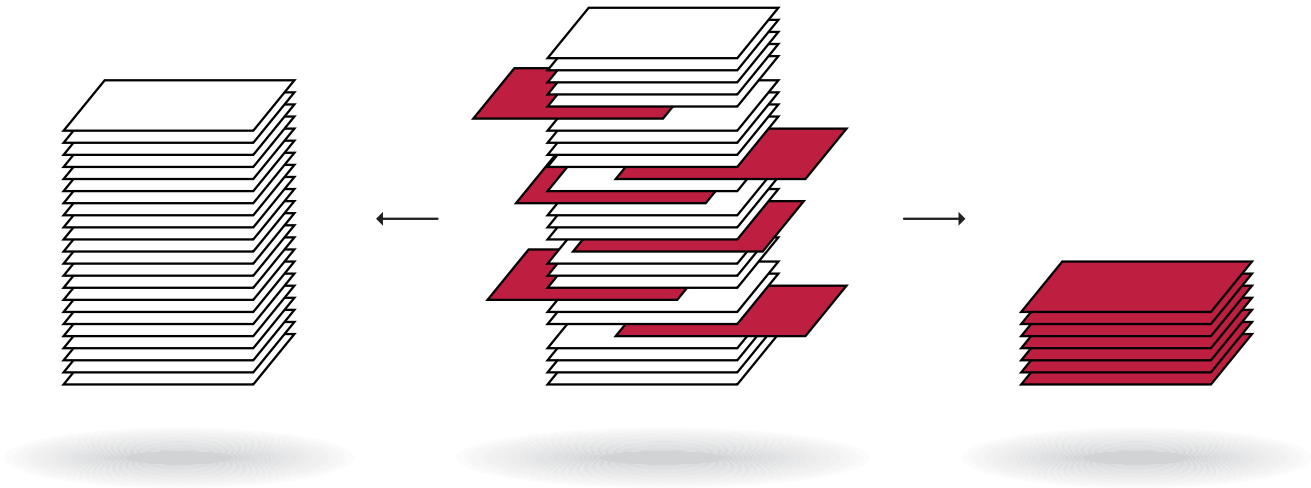
Many organisations are facing challenges relating to the unstructured data they hold. By its very nature, unstructured data is in a form that is difficult to manage, and it is growing rapidly in size. This can make it difficult to understand who owns that data, whether it is being used or even whether it is of any value.

Industry forecasts indicate the volume of data generated by corporates is expected to double over the next three years and, with **General Data Protection Regulation taking effect in May 2018**, organisations need a more efficient way to manage and control this data.

When a piece of information stops changing or is no longer frequently used, it is best to move it to free up valuable primary storage. Archiving rarely accessed data delivers big savings for organisations, particularly those with huge amounts of data.

In many cases data is an organisation's most valuable asset and for many reasons it is vital that it remains highly accessible and easily searchable, not least of which, so that subject data requests can be performed – a requirement under GDPR. That can be problematic if the relevant data has been left sitting on a dusty tape somewhere.

This White Paper provides an overview of the important technical considerations senior business and IT management teams need to review before choosing an archiving provider.



ARCHIVED DATA UNSTRUCTURED DATA ACTIVE DATA

01 Decide whether you want to archive your data on-premise or in the cloud

Archiving in the cloud can be seamless and automated. Historically, on-premise archiving solutions have been tape-based and for organisations with petabytes of data to archive, it is still the most cost-effective method.

Organisations are often reluctant to switch to the cloud because tape itself is cheap. The true price a business pays for archiving, though, can only be calculated when you factor in all the 'grey' costs of administering the tapes.

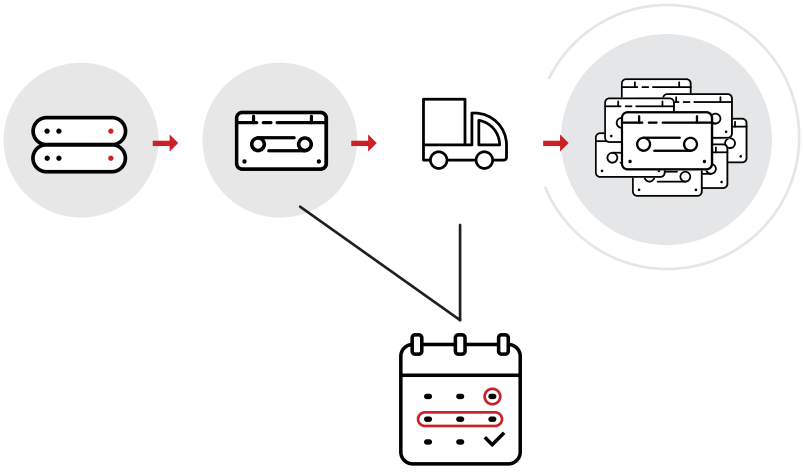
Tape is typically taken away and stored offsite in a vault. The result is that it is not connected to a network. The subsequent delay in recovering or gaining access to data archived in this way makes organisations wary of archiving anything for fear of it being needed. So only really old data is archived, putting a strain on primary storage.

Tape also has a finite lifespan and eventually the time will come when the data will need to be migrated to new media to ensure its integrity remains intact. Consider working with a partner who will assess your requirements and provide a solution that works for your environment and business needs.

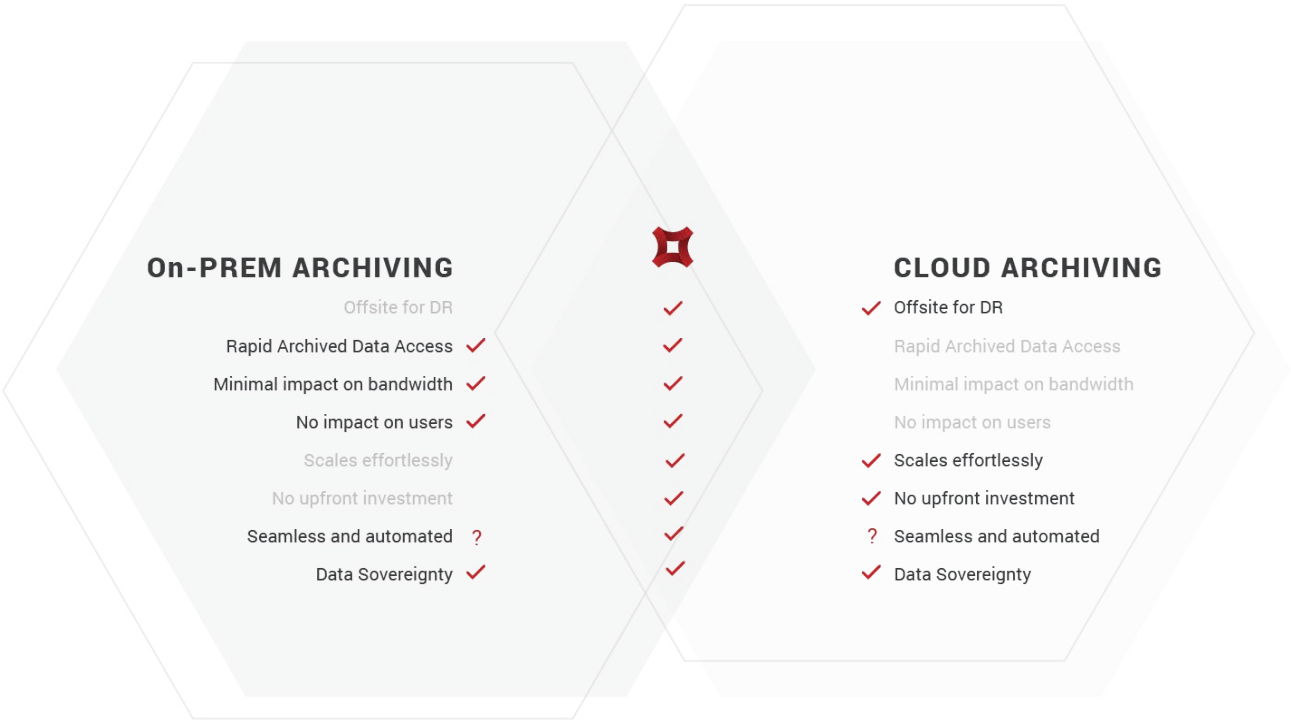
There are many good reasons why the number of organisations adopting cloud solutions continues to grow.

The latest research from the Cloud Industry Forum (CIF) reveals that the overall cloud adoption rate in the UK now stands at 88%.

This is because the cloud often offers a lower cost of ownership, more predictable costs, faster deployment and fewer disruptions in service.



A cloud-based service can eliminate the need to spend hours each week physically managing the data archiving process or securing and transporting tapes. Your company's IT team is free to work on more important projects—rather than monitoring and maintaining the archiving process.



NOT ALL CLOUD ARCHIVING PROVIDERS, THOUGH, ARE CREATED EQUAL.

Modern cloud archiving services deliver all the benefits of the cloud PLUS the best features usually only found with on-premise archiving.

Another consideration with a cloud-based archiving solution is to ensure you retain ownership of your data and the provider does not have access to it.

Cloud-based technology now exists that enables data to be accessed and streamed on demand. Crucially there is no need for users to receive training or change their behaviour at all.

Organisations evaluating their cloud archiving options may want to consider a solution that requires no IT involvement to retrieve data with no delays or special processes for end users accessing data.

When it comes to accessing data, prioritised recovery is key. Ensure there's minimal impact on bandwidth and that there's no waiting for what you need to be retrieved. The performance and overall experience should remain the same for the user.

Redstor's solution, for example, prioritises even bits of files or databases as they're accessed, ensuring even very large files can be accessed instantly as if they are stored locally.

Consider a solution that scales effortlessly with no up-front investment.

Regardless of chosen technology, it is important to ensure that there is a copy of archived data being held offsite for Disaster Recovery. Selecting an archiving technology which features strong integration with a backup and disaster recovery solution can deliver big efficiency gains from a storage utilisation and management time perspective.

There is a lot to consider, including whether it is necessary to use multiple point solutions for each site and challenge. Working with a vendor who can provide expertise and help you procure a solution that fits your requirement can be highly beneficial.

02 Evaluate how easy the archiving solution is to manage and use and how quickly data can be restored

Tape is cheap and more reliable than most people give it credit for and good at holding onto data for really long periods of time.

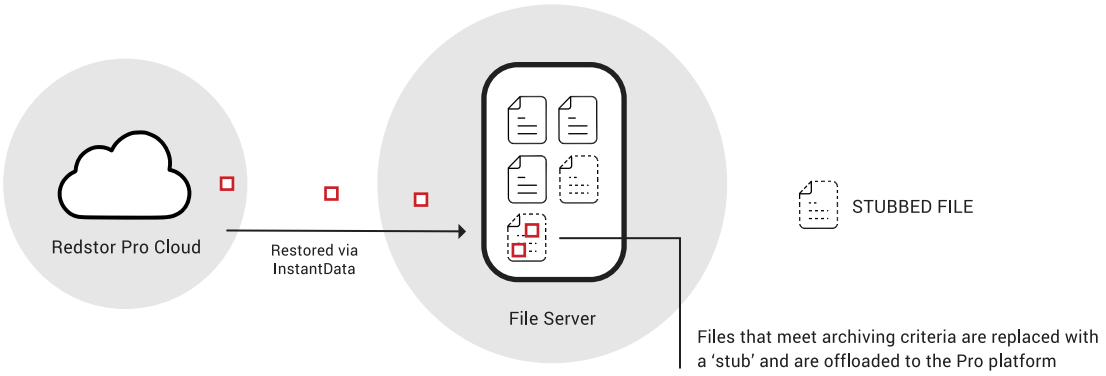
However, data archived to tape in “cold storage”, takes a while to access even if it’s on site - and it will take longer still if it’s held off site, adding to management overheads.

A major benefit of archiving in the cloud is that customers can rest easy knowing that their data remains readily available.

However, when archived data needs retrieving, you need to know employees aren’t left waiting on lengthy retrieval processes or sluggish complete downloads, which cost time in terms of manpower.

Look for a technology that provides easy high-speed access to archived data, enabling you to restore your emails, databases, files and folders in seconds rather than having to hold on for hours - and ideally without end users needing to interact with IT staff, adding to their workload. Being able to access anything you need instantly, simply by streaming it back on demand, brings huge benefits.

For many businesses, it’s not acceptable to have to wait for a full file to be retrieved from a cold archive when access is only needed for bits of an individual file or parts of a database. For example, if you need to work on a 100Kb file from within 20TB of archived data, you want to be able to do so instantly.



Solutions are available that will retrieve the bits of the file you access as you need them without making you wait for the whole file to be recovered before working on it.

When files are archived, it is better for the user if they still appear to be stored on local drives in their original locations and can be opened as normal.

That way the user in the previous example would know where the 100KB file is and would be able to access it immediately - as if it was still stored locally.

It is advisable to mirror all archived data so that it is stored in two geographically separate data centres for Disaster Recovery purposes.

03 Consider a solution that offers backup and archiving together

The cost of deploying archiving, backup, disaster recovery and also a separate solution to address the challenge posed by GDPR - namely that data is secure and searchable - is always going to be a major consideration.

A great way to minimise management overheads, while at the same time increasing visibility, is to choose a unified solution. This is where a provider offers the whole package from one central management interface.

Complete data management – the ability to see a single version of truth from one pane of glass - brings huge advantages and more savings

A unified platform gives complete control over an organisation's most valuable asset, their data. A complete, all-in-one solution makes it simple and easy for customers. There's no need to search across all the different servers, endpoints, platforms, in the cloud or wherever else data might be.

With one central search, customers can find all their data from a single source - the secondary storage data set.

The smarter solution will also help you with data compliance, making it easy to identify where your data came from and when it was gathered.

04 Optimise cost of ownership

According to most estimates, over half of data is ROT - redundant, obsolete or trivial.

Intelligent automation will identify rarely accessed data that is suitable for archiving. Moving infrequently accessed data, including ROT data, into the cloud frees up an organisation's primary storage, reducing costs substantially.

By 2020 the amount of data on the planet will have grown 10-fold in just six years, according to IDC's annual Digital Universe study.

If an organisation buys infrastructure with an intended lifetime of three-to-five years, it is inefficient to be replacing it only a year later because of unanticipated data growth or other unforeseen reasons. In many cases it will be challenging to add to the existing infrastructure so when primary storage is running out, archiving becomes a priority.

For example, an organisation can save time and money by archiving enough data to be able to consolidate from three servers into two.

Ownership of private archive infrastructure is a costly and management-intensive exercise. Archiving is a long-term commitment by its very nature so it is likely that multiple hardware refreshes will be needed

throughout the lifecycle of the data. There are also the extra costs of support contracts and staff turnover to consider.

Look for an archiving service that scans the metadata of files across your entire estate, determining when files were last accessed. So if, for example, data has remained untouched for six months, it can be archived in the cloud.

Be sure, though, to find out whether you have to pay for retrieving archived files. If a service is priced on this basis, the total cost will be difficult to predict. Therefore, it's important to check pricing structures thoroughly.

Some providers may offer what looks like cheap archiving on the face of it, but it may work out to be expensive in the long run if they charge extra to retrieve files, upload files, even interrogate the cloud platform.

Initially a provider may offer free compute time, database usage and storage. However, as a business grows out of the free level, the bills will start to mount up.

If you've already spent months or years on a proprietary platform, packing up and moving somewhere else is not an easy task, no matter how much you're paying.

When making your choice, ensure there is an affordable, transparent price structure. No complicated hidden extras to cover extensions or database licences.

Find a solution that is quick and easy to install, delivering protection in minutes without the need for complex IT training.

05 Think long term

What is right for you now might not be right in the future if the business changes - so be flexible and make sure there is an exit strategy. In the event your company wants to migrate to a new cloud provider in the future, or bring a particular capability back in-house, it is worth establishing now whether the vendor has a pre-determined process for doing so.

Check how easy it is to leave as you don't want to be locked into using a particular hardware or cloud vendor as that may turn out to be expensive in the long run. Making that switch might be harder if the data is on tape rather than in the cloud. It might also be difficult, depending on the software, the length of contract or Service Level Agreement.

Establish whether the vendor has a well-documented road map and vision of where it is going with new functionality that you will need in the future or whether it is playing catch-up.

Consider a provider that not only has the technology to stream back archived data on demand, but is also working towards a solution that allows a customer to manage all data from one place - regardless of the source.

With General Data Protection Regulation coming into effect in May - organisations have an extra reason to want their archived data to be easily accessible and crucially, searchable.

The most agile service providers are those with little-to-no-reliance on third parties.

Companies that develop and own the technology that underpins their service, provide the infrastructure and support and deliver the service are typically able to act fastest on customer feedback, putting it straight into development. Without that direct link to customers, feedback will need to go through several channels, perhaps through multiple organisations and may then fall on deaf ears.

06 Establish how strong the support service is

Different providers will have varying Service Level Agreements. Check if they are punitive. It is also worth finding out if the provider makes guarantees about the availability of your archived data and whether these are strong enough to meet the business requirements.

Be aware that only some providers will have a real person on the other end of the line when you pick up a phone looking to resolve an issue.

Make sure the vendor has premier support agreements with its technology partners, or better still no reliance on any third party.

There needs to be enough qualified IT staff to handle what your organisation requires, such as protecting against data leaks and tech support.

It is also worth finding out if the vendor is using their own technology and infrastructure or another's. If data is being moved out to another third-party cloud, it is important to establish the vendor can guarantee its availability.

Check what specific services are available, who provides them, and whether these will be from the vendor's in-house staff or external consultants.

If 24 x 7 support is offered, establish whether it is live support during non-business hours, or if customers have to submit an email to receive a response the next business day via support ticket. If you have an issue or need help with anything, it is always better to deal with one company who will take complete ownership of the problem, seeing it through from start to finish.

Whether it is archiving, backup or disaster recovery, maintenance is a lot simpler if you only need to speak to one person who is ready to help immediately.

07 Check the provider's reputation and find out who else uses them

Finally, it is important to do background checks, starting with how long the vendor has been in the data management and protection business.

Establish what certifications and accreditations are held by the business such as ISO 27001 or 9001 and whether the vendor has multiple data centres for redundancy and disaster recovery and whether they are able to offer data sovereignty.

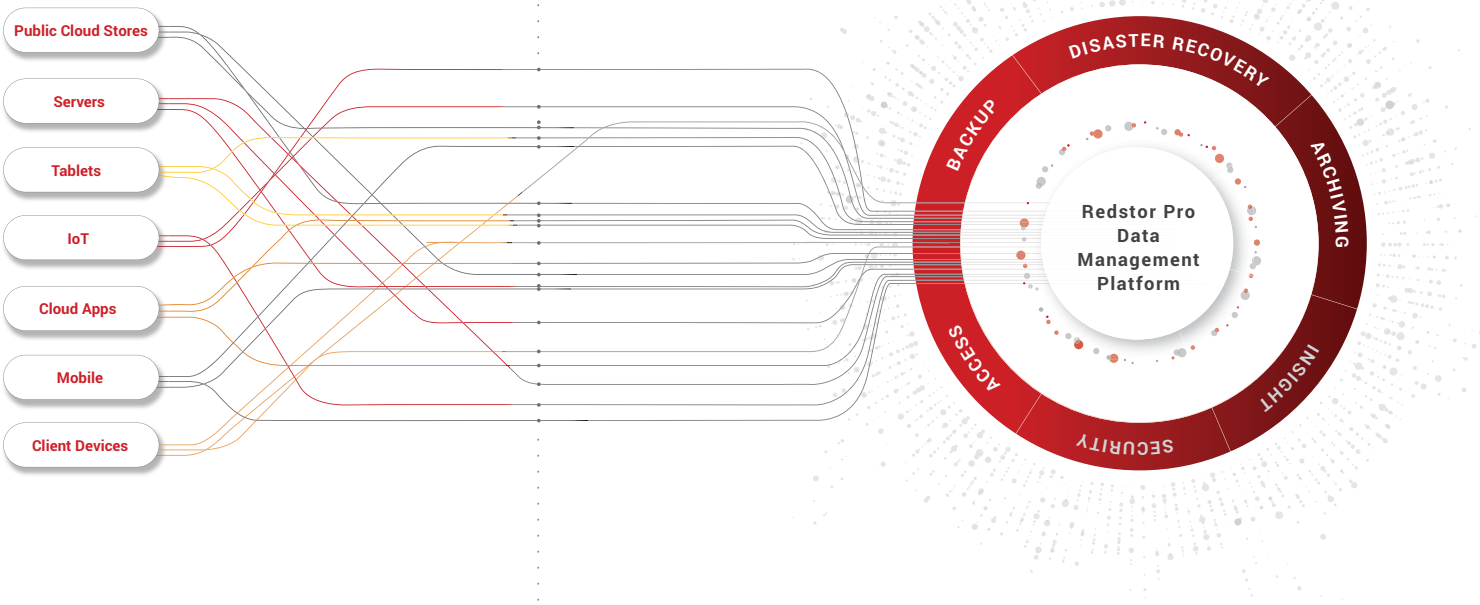
Check how physically secure the vendor's data centres are and how geographically separate they are. Consider working with a partner who will assess your requirements and provide a solution that works for your environment and business needs.

Most vendors will perform full, nightly backups of customer data, but how often do they carry out full tests to ensure data can be restored if necessary? Ask how frequently these tests are performed.

Find out how many customers the vendor has, how many of them are supported and how this has changed, particularly over the last year.

It is also worth knowing the size and type of customers that are supported – and whether those customers include organisations like yours.

If you are seeking a data management solution for the future, check out Redstor Pro. It's easy to use and install and incorporates straightforward simple pricing. Redstor Pro puts the power in the hands of the user and frees up IT managers to focus on delivering value to an organisation.



Redstor data management and protection

More than 40,000 customers around the globe put their trust in Redstor, data management experts since 1998.

Redstor Pro - a complete data management platform incorporating backup, DR and archiving - is an enterprise-level solution for the many, not just the few. Global corporations, with hundreds of TBs of data, value Redstor's secure, compliant, feature-rich service and direct accountability.

Redstor Pro is just as popular with the mid-market and small-to-medium businesses, such as top law firms and accountancies, who value working with the technology vendor and want an automated service that reduces management overheads.

The platform's ease of use, scalability and strong and secure restore capabilities also makes it hugely appealing to small businesses and the education market.

St James' Wharf | 99–105 Kings Road | Reading | Berkshire | RG1 3DD
t +44 (0)118 951 5200 | **e** sales@redstor.com | www.redstor.com
twitter.com/redstor linkedin.com/company/redstor

Checklist

Top 20 questions to ask

If you consider tape:

1. How many hours each week will it take to administer the tapes?
2. How much will it cost to transport the tapes offsite and store them?
3. How quickly can you access an archived tape if you need it back?
4. How secure is the tape, especially if it needs to go off site?
5. Can the provider offer data sovereignty at multiple data centres and are they geographically separate?
6. How many copies of data are kept and what protection methods are used?
7. Does the solution scale easily to address the challenges of data growth?
8. How easy is it to forecast future costs?
9. What investment is needed up front?
10. Is the solution seamless and automated?
11. Is there a copy of archived data held offsite for DR purposes?
12. Will tape meet GDPR compliance requirements by being both secure and searchable?
13. If archived data has a monetary value, how easy will it be to search through it?
14. How strong is the support service, what are the Service Level Agreements and is the provider dependent on a technology partner?
15. How often are full tests carried out to ensure data can be restored if necessary?
16. Does the provider have a well-documented road map and vision of where it is going or is it playing catch-up?
17. Will you be locked into using a particular hardware as that may turn out to be expensive in the long run?
18. How long has the provider been in the data management and protection business?
19. What certifications and accreditations are held by the business such as ISO 27001 or 9001?
20. How many customers does the provider have and do any include organisations like yours?

If you consider the cloud:

1. Is there a minimal bandwidth I will need?
2. Is the solution seamless and automated?
3. How many copies of data are kept and what protection methods are used?
4. What will be the impact on an end-user needing to access archived data?
5. Is there a strong integration with a backup and disaster recovery solution that delivers efficiency gains?
6. Are there one or more point solutions for each site and challenge?
7. How long will it take to retrieve archived emails, databases, files and folders?
8. Is pricing based on the volume of data stored over time?
9. Will it cost extra to retrieve files, upload files, interrogate the cloud platform?
10. Will this solution meet GDPR compliance requirements by being both secure and searchable?
11. Is there any extra functionality to simplify archiving - like the ability to determine when files were last accessed?
12. Does the provider have a well-documented road map and vision of where it is going or is it playing catch-up?
13. Is the provider acting quickly on customer feedback, releasing frequent updates and developing new functionalities that you will need in the future?
14. Does the provider have premier support agreements with its technology partners, or better still no reliance on any third party?
15. What facilities exist for moving away from the provider in the event you want to move in the future?
16. What specific services are available and who provides them, and will these be from in-house staff or external consultants?
17. Can the provider offer data sovereignty at multiple data centres and are they geographically separate?
18. How long has the provider been in the data management and protection business?
19. What certifications and accreditations are held by the business such as ISO 27001 or 9001?
20. How many customers does the provider have and do any include organisations like yours?