

Meeting of:	<b>Cabinet</b>
Date of Meeting:	<b>Monday, 26 April 2021</b>
Relevant Scrutiny Committee:	Corporate Performance and Resources
Report Title:	Backup System Replacement
Purpose of Report:	To gain Cabinet approval to undertake a procurement process for the supply of a centralised Backup Solution
Report Owner:	Executive Leader and Cabinet Member for Performance and Resources
Responsible Officer:	Rob Thomas, Managing Director
Elected Member and Officer Consultation:	Consultation has been undertaken with the Head of Digital and Innovation, Operational Manager for ICT and Senior Procurement Officer (ICT)
Policy Framework:	This report is a matter for Executive decision by Cabinet
<p>Executive Summary:</p> <ul style="list-style-type: none"> <li>This report is to gain approval to undertake a procurement process on the Crown Commercial Services framework for the replacement of the Council's ageing on-premises backup infrastructure, including the addition of a backup and recovery solution for off-premises data (Office 365).</li> <li>The Council requires a new centralised backup and recovery system that will safeguard the Councils critical on-premises and off-premises data, delivering: <ul style="list-style-type: none"> <li>Enhanced protection for the Councils critical data</li> <li>Enhanced reliability of the backup hardware and software</li> <li>Enhanced performance of backup and recovery</li> <li>Improved provision for Disaster Recovery</li> <li>Revenue cost savings over current system</li> <li>Lowered and simplified administration time</li> <li>The addition of Office 365 data backup</li> </ul> </li> </ul>	

## **Recommendations**

1. That delegated authority is granted to the Head of Finance, in consultation with the Managing Director and the Leader, to award the tender to the winning supplier.
2. That delegated authority is granted to the Head of Legal Services in consultation with the Head of Finance to execute a contract with the successful tenderer for the provision of Backup hardware and software.
3. That a new contract is awarded on the most economically advantageous terms to the Council based on 70% cost and 30% quality.

## **Reasons for Recommendations**

1. To allow the award of the contract
2. To have an appropriate contract and backup hardware and software in place to comply with the Civil Contingencies Act and ensure the Authorities data is efficiently and safely backed up and is quickly available in the event of a recovery or a disaster.
3. To have an appropriate contract in place for the cost-effective provision of a new backup system.

## **1. Background**

- 1.1 The backup refresh is a project that has been allocated Capital funding for the financial year 2021 - 2022.
- 1.2 The Council currently uses Veritas NetBackup centralised backup solution to back up, protect, and restore its on-premises data. The solution consists of two on-premises appliances and two servers, split between the Civic Offices and Alps depot. Data is replicated between the two for resilience and Disaster recovery.
- 1.3 The current backup infrastructure has been in operation since 2013 and is now becoming unreliable, not performing as needed, requiring additional capacity and constant IT intervention, and is also nearing its hardware End of Life. They need to be replaced in order to provide the required reliability, capacity and performance levels for safeguarding the Vale's critical data.

## **2. Key Issues for Consideration**

- 2.1 The backup storage appliances have been in use since 2013. They were the first iteration of these types of devices and are now very out of date. The End of Hardware Life (EOHL) for these devices is 2022, however we have been purchasing extended support for them and as each year passes, they are getting more expensive to maintain. Once they have passed their EOHL no security or software updates will be available, and this will contravene our Public Service Network PSN connection agreement.
- 2.2 Historical issues with the backup infrastructure have meant we have investigated other enterprise backup vendors who have the potential to displace Veritas

NetBackup. During this investigation some of them have provided pricing that is significantly less than the cost of replacing with Veritas products.

- 2.3 Veritas Netbackup however has recently undergone a significant re-vamp of its products and has addressed some of the problems we have experienced. They also now have what is regarded as the most comprehensive Office 365 (O365) (Software as a Service) SaaS product in the market currently.
- 2.4 The introduction of O365 throughout the Council has generated additional needs to be able to back up the off-premises data stored in Microsoft's cloud. Office 365 native resilience is based on "Geo Redundancy", this is having the same data replicated in different locations / racks / datacenters. If data were to be accidentally moved, corrupted or deleted there would be a risk of having it replicated to all locations without the ability to recover. Therefore, there is a need to have a point in time recovery solution in order to ensure the off-premises data is safeguarded.
- 2.5 The tender will seek to attract other enterprise backup vendors to respond with their solutions in order to achieve the most cost-effective, technologically future-proofed backup and recovery solution for both on-premises data, and also data that we currently hold in the Cloud (specifically O365).
- 2.6 A full explanation and breakdown of the different options that have been investigated is available in the project Business Case, attached at Appendix A. These options will be presented within the tender for suppliers to present the best solution to fit the Council's needs.

### **3. How do proposals evidence the Five Ways of Working and contribute to our Well-being Objectives?**

- 3.1 Long Term - This proposal will safeguard the backup and recovery needs for the Vale of Glamorgan Council for at least 5 years compliance with Data Protection Act, etc.
- 3.2 Prevention - This proposal will prevent the failure of the backup system and subsequent potential loss of critical data.
- 3.3 Integration - This proposal will cover the backup and recovery for all centrally stored data the Vale of Glamorgan Council currently owns, across all service areas.
- 3.4 Collaboration - This proposal will involve internal and external parties in the implementation, so all parties benefit from it.
- 3.5 Involvement - The ICT section has been canvassed to obtain their views on the functionality the system should have, the Information Governance group has been informed.

### **4. Resources and Legal Considerations**

#### **Financial**

- 4.1 It is proposed that the purchase of the hardware is funded from the Capital Allocation for 2021/2022.

## **Employment**

**4.2** There are no such implications that arise as a result of this report.

## **Legal (Including Equalities)**

**4.3** This contract will be procured using Crown Commercial Services Framework Agreement Technology Products & Associated Services (Ref.:RM6068) and therefore, the Council's Contract Procedure Rules will not apply to this award of contract because Crown Commercial Services, who are a National contracting authority, have already undertaken a compliant procurement process in line with the Public Contract Regulations 2015.

**4.4** However, the Council will need to enter into a call-off contract with the winning supplier and comply with the requirements of the Framework Agreement and the processes, terms and conditions issued under it, in order to be compliant itself with the procurement legislation.

## **5. Background Papers**

None.

# Business Case – Backup Replacement

ICT Services, MD & Resources  
The Vale of Glamorgan Council  
Civic Offices, Holton Road, Barry, CF63 4RU



## Backup System Replacement

### BUSINESS CASE

Author: Emma Williams

Date: 23/02/2021

# Business Case – Backup Replacement

ICT Services, MD & Resources  
The Vale of Glamorgan Council  
Civic Offices, Holton Road, Barry, CF63 4RU



## Revision History

Date	Summary of Changes	Changed by
22/3/2019	Initial Document	EJW
21/5/2020	Updated	EJW
23/2/2021	Updated to add O365 considerations	EJW
06/04/2021	Updated for cabinet meeting	EJW

## Contents

1.	Purpose of the document	3
2.	Objectives	3
3.	Background	3
4.	Scope	5
5.	People	5
6.	Dependencies	5
7.	Strategic Benefits	6
8.	Options	7
11.	Risks of not doing the project	12

# Business Case – Backup Replacement



ICT Services, MD & Resources  
The Vale of Glamorgan Council  
Civic Offices, Holton Road, Barry, CF63 4RU

## 1. Purpose of Document

This document will set out the reasoning for replacing the current Backup infrastructure. It will set out the objectives, benefits and potential costs involved in this project.

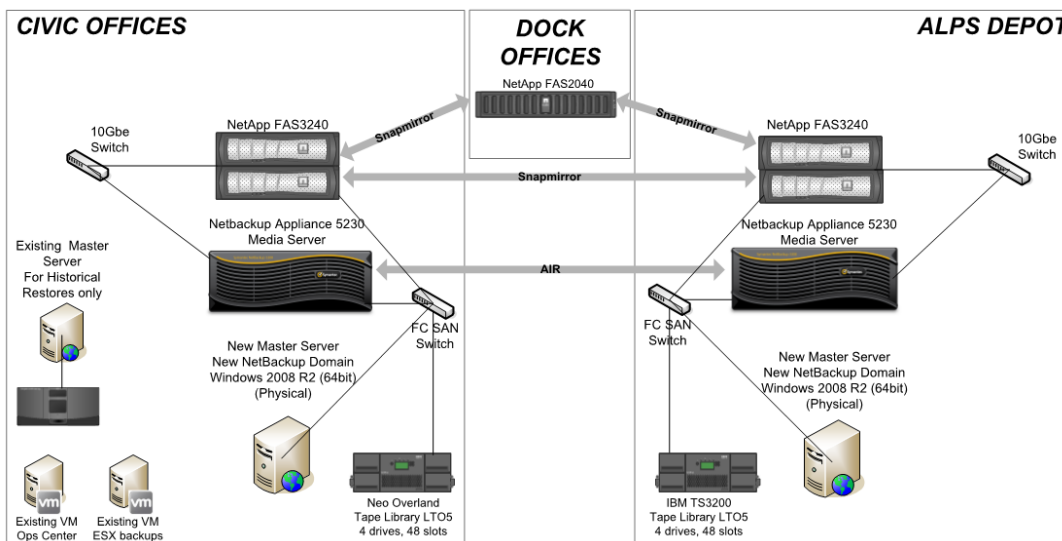
## 2. Objectives

If this business case is approved, then the project can move into the delivery phase and deliver the following benefits:

- Enhanced reliability of the backup hardware and software
- Enhanced performance of backup and recovery
- Backup window reductions
- Revenue cost savings over current system
- Lowered and simplified administration time
- The addition of Microsoft 365 data backup

## 3. Background

The current backup and recovery solution in place is Veritas NetBackup.



# Business Case – Backup Replacement



ICT Services, MD & Resources  
The Vale of Glamorgan Council  
Civic Offices, Holton Road, Barry, CF63 4RU

We back up in the region of 150 terabytes of data in daily, weekly, monthly and yearly retentions. The oldest backup we have is 2 years old. We back up to a disk based appliance, the only time the tape devices are in use is for occasional catalog backups.

We currently have two NetBackup appliances, one at the Civic offices and one in the Alps depot. Data is replicated between the two appliances. These appliances have been in use for over 5 years and are EOSL in 2022. They are becoming more expensive to maintain, and are becoming increasingly unreliable. We have recently put in place a contract with a 3<sup>rd</sup> party NetBackup support partner, and need to call them out multiple times per week to mitigate issues with the backups and the appliances.

The Council is also currently in the process of moving to Office 365 to provide its Microsoft Office based applications and improve mobility and collaboration. The current Email infrastructure is backed up onsite via Veritas NetBackup, and benefits from multiple layers of resilience in the server and storage infrastructure such as high availability and component redundancy, and can provide point-in-time recovery for up to 2 years in the past. This is now not available for any email accounts that have been moved to O365.

Office 365 native resilience is based on “Geo Redundancy”. This is having the same data replicated in different locations / racks / datacenters. So, if your data is accidentally moved, corrupted or deleted you risk having it replicated to all locations without the ability to recover. However, Microsoft’s ethos is to stop corruption or ransomware from happening, so you don’t need to recover, and they have designed in features such as monitoring and Advanced Threat Protection to mitigate this.

Microsoft guarantee “three nines” 99.9% availability in their SLA’s for O365. They state “ Get peace of mind knowing that your services are available with a guaranteed **99.9%** uptime, financially backed service level agreement (SLA)”. An availability of three nines in reality means downtime of:

- 8.76 hours per year
- 43.2 minutes per month

It is widely recognized that it is an organisations responsibility to protect and manage your Microsoft Office 365 data, not Microsoft’s.



# Business Case – Backup Replacement



ICT Services, MD & Resources  
The Vale of Glamorgan Council  
Civic Offices, Holton Road, Barry, CF63 4RU

## 4. Scope

The project will include the replacement of the backup and recovery function for all NetApp Storage, ESX VMWare, Windows, Active Directory, Solaris and Linux, Oracle, Ingres, SQL Server, Exchange and CIFS Share data in use at the Council, both on premises and in the Cloud, including Microsoft 365.

## 5. People

The following people will be involved in the project from an internal Vale of Glamorgan ICT department point of view:

Project Sponsor: Nick Wheeler  
Project Manager: Emma Williams  
Project Team Members: Sam Harrison, Russ Blight

## 6. Dependencies

Any new backup solution will need to tightly integrate with the Vale's NetApp storage, this storage is currently being migrated to new hardware/OS, and there may be a period of transition where we are backing up both old and new versions of the storage.

There will be a period of "parallel running" where the existing backup solution stays live until its backups have aged out unless there is a migration option with the new solution.

Backup retentions are a key factor in this project. Backup retention policies vary between organisations with some, for example Blue Light organisations having only 6 weeks retention, however in these cases there is normally an archive solution also in place, which we do not have. Some retentions are longer, for example the finance industry is normally 7 years retention. Our current retentions were agreed many years ago by the Information Governance Board, where they were lowered from a retention of 10 years. This is our current backup retention schedule:

Yearly	Kept for 2 years, replicated to the Alps with 2 years retention
Monthly	Kept for 12 months replicated to the Alps with 12 months retention
Weekly	Kept for 4 weeks replicated to the Alps with 4 weeks retention
Daily incremental (5 per week)	Kept for 2 weeks replicated to the Alps with 2 weeks retention

# Business Case – Backup Replacement



ICT Services, MD & Resources  
The Vale of Glamorgan Council  
Civic Offices, Holton Road, Barry, CF63 4RU

**This is as an opportune time to review the backup retentions and to ensure that they fit the business need, as well as balancing the cost of protecting the ever-growing amount of data we generate every day.** Potential changes to streamline the backup retentions are highlighted below:

## Civic Production data

Yearly	Kept for 2 years replicated to the Alps with 2 years retention
Monthly	Kept for 6 months replicated to the Alps with 6 months retention
Weekly	Kept for 4 weeks replicated to the Alps with 4 weeks retention
Daily incremental (4 per week)	Kept for 2 weeks replicated to the Alps with 2 weeks retention

## Alps Development data

Yearly	Kept for 1 years replicated to Mango 1 years retention
Monthly	Kept for 6 months replicated to Mango 6 months retention
Weekly	Kept for 4 weeks replicated to Mango 4 weeks retention
Daily incremental (4 per week)	Kept for 2 weeks replicated to Mango 2 weeks retention

The main change above is for example, if a customer doesn't realise something is missing / corrupt within 6 months, our next recovery option is the yearly backup. Whereas at the moment the retentions allow us to go back up to 12 consecutive months in monthly backups. We would potentially like to go a step further and change the Civic yearly retention to be only 1 year.

The above changes to the retention schedules would need to be ratified by the Information Governance Group.

## 7. Strategic Benefits

To reduce risk;

- To ensure the Authorities data is efficiently and safely backed up, and is quickly available in the event of a recovery or a disaster.

To reduce costs;

- Revenue cost reduction – the current licencing model used by Veritas is partially capacity based, and this will only increase over time, as will the cost of maintaining the appliances as they age and go past their EOSL date.

Compliance for Civil Contingencies Act;

- To ensure that the Authority is confident in its data protection, in the event of a disaster.

# Business Case – Backup Replacement

ICT Services, MD & Resources  
 The Vale of Glamorgan Council  
 Civic Offices, Holton Road, Barry, CF63 4RU



## 8. Options

### Option 1 – Do nothing

Pros	No resource needed to run project
Cons	Resources still tied up with resolving issues on the current system
	Hardware/software is unreliable, backups fail frequently, recovery difficult.
	Unable to move to the latest version of the software. The current appliances are not capable of upgrading to the latest version, creating a security issue. The architecture is so old that the new code for the latest software won't run properly on it

### Option 2 – Replace hardware and remain with Veritas NetBackup for On-Prem and Off-Prem Backups

Pros	In-house expertise
	Market leader for backup and recovery products with worldwide support.
	Covers all technologies we need to protect, on prem and in the cloud, in one product.
	Good relationship with current Veritas/NBU partner
	Products have had a technology “make-over”, and account managers are eager to make amends for past problems.
	Comprehensive Office 365 SaaS offering
Cons	Historical relationship problems with Vertias due to unexpected cost rises.
	Long periods of unreliability of hardware/software
	Requires significant skills to administer (additional support contract currently in place)

### Option 3 – Replace hardware by moving to a different vendor – On-Prem and Off-Prem Backup Solution from same Vendor

Pros	Potential for new technology
	Potential for new relationships with vendor
	Potential for significant solution cost savings to “unseat” Veritas
	Potential for a less admin-heavy solution so all team can administer
	Single pane of glass to administer on-prem and off-prem backups

# Business Case – Backup Replacement



ICT Services, MD & Resources  
 The Vale of Glamorgan Council  
 Civic Offices, Holton Road, Barry, CF63 4RU

Cons	Initial skilling up period needed for new software
	Will need to administer and maintain two backup solutions for 2 years
	Unknown quality for support / service
	On-prem solution may be better than off-prem solution (and vice versa)

Option 4 – Replace hardware by moving to a different vendor for on-prem backups, and move to a separate vendor for off-prem backups (or vice versa).

Pros	Potential for new technology
	Potential for new relationships with vendor
	Potential for significant solution cost savings to “unseat” Veritas
	Potential for a less admin-heavy solution so all team can administer
	Able to pick best of breed for both on-prem and off-prem solutions.
Cons	Initial skilling up period needed for new software
	Will need to administer and maintain two backup solutions for 2 years
	Unknown quality for support / service
	No single pane of glass to administer on-prem and off-prem backups

## O365 Considerations

In order to maintain the current levels of resilience and data safety that was enjoyed when the O365 data was on-premises, the Council needs to invest in additional services to ensure it meets its needs. Vendors for O365 backup solutions vary in what they offer, and the way they offer it:

- They offer subscription based services, normally for 1 year but some offer for 3 years.
- Some offer the choice between “bringing your own storage” BYOS, which means we point it towards our own Amazon S3 bucket / Microsoft Azure Blob and pay the cost for that separately. Others will provide the cloud storage within the price of the subscription, and some offer unlimited storage for this model.
- Some offer to bring your O365 data back to an appliance onsite. There may be ingress/egress costs for this and also potential for bandwidth issues on the link to the internet.

Office 365 native “backup and recovery” options we already have are:

# Business Case – Backup Replacement



ICT Services, MD & Resources  
The Vale of Glamorgan Council  
Civic Offices, Holton Road, Barry, CF63 4RU

## Email

In-place and litigation hold. These options can be set to indefinitely keep all mail in a mailbox: <https://docs.microsoft.com/en-us/exchange/security-and-compliance/in-place-and-litigation-holds>  
Without a third-party service, point-in-time restoration for your Exchange server is not available. In case of a ransomware attack, or accidental deletion, you would not be able to roll back your inbox to an earlier version.

Office 365's provides native recycle bins and version histories, however, they are not true backups. They don't allow internal IT organizations to control backup and recovery. If a hold isn't placed on a mailbox before it's deleted, the mailbox contents will not be preserved or discoverable after 30 days (plus an additional 14 days if you specifically request it from Microsoft).

Email archiving is available with an E3 licence, and use of this does not consume any tenant storage (Source: Avanade), so could potentially be used as a backup type solution for up to 100Gb per licence.

If an O365 user leaves the organisation and the licence re-used elsewhere, their mailbox ages out after 30 days, unless it is converted to a shared mailbox, which does not require a licence unless it is larger than 50Gb.

## Sharepoint

Microsoft provide 14 days metadata backup: <https://docs.microsoft.com/en-us/sharepoint/safeguarding-your-data> "Metadata backups are kept for 14 days and can be restored to any point in time within a 5-minute window"

There is also a recycle bin for deleted items that retains items for 93 days, and a 2<sup>nd</sup> stage recycle bin giving a total of 186 days, unless the recycle bin exceeds its quota and starts to purge older items. <https://support.office.com/en-us/article/restore-deleted-items-from-the-site-collection-recycle-bin-5fa924ee-16d7-487b-9a0a-021b9062d14b?ui=en-US&rs=en-US&ad=US>

This doesn't appear to cover corrupted or damaged files, just consciously deleted ones. Ransomware is still a problem if you are syncing from on-premises, Microsoft see no problem as the file is still there, but encrypted. Any end user or administrator can remove from recycle bin, and mistakes can be made. It remains our responsibility to protect the data.

# Business Case – Backup Replacement



ICT Services, MD & Resources  
The Vale of Glamorgan Council  
Civic Offices, Holton Road, Barry, CF63 4RU

## OneDrive

Onedrive has similar recovery options to Sharepoint, and consideration should be given to syncing the Vale H: drives with OneDrive, as this could then be backed up by the on-premises backup infrastructure.

## Groups

AD Groups are replicated from the onsite Active Directory and will be backed up by the on-prem backup solution, however, Groups created in O365 are not replicated.

## Teams

Teams stores chat data, conversation history and calendar data in Exchange. It stores chat files in OneDrive and Channel files and Wikis in Sharepoint. So, the only way to back up all Teams data is to back up Exchange, Sharepoint and OneDrive (Source: TechTarget)

Application	Data safety options for active account	Retention after account marked for deletion
Email (Inc. Calendar, Contacts, Tasks, Shared mailbox, Public folders, In-place archive)	Litigation hold (2 years if required) Archiving (forever)	30 days Or convert to shared mailbox (forever)
Sharepoint	Metadata: 14 days User Data: 1 <sup>st</sup> and 2 <sup>nd</sup> stage recycle bin (186 Days)	
OneDrive	1 <sup>st</sup> and 2 <sup>nd</sup> stage recycle bin (186 Days)	365 days
Groups	AD groups are synced so can use on-prem retentions, but O365 specific groups can not.	n/a
Teams	Retention policies	

# Business Case – Backup Replacement



ICT Services, MD & Resources  
The Vale of Glamorgan Council  
Civic Offices, Holton Road, Barry, CF63 4RU

Further reasons for additional protection for O365:

- Microsoft Office 365 guarantees the availability of your data, but not the protection of it.
- The responsibility for protecting the data lies with the organisation. Every SaaS provider explicitly says that clients are responsible for protecting their own data.
- SaaS providers can offer DR against data center outages, but do not guarantee against accidental deletion, virus or malware, hackers, or ransomware attacks.
- Security and compliance reasons, ideally, the data should be compliant, encrypted and backed up at a secondary location to the SaaS provider's data center for audit purposes.
- The number one cause of data loss in a SaaS deployment, such as Microsoft Office 365, is accidental data deletion. A large percentage of all lost data is due to either accidental or malicious deletion of data by end-users. Other ways that data can be lost include misconfiguration, client sync issues, and most recently the widespread presence of malware and ransomware, which can render data unusable.
- Although Microsoft Office 365 provides some basic recovery options with the recycle bin and email retention, Microsoft's primary focus within Office 365 is ensuring that service and data availability are not disrupted. It is the organisations responsibility to protect the data that they store in the Office 365 cloud.
- Data loss is very common, in the Vale we get requests to restore data for different reasons multiple times a week. Even small data loss incidents can impact day-to-day business.

# Business Case – Backup Replacement

ICT Services, MD & Resources  
The Vale of Glamorgan Council  
Civic Offices, Holton Road, Barry, CF63 4RU



## 9. Risks of not doing the project

The risks of not implementing this project are:

- We will not realise the benefits set out in points 2 and 7.
- The cost of maintaining the NetBackup infrastructure will continue to go up over time as the appliances will need extended support.
- The ability to backup and recover the Authorities data becomes more and more unreliable, potentially leading to a data loss situation.
- The current appliances are at capacity, and the DR (replication) element is being eroded by space needed for normal backups.
- We will be using backup and recovery software that cannot be upgraded, creating a PSN compliance issue.
- Off-Premises (Cloud) data will not be protected for point in time restores, or against accidental deletion or malware.