Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	[redacted]
THE BUYER:	The Secretary of State for the Home Department
BUYER ADDRESS	2 Marsham Street, London, SW1P 4DF
THE SUPPLIER:	Softcat Plc
SUPPLIER ADDRESS:	Thames Industrial estate, Fieldhouse Lane, Marlow, Bucks, SL7 1LW
REGISTRATION NUMBER:	[redacted]
DUNS NUMBER:	[redacted]
SID4GOV ID:	[redacted]

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated **8th December 2023**.

It's issued under the Framework Contract with the reference number RM6068 for the provision of Technology Products and Associated Services.

CALL-OFF LOT(S):

- Lot 1 Hardware & Software & Associated Services

CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1 This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.

2 Joint Schedule 1(Definitions and Interpretation) RM6068

3 The following Schedules in equal order of precedence:

- Joint Schedules for RM6068
  - Joint Schedule 2 (Variation Form)
  - Joint Schedule 3 (Insurance Requirements)

    - Joint Schedule 6 (Key Subcontractors)
    - Joint Schedule 10 (Rectification Plan)
- Call-Off Schedules for C23462
    - Call-Off Schedule 1 (Transparency Reports)
    - Call-Off Schedule 5 (Pricing Details)
    - Call-Off Schedule 9 (Security) Part C
    - Call-Off Schedule 10 (Exit Management) Part B
    - Call-Off Schedule 18 (Background Checks)
    - Call-Off Schedule 20 (Call-Off Specification)

4 CCS Core Terms (version 3.0.6)

5 Joint Schedule 5 (Corporate Social Responsibility) RM6068

6 Annexes A to E Call-Off Schedule 6 (ICT Services)

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS

The following Special Terms are incorporated into this Call-Off Contract:

[redacted]

Call-Off Start Date:	08/12/2023
Call-Off Expiry Date:	07/12/2026
Call-Off Initial Period:	36 months
Call-Off Optional Extension Period:	2 periods of up to 12 months

CALL-OFF DELIVERABLES

See details in Call-Off Schedule 20 (Call-Off Specification)

LOCATION FOR DELIVERY

HODC01, [redacted]

HODC02, [redacted]

DATES FOR DELIVERY OF THE DELIVERABLES

Milestone Number	Phase	Project Milestone	Milestone Date (DD-MM-YYYY)
1	Design	Design Milestone Design-M2 – Discovery and Architecture	29/02/2024
2	Delivery	Implementation Milestone Imp-M1: Procurement and Delivery	21/03/2024
3	Delivery	Implementation Milestone Imp-M2: Install and Configure	21/04/2024
4	Delivery	Testing Milestone ImpTest-M1: Design Baseline Conformance	04/05/2024
5	Delivery	Testing Milestone ImpTest-M2: Template Creation and Deployment	04/05/2024
6	Acceptance	Acceptance Milestone ImpAcc-M1: Acceptance of Live Service	31/05/2024

TESTING OF DELIVERABLES

N/A

WARRANTY PERIOD

The warranty period for the purposes of Clause 3.1.2 of the Core Terms shall be the duration of the full Contract Period including it's Extension Periods.

MAXIMUM LIABILITY

The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.

The Estimated Year 1 Charges used to calculate liability in the first Contract Year is [redacted]

CALL-OFF CHARGES

See details in Call-Off Schedule 5 (Pricing Details)

This Call-Off Contract has no minimum spend or volume commitments. The Total contract value (TCV) [redacted] for both the 3 year initial term and for the provision of the option 1+1 extension.

The total published TCV is [redacted]

The Charges will not be impacted by any change to the Framework Prices. The Charges can only be changed by agreement in writing between the Buyer and the Supplier because of a Specific Change in Law or Benchmarking using Call-Off Schedule 16 (Benchmarking) where this is used.

REIMBURSABLE EXPENSES

N/A

PAYMENT METHOD

The payment method for this Call-Off Contract is BACS.

BUYER'S INVOICE ADDRESS:

Invoices will be sent via email as the primary method for delivery to the address below:

hosupplierinvoices@homeoffice.gov.uk

Invoices can be submitted in hard copy via post to the address below, however this will significantly delay the processing of the payment to the supplier.

Home Office Shared Service Centre HO Box 5015 Newport, Gwent NP20 9BB United Kingdom

Tel: 08450 100125 Fax: 01633 581514

BUYER'S AUTHORISED REPRESENTATIVE

[redacted]

BUYER'S ENVIRONMENTAL POLICY

The Supplier shall, when working on the Sites, perform its obligations under this Call Off Contract in accordance with the Environmental Policy of the Customer.
The Customer shall provide a copy of its written Environmental Policy (if any) to the Supplier upon the Supplier's written request.

"Environmental Information Regulations or EIRs"	a) means to conserve energy, water, wood, paper and other resources, reduce waste and phase out the use of ozone depleting substances and minimise the release of greenhouse gases, volatile organic compounds and other substances damaging to health and the environment, including any written environmental policy of the Customer;
"Environmental Policy"	a) means the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issued by the Information Commissioner or relevant government department in relation to such regulations;

BUYER'S SECURITY POLICY

The Supplier warrants that it has obtained ISO 14000/14001 certification for its environmental management and shall comply with and maintain such certification requirements.

The Supplier shall comply with relevant obligations under the Waste Electrical and Electronic Equipment Regulations 2006 in compliance with Directive 2002/96/EC and subsequent replacements.

The Supplier shall (when designing, procuring, implementing and delivering the Services) comply with Article 6 and Annex III of the Energy Efficiency Directive 2012/27/EU and subsequent replacements.

The Supplier shall comply with the EU Code of Conduct on Data Centres' Energy Efficiency and any subsequent replacements. The Supplier shall ensure that any data centre used in delivering the Services are registered as a Participant under such Code of Conduct.

The Supplier shall comply with the Authority and HM Government's objectives to reduce waste and meet the aims of the Greening Government: IT Strategy contained in the document "Greening Government: ICT Strategy issue (March 2011)" at https://www.gov.uk/government/publications/greening-government-ict-strategy.

SUPPLIER'S AUTHORISED REPRESENTATIVE

[redacted]

SUPPLIER'S CONTRACT MANAGER

[redacted]

PROGRESS REPORT FREQUENCY

Detailed within Appendix B – Statement of Requirements

PROGRESS MEETING FREQUENCY

Detailed within Appendix B – Statement of Requirements

KEY STAFF

N/A

KEY SUBCONTRACTOR(S)

Rubrik, Inc.

COMMERCIALLY SENSITIVE INFORMATION

1.1. In this Schedule the Parties have sought to identify the Supplier's Confidential Information that is genuinely commercially sensitive and the disclosure of which would be the subject of an exemption under the FOIA and the EIRs.

1.2. Where possible, the Parties have sought to identify when any relevant Information will cease to fall into the category of Information to which this Schedule applies in the table below and in the Order Form (which shall be deemed incorporated into the table below).

1.3. Without prejudice to the Relevant Authority's obligation to disclose Information in accordance with FOIA or Clause 16 (When you can share information), the Relevant Authority will, in its sole discretion, acting reasonably, seek to apply the relevant exemption set out in the FOIA to the following Information:

Item(s)	Duration of Confidentiality
Any detail around pricing or commercial models	In perpetuity
Any detail around Softcat facilities, personnel or resources	In perpetuity
Any detail around business processes	In perpetuity
Any detail around business IT systems employed	In perpetuity

SERVICE CREDITS

N/A

ADDITIONAL INSURANCES

N/A

GUARANTEE

N/A

SOCIAL VALUE COMMITMENT

Not applicable.

For and on behalf of the Supplier:	For and on behalf of Buyer:
Signature: [redacted]	Signature: [redacted]
Name: [redacted]	[redacted]
[redacted]	[redacted]
Date: 08/12/2023	Date: 08/12/2023

Call-Off Schedule 5 (Pricing Details)

Appendix D - Pricing Model

C21699 Replacement Backup

RM6100: Technology Services 3: Further Competition

Background

The baseline requirements are the current workloads today.
There are a number of future events which have been illustrated by the Authority as examples of future growth.
The Potential Provider should enter pricing details for all pricing scenarios.
Each scenario is a realistic potential outcome given the information available to the Authority at this time.
The Authority expects the pricing provided to be consistent against each scenario provided.
The Authority will decide as part of contract award the level of resources required for the Replacement Backup Platform using the provided pricing. The values shown in the Baseline Requirements (rows 21-23) of the Solution Details tab represent the requirements as of April 2023. the Authority will, at a minimum, contract for the level of resources shown in these orange cells in Section 1 – Baseline Requirements of the Solution Details tab. the Authority may add Scale Options as required to provide the initial Replacement Backup Platform if the requirements have increased from those shown in Section 1 – Baseline Requirements of the Solution Details tab by the time of contract award.
The Authority will decide as part of contract award whether Pay as You Go or Volume Commitment pricing will apply.
The Authority may use the prices submitted in all scenarios as part of contract award.
The pricing scenarios show 60 Service Periods. Service Periods commence from the Achievement of Acceptance Milestone ImpAcc-M1: Acceptance of Live Service. The actual number of Service Periods will depend on the date of Achievement of Acceptance Milestone ImpAcc-M1: Acceptance of Live Service.

General Instructions

Please fill in only the yellow fields provided throughout each of the following tabs in this template workbook (Solution Details, Pricing – MVP Scenario, Pricing – Growth Scenario).
All amounts should be in GBP (£) excluding VAT and be fully inclusive of all costs, charges, expenses and disbursements necessary for the Supplier to comply with its obligations as set out in the Contract (including the Services and the Call Off Terms), including, but not limited to, travel and subsistence, training costs, security clearance/vetting costs, all risks, all costs associated with the compliance of the Employment Regulations and Call Off Schedule S4 (Staff Transfer), the provision of materials, stationery, postage, equipment, insurance, wages, salary and recruitment charges, labour costs, including (amongst other things) wages, payroll burden, all taxes, dues and allowances, telephone, telex and facsimile costs, photocopying, reprographic, word processor, internet access, and computer charges, material costs (net of trade discounts), all direct, indirect and other overheads, profits and the like necessary for the complete and proper fulfilment of all the Services, obligations and liabilities of the Supplier under the Contract as specified or implied therein. The reference to "all risks" within this paragraph includes any risks, as may be determined by the Potential Provider, associated with any information which the Authority may be unable to provide within the Further Competition Invitation documentation (including within its clarification responses) and/or associated with any information provided by the Authority which is discovered to be inaccurate.
White cells are automatically calculated by the values entered into the yellow cells and therefore should not be edited.
Orange cells are populated with data pre-provided and should also not be edited.

Section 1 Solution Details Tab	Section 1 ('Baseline Requirements ') details the software and hardware requirements for the Authority Workloads at the present time. It is to be completed with the Supplier suggestion of how these Workloads should be protected. Section 1 ('Baseline Requirements') should be completed first Section 1 ('Baseline Requirements') should be populated with the following: - The proposed capacity requirements for ???? - These proposed values for capacity should be used for the purposes of section 3. Replacement Backup Pricing.
Section 2 Solution Details Tab	Section 2 ('Replacement Backup Supply') is to be completed with the proposed solution components. Section 2 ('Replacement Backup Supply') should be populated with the following: The proposed software and hardware components The surplus capacity provided beyond the requirements
Section 3 Solution Details Tab	Section 3 – ('Solution Delivery Payment Milestones') is to be completed with the proposed additional costs for the completion of the milestones - All required cost details for the payment milestones
Section 4 Solution Details Tab	Section 4 ('Replacement Backup Solution Component') is to be completed with the details of each supplied component for expansion options shown. Section 4 ('Replacement Backup Solution Component') should be populated with the following: - The capacity and required prices and discounts of each component specified as required
Section 5 Pricing – Growth Scenario	Section 5 ('Replacement Backup Pricing – Growth Scenario') is to be completed with the details of the prices for the first pricing scenario Section 5 ('Replacement Backup Pricing – Growth Scenario') should be populated with the following: - The monthly prices for the Pay As You Go and Volume Term for the initial baseline requirement (Service Period 1) - The Hardware Resources proposed by the Potential Provider to maintain the hardware requirements in line with the stated requirements. - Based on the hardware requirements the Potential Provider should provide the charges for each Service Period in the first 3 years - The Potential Provider should only increase the hardware resouces using the components proposed in the Solution Details
Section 6 Evaluation Sheet Tab	Section 6 ('Total Contract Charges') collates the required information for the scoring of the pricing model. Section 6 ('Total Contract Charges') is automatically populated based on the values provided in the other sections covering the full duration of the contract. The summary numbers in this section will be used together to form a basis for evaluation (including any extension period).

Note: Any information provided by the Potential Provider outside of the yellow fields will be disregarded
Note: The prices proposed within the Pricing Model shall represent the Contract Charges and shall remain firm for the entire Contract Period.

Potential Provider Business Name | Softcat plc.

Section 1 - Baseline Requirements

Please complete ALL YELLOW CELLS

Backup workload totals to serve as a baseline requirement for capacity.

Backup Workload Totals - Existing Locations

Primary Backup (HODC)	
Volume of Storage (TB) on NetApp FAS storage	456
Number of protected virtual machines	363
Storage (TB) consumed by protected virtual machines	1469.4

Section 2 - Replacement Backup Supply

The Potential Provider shall complete the Total Hardware Capacity table below by entering Hardware Component Volume values. The Platform Required for Workloads is determined from the Baseline Requirements identified in section 1.
The Potential Provider shall complete the Hardware Component Table detailing all of the components (both hardware and software) required for the provision of the Replacement Backup Product
The Potential Provider shall ensure that every component required for the Replacement Backup Solution is included in the detail provided in rows 50-60
The Potential Provider shall provide monthly prices on the "MVP Scenario" tab to provide for the "Backup Workload Totals" in rows 21 and 22.
The Potential Provider shall provide prices for the Authority to acquire the Replacement Backup Platform Hardware at the intervals detailed.

The Potential Provider shall assume that two copies of each backup are required - the secondary backup copy is to be held in a different physical location and cannot rely on any hardware component used for the primary backup

Monthly pricing will take effect from the first Service Period. As per Appendix B Specification and Requirements, section 4.3.4 the first Service Period commences upon the Achievement of Acceptance Milestone ImpAcc-M1.

The Potential Provider shall ensure that the pricing for the baseline requirements takes account of the exit related costs as per Appendix B Specification and Requirements - section 2.7.

The Authority may during the term of the Contract wish to reduce the SLA required through Contract Change Control.

Total Hardware Capacity to meet Baseline Requirements

Primary Backup Location

Platform Required for MVP		
Replacement Backup Solution Component	**Component Volume**	**Surplus Included**
RS-FT-NCD-PE-PA - Rubrik NAS Cloud Direct; per FETB; Premium support; pay annual - Term: 36 Months	[redacted]	
Rubrik Foundation Edition; per usable BETB; Premium support; pay annual - Term: 36 Months		
Support for R6000S Tier 3 hardware, prepay; Premium support - Term: 36 Months		
r6420 Appliance, 4-node, 240TB raw HDD, 1.6TB SSD, SFP+ NIC		
Fiber Optic OM3 LC/LC Cable, 3M, pack of 4		
10G/1G Dual Rate SFP+ Transceiver, pack of 4		
Services		

Secondary Backup Location

Platform Required for MVP		
Replacement Backup Solution Component	**Component Volume**	**Surplus Included**
Rubrik Foundation Edition; per usable BETB; Premium support; pay annual - Term: 36 Months	[redacted]	
Support for R6000S Tier 3 hardware, prepay; Premium support - Term: 36 Months		
r6420 Appliance, 4-node, 240TB raw HDD, 1.6TB SSD, SFP+ NIC		
Fiber Optic OM3 LC/LC Cable, 3M, pack of 4		
10G/1G Dual Rate SFP+ Transceiver, pack of 4		

Pay as You Go pricing - No assumption should be that any volume or term commitment will be made

Backup Component Pricing

Platform Required for Baseline Requirements	
Monthly Price in Years 1 - 3	[redacted]
Monthly Price in Year 4	
Monthly Price in Year 5	
Price to Acquire Hardware at 36 months	
Price to Acquire Hardware at 48 months	
Price to Acquire Hardware at 60 months	

Total Pay as You Go Price for initial 3 years

Volume Term Commitment - the Authority will contract for the Total Hardware Requirements for the terms listed below

the Authority will commit to maintain the baseline requirements for the initial contract term of 3 years.
the Authority will subsequently commit for 1 year if they should choose to exercise either of the contract extension options.

Backup Component Pricing

Platform Required for Baseline Requirements	
Monthly Price in Years 1 - 3	[redacted]
Monthly Price in Year 4	
Monthly Price in Year 5	
Price to Acquire Hardware at 36 months	
Price to Acquire Hardware at 48 months	
Price to Acquire Hardware at 60 months	
Total Volume Commitment Pr	

Section 3 - Solution Delivery Payment Milestones

The Potential Provider shall detail dates and costs for each milestone identified in Appendix B, Specifications and Requirements, Section 4.4. The Potential Provider shall not duplicate these costs in their monthly costs.
The Potential Provider should accurately determine milestone costs. the Authority requests that the Potential Provider supply the internal calculations used to determine the cost of each milestone.
In the event the costs incurred by the Supplier relating to a Milestone ("Incurred Costs") are lower than the corresponding Milestone Costs identified in the Pricing Model, the difference between the Incurred Costs and the Milestone Costs shall be shared equally between the Parties, by means of a credit (shown as a separate line) within the corresponding Supplier invoice, or by means of a separate credit note received by the Authority no later than thirty (30) days of the corresponding invoice. The Supplier's invoices for all Milestones shall detail the Incurred Costs, whether or not the Incurred Costs are lower than

Milestone Number	Phase	Project Milestone	Milestone Date (DD-MM-YYYY)	Pricing Mechanism	Milestone Percentage of milestone overall	Milestone Cost (Direct Costs Only)	Bidder Profit Markup	General Overheads Markup	Milestone Payment
1	Design	Design Milestone Design-M2 –	[redacted]	Milestone Payment	0.00%	[redacted]			
2	Delivery	Implementation Milestone Imp-M1:		Milestone Payment	0.00%				
3	Delivery	Implementation Milestone Imp-M2:		Milestone Payment	0.00%				
4	Delivery	Testing Milestone ImpTest-M1:		Milestone Payment	0.00%				
5	Delivery	Testing Milestone ImpTest-M2:		Milestone Payment	0.00%				
6	Acceptance	Acceptance Milestone ImpAcc-		Milestone Payment	0.00%				
			Sub Total		0.00%				

Instructions | Solution Details | Pricing - Growth Scenario | Evaluation Sheet

Section 5 - Replacement Backup Pricing - Growth Scenario

Description

In this pricing scenario the Baseline Requirements grow over 5 years.
The increased requirements are served by components entered by the Potential Provider in the "Solution Details" tab.
the Authority acquires all hardware components at the end of the 5 year term

Replacement Backup Requirements Over Term

The values for Service Period 1 requirements are determined from the baseline requirements distribution data entered in Section on the Solutions Details tab
The Potential Provider shall assume that two copies in phsyically distinct locations are required for each component
The Potential Provider shall highlight where the backup will not be provided via direct integration with the source service

Requirement	Timing of addition	Storage (TB)		Protected Resource Type	Number of Protected Resources	Protected by direct integration
Initial Requirements	Month 1	456		NetApp FAS	1	[redacted]
		991		Virtual Machines - VMWare	243	
		478		Virtual Machines - AzureStack Hub	120	
Oracle Databases	Month 2	24		Oracle databases in a single node RAC Cluste	4	
Azure Virtual Machines	Month 3	40		Azure Virtual Machine	135	
AWS RDS Database	Month 5	90		AWS RDS Databases	14	
Azure Managed SQL	Month 8	15		Azure Managed SQL Databases	24	
Azure Active Directory	Month 9	2		Azure Active Directory	1	
Microsoft Office 365 Email	Month 10	2500		Office 365 Mailboxes	50000	
Microsoft Office 365 Sharepoint	Month 12	800		Office Sharepoint 365 Site Content	4500	
SMB Data Backup	Month 13	21		SMB share containing Data Backups	6	
Exchange 2019 Databases	Month 18	11		Exchange 2019 Mailbox data	14	
AWS S3 Storage Buckets	Month 22	140		Multiple S3 Storage Buckets	1030	
AWS EC2 Instances	Month 26	45		AWS EC2 instances using EBS Volumes	260	
AWS EKS Cluster	Month 30	5		AWS EKS Cluster	88	

Instructions | Solution Details | Pricing - Growth Scenario | Evaluation Sheet

Pricing Schedule

The Potential Provider shall detail the Service Period Charges in the tables below ensuring that the Service Period Charges accurately reflect any components added or removed from the Replacement Backup Platform.

The Potential Provider shall ensure that the Service Period Pricing is made up from solely the "Monthly Prices" entered in this pricing scenario tab for Pay as You Go and Volume Term Commitment and the monthly Prices for any components entered on the Solutions Details tab which are required to provide the required hardware resources

The Potential Provider shall ensure that prices remain firm during the initial term and both extension options of the contract.

Pay As You Go Pricing

Service Period		Service Period Charges
Initial Requirement	1	[redacted]
Oracle	2	
Azure VM	3	
	4	
AWS RDS	5	
	6	
	7	
Azure SQL	8	
Azure AD	9	
M365 Email	10	
	11	
M365 Sharepoint	12	
SMB Data	13	
	14	
	15	
	16	
	17	
Exchange DB	18	
	19	
	20	
	21	
AWS S3	22	
	23	
	24	
	25	
AWS EC2	26	
	27	
	28	
	29	

Volume Term Commitment Pricing

Service Period		Service Period Charges
Initial Requirement	1	[redacted]
Oracle	2	
Azure VM	3	
	4	
AWS RDS	5	
	6	
	7	
Azure SQL	8	
Azure AD	9	
M365 Email	10	
	11	
M365 Sharepoint	12	
SMB Data	13	
	14	
	15	
	16	
	17	
Exchange DB	18	
	19	
	20	
	21	
AWS S3	22	
	23	
	24	
	25	
AWS EC2	26	
	27	
	28	
	29	

Volume Term Commitment has been assumed to be a purchase with licensing terms upto 3 years, with extentions at years 4 and 5 if desired. The purchases within the first 3 years are therefore cotermed to the 36th month.

Instructions | Solution Details | Pricing - Growth Scenario | Evaluation Sheet

Pay As You Go Pricing

Service Period		Service Period Charges
AWS EKS	30	[redacted]
	31	
	32	
	33	
	34	
	35	
	36	
Extension Period 1	37	
	38	
	39	
	40	
	41	
	42	
	43	
	44	
	45	
	46	
	47	
	48	
Extension Period 2	49	
	50	
	51	
	52	
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	
H/W Acquisition		

Total Pay as You Go Price for 5 Years

[redacted]

Volume Term Commitment Pricing

Service Period		Service Period Charges
AWS EKS	30	[redacted]
	31	
	32	
	33	
	34	
	35	
	36	
Extension Period 1	37	
	38	
	39	
	40	
	41	
	42	
	43	
	44	
	45	
	46	
	47	
	48	
Extension Period 2	49	
	50	
	51	
	52	
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	
H/W Acquisition		

Total Volume Term Commitment Price for 5 Years

[redacted]

Section 6 - Total Contract Charges

Green cells = instructions
Yellow cells = Supplier to complete
Blue cells = for evaluation

The scored prices and values from each section are summarised below.

		Submissions	Weightings	Scores
Pricing - Baseline Requirements	Milestone Payments	[redacted]		
	Total Pay As you Go Price for 3 years - MVP Scenario			for internal use
	Total Volume Commitment Price for 3 years - MVP Scenario			for internal use
Pricing - Growth Scenario	Milestone Payments			
	Total Pay As you Go Price for 3 years - Growth Scenario			for internal use
	Total Volume Commitment Price for 3 years - Growth Scenario			for internal use
TOTAL SCORE				for internal use

Call-Off Schedule 20 (Call-Off Specification)

This Schedule sets out the characteristics of the Deliverables that the Supplier will be required to make to the Buyers under this Call-Off Contract

Appendix B – Statement of Requirements

Further Competition for C23462 Backup Replacement

Appendix B:

Specification and Requirements

for Call Off Contract under Framework RM6068 Technology Products & Associated Services - Lot 1: Hardware & Software & Associated Services

Version History

[redacted]

Authorisation

[redacted]

Table of Contents

1. Introduction 21
1.1. This document 21
1.2. Background to the Authority 21
1.3. Background to the Requirements 23
2. High Level Requirements and Scope 24
2.1. Objectives 24
2.2. Supplier Characteristics 28
2.3. High Level Technical Scope 29
2.4. High Level Call Off Contract Components 32
2.5. High Level Contract Scope 34
2.6. Overarching Requirements 35
2.7. Contract Exit 35
3. Design Detailed Requirements 36
3.1. Overview of Design Requirements 36
3.2. Design 36
3.3. Design Milestones table 38
4. Implementation, Testing and Acceptance 41
4.1. Implementation 41
4.2. Testing 43
4.3. Acceptance 44
5. Maintenance, Expansion and Upgrade 45
5.1. Maintenance 45
5.2. Expansion 47
5.3. Monitoring and Reporting requirements 48
5.4. Authority policies and procedures 50
5.5. Testing requirements 50
5.6. Training requirements 50
Annexes 51
6. Annex 1 Sizing 51
6.1. Current Volumetrics 51
6.2. Required Initial Sizing 52
7. Annex 2 – Defined terms 53
8. Authority Policies 65
8.1. Government policies 65
8.2. Authority Policies - Cyber security 65

Figures and Tables

No table of figures entries found.

Table 1 - Contract Scope 34
Table 2 - Design Milestones 40
Table 7 – Defined Terms 64
Table 8 - Data Centre Management ..... **Error! Bookmark not defined.**

1. Introduction

1.1. This document

1.1.1. This Specification and Requirements document relates to the Further Competition to award a Call Off Contract for a Backup Replacement Solution to a sole Supplier.

1.1.2. This Further Competition is being conducted under the CCS Framework RM6068 Technology Products & Associated Services - Lot 1: Hardware & Software & Associated Services.

1.1.3. This Specification and Requirements document (ITT Appendix B) contains detail of the hardware, software and services the Supplier will be required to supply to the Authority in accordance with the Contract.

1.2. Background to the Authority

1.2.1. The Home Office is one of the original great Departments of State and has one of the most challenging jobs in government. Its mission is fundamentally important: to keep Britain safe and secure.

1.2.2. The Home Office mission is to deliver a safe, fair and prosperous UK via 4 priorities:

- Restore confidence in the criminal justice system
- Attract talent and take back control
- Protect homeland security
- Advance Britain’s place in the world

1.2.3. The Home Office leads on immigration and passports, drugs policy, crime policy, counter-extremism and counterterrorism and works to ensure visible, responsive and accountable policing in the UK.

1.2.4. The Digital, Data and Technology (DDaT) function within the Home Office is at an exciting point of evolution. Since 2010, the delivery of technology services within the UK government has been radically transformed, with major changes implemented to enable departments to take back increased control of the design, build and/or operation of their key technology services.

1.2.5. DDaT is made up of 1800 Civil Service staff, augmented by a further 2700 contractors and many supplier partners. Every year, our systems support over 3 million visa applications, checks on 100 million border crossings, 5 million passport applications and 140 million police checks on people, vehicles and property. Many of these services support critical national functions and contain sensitive public information.

1.2.6. Within DDaT, the Enterprise Services (ES) teams are responsible for delivering common infrastructure services (not applications) that are consumed by multiple Home Office business Portfolios; for example, HM Passport Office ("HMPO") and Borders. The ES team are supporting and enhancing services in a complex and demanding operational multi-supplier environment whilst at the same time delivering service transformation.

1.2.7. In 2016, the Home Office began using the Crown Hosting Framework Agreement for its strategic Data Centre capability (HODC1 and HODC2) and in 2018, ES awarded the running of the infrastructure located in these Data Centres to a supplier. ES continued refining and maturing the infrastructure and services offered out of these Data Centres over time including separating Secret and Official Security domains and invested in key service improvement activities targeted at improving service quality, service commonality and overall service availability.

1.2.8. In HODC1 and HODC2, programs of work are refreshing infrastructure foundational services to remove technical debt. This will pave the way for a wider infrastructure transformation program to coincide with natural refresh junctions.

1.3. Background to the Requirements

1.3.1. The Authority has existing commercial arrangements with a supplier to provide backup software and infrastructure for data of OFFICIAL classification. This Contract is to recompete and extend these capabilities as existing commercial arrangements comes to an end.

1.3.2. The Authority's strategic direction is to continue the digital transformation of services, adopt innovative technologies, provide secure hosting services based on a consumption model, and support for on premise infrastructure (on-premise and private cloud) in our strategic Data Centres in addition to the continuing use and development of our Cloud estate.

1.3.3. The Authority's key strategic principles are:

- Technology convergence
- Shared technology products
- Becoming product centric
- Becoming data driven
- Effective delivery
- Effective innovation

1.3.4. A new single Contract for a Backup Infrastructure and Software Supplier is required with a sole supplier to provide procurement, licence management, expansion and upgrade capabilities over the next 3 to 5 years. This document provides the specification and requirements for the new Contract, which is divided into 3 components:

- Design of Replacement Backup Solution for implementation by the Authority incorporating a broad range of Authority and Authority third party stakeholders
- Supply of materials to support Authority Implementation, Testing and Acceptance
- Ongoing Product Support, facilitate Expansion and supply of materials for Authority maintenance

- Once Accepted into Service by the Authority, the resulting Backup service will be operated by the Authority and its third parties. There is no requirement for any level of service beyond the maintenance of the supplied materials. The Supplier shall be responsible for the maintenance of service levels for those supplied materials and the Authority expects these service levels to be aligned to those for the Authority service.

1.3.5. **For the design component of the Contract, the Supplier shall align to key themes of the Authority's Target Operating Model, these are**

- Improved productivity
- Reduced TCO
- Secure by design

2. High Level Requirements and Scope

2.1. Objectives

The main objective is to fulfil the Digital Data and Technology (DDaT) strategy for backup provision.

…Backup Infrastructure and software with the scale and scope to provide options for backup to cover our data centre and cloud estate encompassing a wide variety of Authority services whilst maintain data integrity as part of the transition between backup technologies. Any backup provision must be able to deliver a secure and stable platforms with options for extended protection such as immutability.

2.1.1. Currently this strategy is partly fulfilled by an existing Dell EMC Networker deployment. This deployment was implemented in 2015. Since implementation, the above strategy has been defined and we now require a consolidated platform that can be scaled to be consumed by projects and portfolios across the organisation as needed and to add the capability of immutability.

2.1.2. The current offering is providing live service with an existing SLA of 99.99% availability and we require to maintain this availability in our future service offerings. As this procurement does not involve the operation or management of the backup service it is understood that the availability shall be measured from an infrastructure and software application perspective. The Supplier shall ensure that the design agreed with the Authority enables the Authority to achieve the required service levels.

2.1.3. We will require a support Operational Level Agreement (OLA) to match the commitments from our incumbent suppliers and therefore require 24/7/365 Level 2 & Level 3 support of replacement Backup solution for this new opportunity.

2.1.4. As indicated above this procurement does not include the operation or management of the Authority backup systems therefore it is vital that the Supplier engages both with Authority teams but also with Authority third parties who hold the responsibility of providing the underlying service. Any activity involving the establishment, acceptance into service or support required from the Supplier to maintain the Authority service shall consider both the Authority and Authority third parties as required stakeholders.

2.1.5. The Authority must maintain existing backup images in line with our requirements for data retention and therefore any proposal must include both design and capability for the transition and ongoing maintenance of existing EMC Networker backups in the new backup solution. The expected outcome from design is that the Authority will be able to restore pre-existing backups for the currently defined retention periods. The Supplier will be provided with details of the volume of backups and their respective retention periods.

2.1.6. The Authority wishes to make use of infrastructure that can support rapid and cost-effective expansion both in scale and in scope.

2.1.7. The requirement for immutability is based on the Authority's strategic aim to make solutions "secure by design". The Authority requires that such immutability should be offered in a way that provides the highest levels of surety for the backups protected with such features – ideally by full separation of the immutable backups from the primary backups.

2.1.8. Immutability for the Authority refers to the continued efficacy of existing backups in the event of actions or events which impact the backup service. The Replacement Backup solution and its backups should not be affected by any such impact and ensure that the backups cannot be altered / deleted without appropriate procedure to ensure that the operation is authorised.

2.1.9. The Authority wishes to maintain storage for backups that can provide separate storage instances to allow for both storage local to the backup target and remote from the target. Therefore, the Replacement Backup solution must be able to provide backup storage capabilities in the Crown datacentres and all Authority cloud environments.

2.1.10. The Authority requires that the Replacement Backup solution be able to allow recovery of data in a timescale unaffected by backup operations or product limitations in relation to the relative priority of backup and restore jobs. An example would be a product that limits the speed of restore due to running backup jobs.

2.1.11. In the Authority Crown data centres, the Replacement Backup solution architecture must allow for the continued function of the Replacement Backup solution in the event of a loss of one of two physical datacentres.

2.1.12. The Replacement Backup solution shall resist malicious attempts to modify or interrupt the functionality of the backup product.

2.1.13. The Replacement Backup solution shall not be negatively impacted by the scale of the resources under protection.

2.1.14. The Replacement Backup solution shall be capable of maintaining a Authority backup methodology that allows for multiple copies of each backup stored on multiple devices in multiple locations. The Authority will determine for each backup target how many copies are required.

2.1.15. The Authority operates separate, secure operational environments. The Replacement Backup solution must support separation of responsibilities and separation of backups via a Role Based Access methodology.

2.1.16. This separation exists at the authentication, network, operations, technical and security assurance layers. The Supplier shall ensure that the Replacement Backup solution can work in such separated environments.

2.1.17. This separation must allow for multiple Authority and Authority third party teams to operate control over primary backups for their own workloads without access to primary backups for other workloads.

2.1.18. The separation must also account for the ability to maintain separate secondary backups of these workloads which would be managed via different Authority and Authority third party teams and not accessible to the teams responsible for the primary backups.

2.2. Supplier Characteristics

2.2.1. The Supplier shall (this is not an exhaustive list):

- Work collaboratively with the Authority and its suppliers
- Work pro-actively with the Authority and its suppliers in a spirit of trust and mutual confidence
- Cooperate with the Authority and its suppliers to enable the efficient delivery and operation of the Backup solution
- Assist in sharing information with the Authority and its suppliers for the purposes of facilitating adequate provision of the Services.
- Agree hand-offs across Supplier boundaries
- Provide joint problem solving and resolution of problems
- Collaboratively participate in the existing multi-Supplier change boards and move to modern release-based controls over time
- Assist the Authority in driving innovation to reduce cost, improve service and ensure diversity of service
- Work with the HO Assurance and 3rd party assurance leads to ensure an acceptable level of compliance and improvement

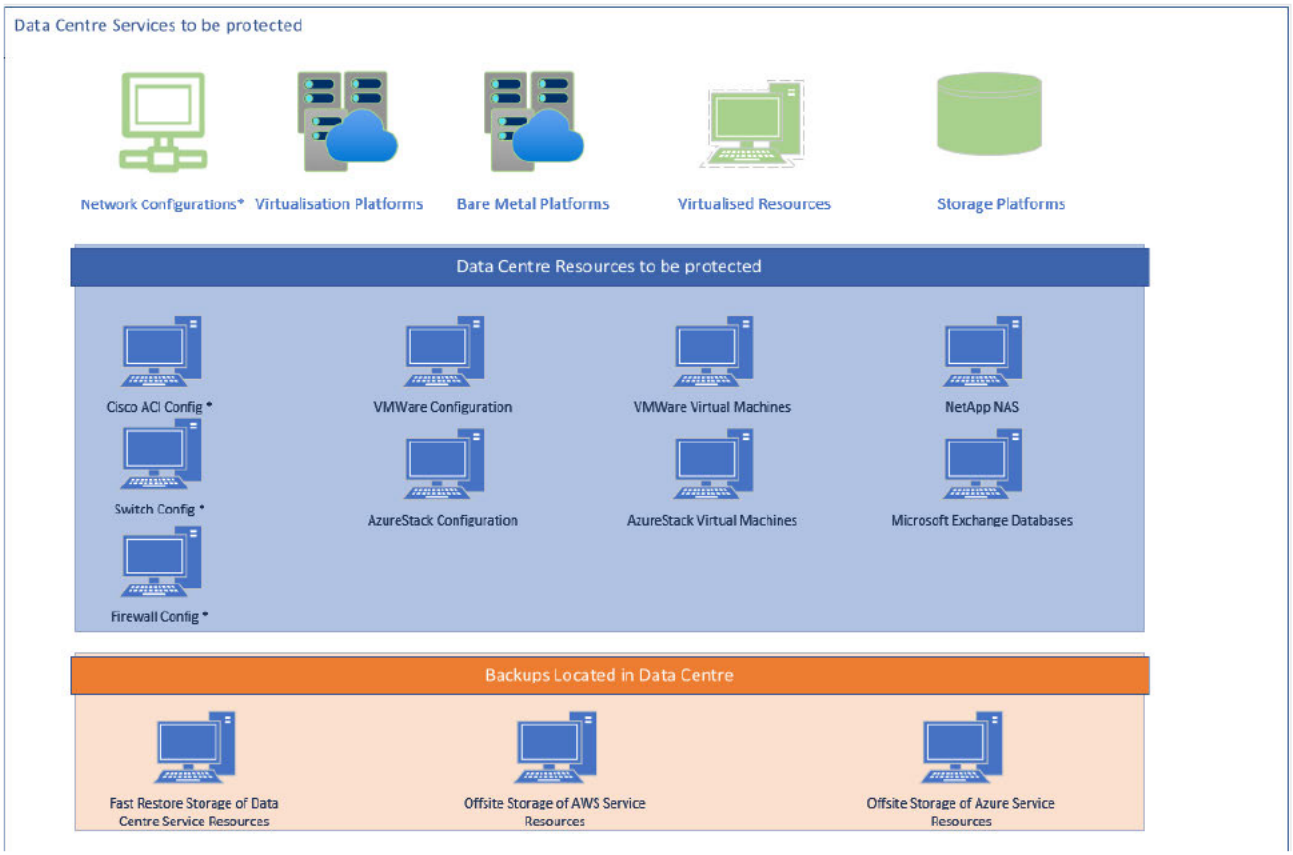
2.3. High Level Technical Scope

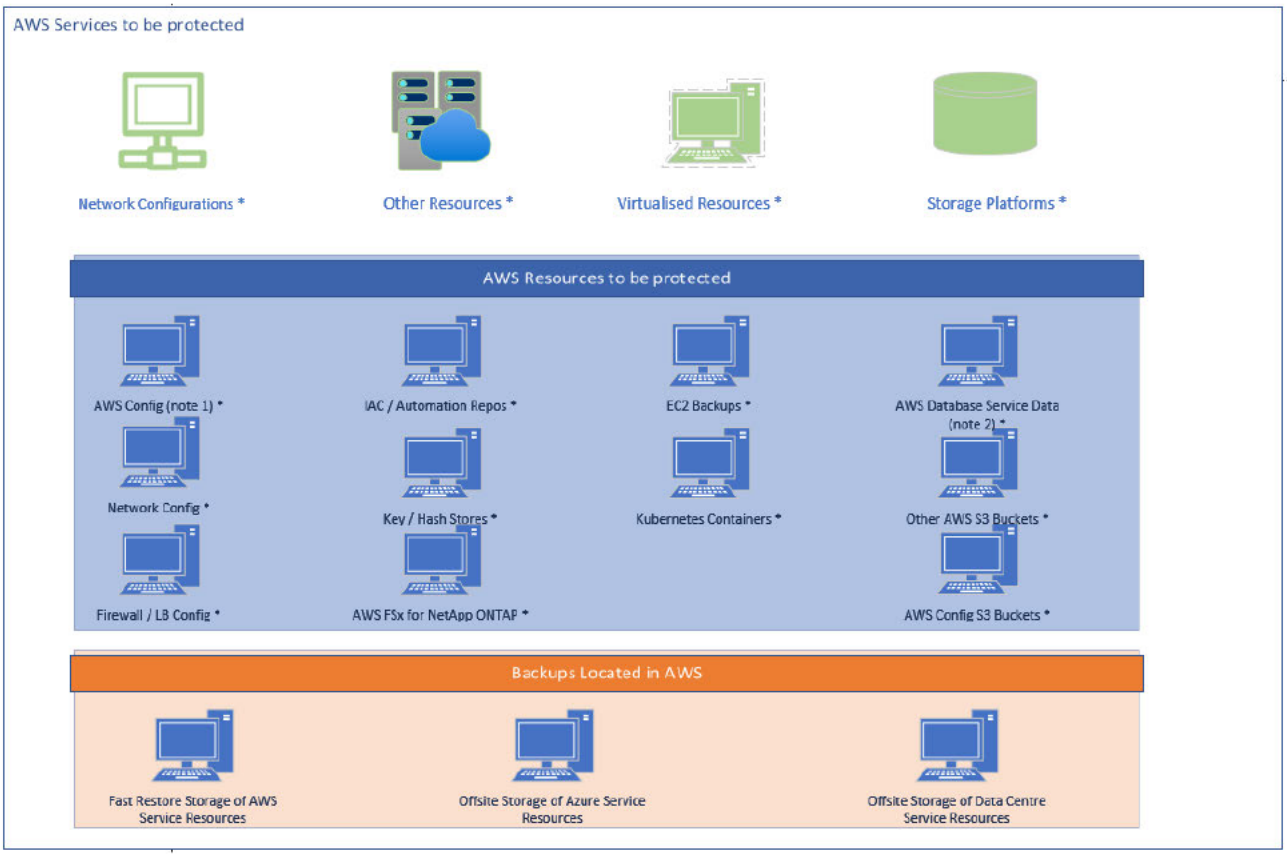
2.3.1. The high-level technical scope of the Replacement Backup solution is detailed in Figure 1 – High-level Technical Scope and will hereafter be referred to as the Backup Solution. Further lower level details are provided in the Data Library.

The services and resources to be considered within the potential scope of the Backup Solution are listed below

Note Services and resources marked with an asterisk are to be considered options for which the Authority may require backups but for which the Authority may require additional tooling / configuration. The Supplier should identify to the Authority any known integrations or best practice methodologies relevant to these services in their product.

2.3.2. The separately supplied document “Backup Target Matrix” should be completed by all Potential Providers to detail their integrations for the products listed in that document.


Data Centre Services to be protected
Network Configurations*
Virtualisation Platforms
Bare Metal Platforms
Virtualised Resources
Storage Platforms
Data Centre Resources to be protected
Cisco ACI Config *
VMWare Configuration
VMWare Virtual Machines
NetApp NAS
Switch Config *
AzureStack Configuration
AzureStack Virtual Machines
Microsoft Exchange Databases
Firewall Config *
Backups Located in Data Centre
Fast Restore Storage of Data Centre Service Resources
Offsite Storage of AWS Service Resources
Offsite Storage of Azure Service Resources


AWS Services to be protected
Network Configurations *
Other Resources *
Virtualised Resources *
Storage Platforms *
AWS Resources to be protected
AWS Config (note 1) *
IAC / Automation Repos *
EC2 Backups *
AWS Database Service Data (note 2) *
Network Config *
Key / Hash Stores *
Kubernetes Containers *
Other AWS S3 Buckets *
Firewall / LB Config *
AWS FSx for NetApp ONTAP *
AWS Config S3 Buckets *
Backups Located in AWS
Fast Restore Storage of AWS Service Resources
Offsite Storage of Azure Service Resources
Offsite Storage of Data Centre Service Resources

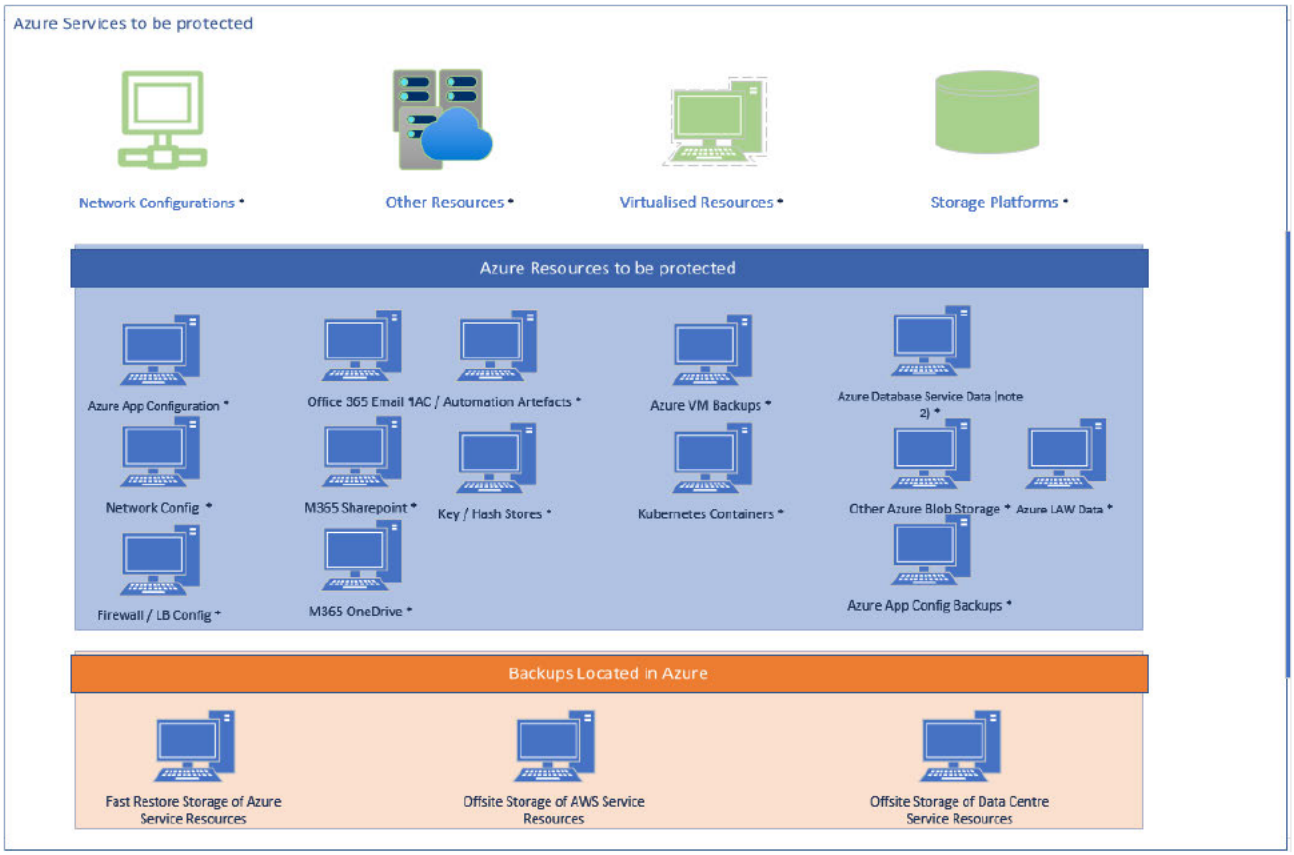


Figure 1 – High-level Technical Scope

2.4. High Level Call Off Contract Components

2.4.1. The Contract has 3 distinct components which are summarised below:

- Design of Authority implementation in co-operation with the Authority and Authority third parties
- Supply of materials to support Authority Implementation, Testing and Acceptance
- Ongoing Product Support, facilitate Expansion and supply of materials for Authority maintenance

2.5. Design

2.5.1. The Supplier shall follow the Authority approved methodology for Technical Architecture.

2.5.2. The Supplier shall provide a full set of architectural artefacts using Authority approved document templates to include as a minimum a context model, component model (high level design), deployment model (low level design), test plan and a delivery plan. The Authority will supply document templates to be used for these artefacts. Only artefacts produced using the supplied templates will be considered for agreement.

2.5.3. The Supplier shall work with the ES Technical Architect team and follow Authority governance models including both ADF and TDA forums.

2.5.4. The Supplier shall be responsible for supporting their design in the Authority processes required to transition the Replacement Backup into live service.

2.5.5. A design can only be considered agreed by the Authority.

2.6. Implementation Support, Testing Support, Product Acceptance and Handover

2.6.1. The Supplier shall procure and deliver the required solution components and liaise with the Authority to support the implementation of the associated Authority backup Service to the agreed design.

2.6.2. The Supplier shall assist the Authority to complete testing to the agreed test design. That test design shall involve engagement with the Authority Quality and Service teams.

2.6.3. The Supplier shall seek acceptance of the product delivery completion, resolving any issues identified.

2.6.4. The Supplier shall provide training, produce documentation and perform handover to Authoritys' Hosting Supplier as part of the Authority acceptance process.

2.7. Ongoing Maintenance, Expansion and Upgrade

2.7.1. The Supplier shall provide 24/7/365 support of the backup product to the Authority suppliers for all components supplied under this agreement.

2.7.2. The supplier shall engage with the Authority and their suppliers to scale the Service by further acquisitions of hardware and/or software under this contract as required.

2.7.3. The Supplier shall provide components to the Authority to facilitate Authority upgrades to the associated Service. These components may be hardware, software, configuration or documentation components.

2.7.4. The Supplier shall provide an example of a scheduled maintenance plan which shall be underpinned by an understanding that such a plan shall not impact agreed service levels.

2.8. High Level Contract Scope

In Scope	Out of Scope
OFFICIAL VxRail VMWare platform in Home Office Crown Data Centres	[redacted]
OFFICIAL AzureStack Hub platform in Home Office Crown Data Centres	[redacted]
OFFICIAL Netapp AFF storage platform in Home Office Crown Data Centres	
OFFICIAL AWS FSx NetApp ONTAP in Home Office AWS environment	
Any backup targets / storage as requested to be added by the Authority throughout the Contract Period by Change Control Procedure	
Bare Metal recovery	

Table 1 - Contract Scope

2.9. Overarching Requirements

2.9.1. The overarching requirements that cover all three components of the Contract are:

- All Supplier Personnel shall be Cleared Resources.
- All Cleared Resources to be located within the United Kingdom.
- All OFFICAL retained backups from the existing backup product (EMC Networker) must be transferred into the Backup Solution or otherwise made available for potential restore before the end of August 2023.
- Acceptance of the Backup Solution into live service must complete [redacted] as per agreed milestones.

2.10. Contract Exit

2.10.1. The Initial Term of the Contract is three years.

2.10.2. After the Initial Term, the Extension Periods may be exercised for either one or two further 12-month periods.

2.10.3. The Supplier shall produce a Handover Plan and enact a Handover process to carry out transition to the Hosting Capability supplier. The Handover Plan and Handover process must be delivered and agreed as part of Implementation Milestone Imp-M3.

2.10.4. On the expiry or termination of the Contract, the Supplier shall be responsible for all exit costs (both identifying and undertaking the agreed exit activities) incurred. The Authority considers the primary exit activity is the identification of all components that form the Backup solution for discussions to occur between Supplier and the Authority in relation to its removal or transfer into a potential new agreement.

3. Design Detailed Requirements

3.1. Overview of Design Requirements

3.1.1. This chapter details the constraints of the physical environment and the requirements of the Backup Solution design.

3.2. Authority Data Centre constraints

3.2.1. The Authority Data Centres have the following constraints:

3.2.2. Racks, power and any structured cabling for the Service is provided by the Authority

3.2.3. There is a 12-week lead time to install any request for additional structured cabling

3.2.4. Installation activities and testing of the components shall be provided by the Supplier, subject to relevant policies and procedures.

3.2.5. There is a maximum power and cooling constraint within the Authority Data Centre environments which should not currently exceed 109KwH per Data Centre.

3.2.6. The Data Centres HODC1 and HODC2 have solid concrete floors with no known loading constraints.

3.2.7. All cabling is overhead.

3.2.8. Inter cabinet patching is prohibited without leveraging structured cabling.

3.3. Design

3.3.1. The design is to be agreed solely by the Authority. The Authority has multiple customers and suppliers who are stakeholders in the backup Service that will be based on the Replacement Backup Solution. The Supplier shall provide the Authority with the information required to address any design query related to the Replacement Backup Solution.

3.3.2. The Supplier shall collate a table of deliverables in relation to design activities to be used to co-ordinate progress on design documentation approval. That table shall be maintained in the Authority document management system.

3.3.3. The Supplier shall perform a discovery of the existing Backup Solution based on materials provided by the Authority during the procurement. The discovery will be based on the provided extract of the current backup platform.

3.3.4. The Supplier shall provide a report detailing the output from the discovery process. This report will be used to inform the agreed design.

3.3.5. The Supplier shall produce a report detailing any remediation required in the existing platform to achieve the agreed design.

3.3.6. The Supplier shall provide a report which details both the capacity of the proposed backup platform and the utilisation of the capacity based on Authority requirements.

3.3.7. The Supplier shall detail in the design where functions may be enabled by additional procurement by the Authority.

3.3.8. The design of the Backup Solution will include reference to maintaining the existing backup platform that was the subject of the discovery but must ensure that no continuing reliance on the existing solution is required in the design to allow for the removal of the existing platform when retention periods expire.

3.3.9. The Supplier shall ensure the design details the available functions in relation to:-

- Billing
- Capacity management/future expansion
- Migration
- Protection
- Restoration targets

3.3.10. The Supplier shall ensure that the design details the initial physical footprint and connectivity requirements.

3.3.11. The Supplier shall ensure that the design details the power requirements at both power saving settings and at maximum performance settings.

3.3.12. The Supplier shall ensure that the design details the available expansion options for the backup product.

3.3.13. The Supplier shall ensure that the design details the physical resilience in a single data centre and between the 2 Crown data centres required.

3.3.14. The Supplier shall ensure that the design details how the SLA is to be achieved.

3.3.15. The Supplier shall ensure that the design details how Backup Solution shall be integrated into Service Management (ITOC) and Security (CSOC) tooling and processes.

3.3.16. The Supplier shall ensure that the design provides a fully populated Break-Fix RACI itemising the technical services and the support framework requirements in scope for agreement with the Authority. The RACI shall specify where there is a requirement for the Authority to participate in any service activity that is underwritten by the Service Levels.

3.4. Design Milestones table

3.4.1. Table 2 below shows Deliverables for Design Milestones Design-M1 and Design- M2.

Design Milestone Design-M1 – Security Clearance and Connectivity	
Deliverables	• Week 1: Submit all Supplier Cleared Resources (SC) requests/transfer requests for entire Supplier Personnel team where required. • Week 1: A proposed organisation chart of the Supplier Personnel with clearance expiry dates for any Cleared Resources who already hold the required clearance. To include Date of Birth and National Insurance Number • Week 1: Identify any physical infrastructure and networking requirements in the HODCs.

	• Week 1: Agree a document format for tracking issues and collaborative actions with the Authority and Authority third parties • Week 1: Provide dates for training courses for Authority and third parties to run in the timeframe of Design-M2
Design Milestone Design-M2 – Discovery and Architecture	

+9 Deliverables	• Achievement of Design Milestone Design-M1
	• Resource onboarding plan
	• Discovery Report (section 3.2.3)
	• Remediation Report (section 3.2.4)
	• MVP and Capacity Report (section 3.2.5)
	• Supplier Software and Supplier Background IPRs (Call Off Terms Clause 21.4.2)
	• Training courses delivered
	• Achieve Acceptance of architectural artefacts (section 2.4.2.2)
	  ○ Context Model
	  ○ Component Model (High Level Design)
	  ○ Deployment Model (Low Level Design)
	  ○ Delivery Plan
	  ○ Test Strategy Plan and testing artefacts
	• Within 30 Working Days of the Commencement Date, provide
	  ○ Business Continuity BCDR Plan (ref. 4.8.6.3 and Call Off Terms Clause Schedule S6 Business Continuity and Disaster Recovery)
	  ○ IT Service Continuity Management Plan
	  ○ Break-Fix RACI (ref. 3.2.14.1)
	• 20 Working Days of the Commencement Date, provide
	  ○ Security Management Plan (Call Off Terms Schedule S3 (Security Requirements), Part B (Long Form Security Requirements))

Milestone Date	Commencement Date + 4 weeks
Time of the essence? (Y or N)	No
Authority responsibilities	• Procure and provision POISE laptops
Milestone Payments	[TBC from Tender]
Delay Payments	None

Table 2 - Design Milestones

4. Implementation, Testing and Acceptance

4.1. Implementation

4.1.1. The Supplier shall procure all required hardware, software and accessories required for the implementation to be completed as per the agreed design.

4.1.2. The Supplier shall work with the Authority's teams to reserve or allocate physical data centre space and power, smart hands support and network connectivity required for the implementation to be completed as per the agreed design.

4.1.3. The Supplier shall allocate personnel for the implementation to be completed collaboratively (utilising Supplier, Authority and Authority third parties' resources) as per the agreed design.

4.1.4. The Supplier shall document the changes required for hardware installation and assist the Authority in seeking agreement via technical change control.

4.1.5. The Supplier shall liaise with the Authority Data Centre teams to arrange for delivery of hardware to both data centres.

4.1.6. The Supplier shall deliver the required hardware and associated accessories to both data centres

4.1.7. The Authority and Authority third parties shall perform the physical installation in both data centres and cloud environments. The Supplier will assist the Authority and Authority third parties with the installation by providing information as required.

4.1.8. The Supplier shall document the changes required for hardware configuration and assist with the Authority with gaining agreement via Authority technical change control.

4.1.9. The Supplier shall agree successful hardware and software configuration with the Authority.

4.1.10. The Supplier shall document the changes required for monitoring / management integration configuration and seek agreement via technical change control.

4.1.11. The Supplier shall engage with the Authority and Authority third parties to implement the agreed monitoring / management configuration.

4.1.12. The Supplier shall agree successful monitoring / management configuration with the Authority.

4.1.13. The table below shows Implementation stages and Milestones applicable to the implementation of the Backup Solution Service.

Implementation Milestone Imp-M1: Procurement and Delivery	
Deliverables	• Hardware and Software Ordered (section 4.1.1) • Reservation of HODC's Physical Space and Power (section 4.1.2) • Defined technical change for Network requirements (section 4.1.2) • Defined Resource Plan (section 4.1.3) • Required Hardware and Software delivered to HODC's (section 4.1.6)
Milestone Date	Commencement Date + 5 weeks
Time of the essence? (Y or N)	No
Authority responsibilities	None
Milestone Payments	[TBC from Tender]
Delay Payments	None
Implementation Milestone Imp-M2: Install and Configure	
Deliverables	• Achievement of Implementation Milestone Imp-M1 • Backup Solution Physical Install (section 4.1.8) • Backup Solution Monitoring Configuration (section 4.1.11)
Milestone Date	End of Discovery Milestone (Disc-M1) + 13 weeks
Time of the essence? (Y or N)	No
Authority responsibilities	None
Milestone Payments	[TBC from Tender]
Delay Payments	None

4.2. Testing

4.2.1. The Supplier shall provide details of vendor compliance tests to ensure alignment to the reference architecture design for the replacement backup product.

4.2.2. The Supplier shall provide collateral to allow the Authority to test all (including cross DC) failover capabilities of the replacement backup product to demonstrate compatibility with meeting SLA requirements.

4.2.3. The Supplier shall validate a performance baseline report for the Authority's Acceptance based on the data from the Authority test operations.

4.2.4. The Supplier shall participate in Authority security assurance and provide remediation of any Supplier materials or deliverables which are highlighted as requiring remediation during assurance.

4.2.5. The Supplier shall provide a report detailing their understanding of the completed test plan and confirm alignment to Supplier best practice for testing.

4.2.6. The table below shows Implementation stages and Milestones applicable to the implementation of the Backup Solution Service.

Testing Milestone ImpTest-M1: Design Baseline Conformance	
Deliverables	• Vendor Compliance Confirmation (section 4.2.1) • Failover and Resilience Confirmation (section 4.2.2) • Integration with existing toolsets and processes (section 4.2.3 / 4.2.4)
Milestone Date	Commencement Date + 13 weeks
Time of the essence? (Y or N)	No
Authority responsibilities	None
Milestone Payments	[TBC from Tender]
Delay Payments	None
Testing Milestone ImpTest-M2: Template Creation and Deployment	
Deliverables	• Achievement of Testing Milestone ImpTest-M1 • Templates Deployed (section 4.2.5)

	• Test Workloads Created (section 4.2.6) • Workload Migration Testing Complete (section 4.2.7 / 4.2.8) • Service Testing Complete (section 4.2.10) • Backup Testing Complete (section 4.2.12 / 4.2.13) • Performance Baseline Report (section 4.2.14)
Milestone Date	Commencement Date + 17 weeks
Time of the essence? (Y or N)	No
Authority responsibilities	None
Milestone Payments	[TBC from Tender]
Delay Payments	None

4.3. Acceptance

4.3.1. For the Authority to consider Acceptance, The Supplier will have obtained Achievement of both Implementation Milestone Imp-M2 and Testing Milestone ImpTest-M2.

4.3.2. The Supplier shall provide evidence for acceptance by the Authority to demonstrate: -

- Documentation of the provided Service
- Asset details of all infrastructure for inclusion in the Authority CMDB
- Licence details for all components
- Report detailing confirmation of compliant test results from Test Plan
- Sample of available operational reports (to include alert, event, capacity and billing reports)

4.3.3. The Supplier shall upon Authority Acceptance perform a handover operation to the Authority's Hosting suppliers.

4.3.4. The Authority shall Accept the handover operation as complete once all requirements have been met.

4.3.5. The Supplier shall seek Acceptance from the Authority to transition into Live Service.

4.3.6. Contract Commencement begins at Acceptance of Live Service.

5. Maintenance, Expansion and Upgrade

5.1. Maintenance

5.1.1. The Supplier shall provide Service Support of the Backup Solution Service including hardware break/fix and software support of the supplied components.

5.1.2. The Supplier shall provide 24/7 operational support for the Backup Solution platform to a 99.99% Availability Service Level.

5.1.3. The Supplier shall use the existing Authority Problem & Incident Management Processes and tooling in their support and maintenance role.

5.1.4. The Supplier shall use the existing Authority Technical Change Management processes and tooling in their support and maintenance role as required to maintain the Authority service.

5.1.5. The Supplier shall carry out the following support work:

- Operational – 24/7 operational support for Backup Solution infrastructure
- Performance – maintain all Service Levels
- Security – advise and offer mitigation for all cyber and data security concerns
- Monitoring and reporting where agreed with the Authority
- Maintenance of all hardware and software licence validity
- Maintenance of all support contracts

5.1.6. The Supplier shall adhere to all Authority policies and processes specified in the Contract, including those within Annex 6 of this document. Copies of these policies can be found in the Data Library section.

5.1.7. Shared service support (Authority, Supplier and Authority's Supplier)

5.1.8. The Supplier will have a general reliance on the Authority Networks and Infrastructure (N&I) team to grant the relevant access rights to network and compute components through Active Directory (AD).

5.1.9. The Supplier shall engage with both Authority and Authority's Supplier teams in relation to their Service Support responsibilities.

5.2. Out of scope for Supplier service support

5.2.1. The Authority and Authority's Suppliers are responsible for support of all infrastructure which is not part of the contracted Service.

5.3. Hardware and software licencing

5.3.1. The Supplier is responsible for buying hardware and software licencing for all in-scope services.

5.3.2. The Supplier is responsible for maintaining up to date Third Party Software licensing and is responsible for reporting consumption and volumes of the licencing against asset lists and advising when renewal is required. The Authority requires that the Supplier provide any information it has in relation to any licencing model which could provide reduced cost to the Authority.

5.4. Asset Management

5.4.1. The Supplier shall align to the Authority "Service Asset & Configuration Management Operating Model" policy for SACM (Security Asset Configuration Management).

5.4.2. The Supplier shall actively identify and inform the Authority about redundant Assets (hardware and software) to support cost reduction on a calendar quarterly basis.

5.4.3. The Supplier shall supply the required information to the Authority to facilitate the Authority to ensure all hardware and software remains on supported versions. The Supplier shall inform the Authority of any information that the Supplier requires in relation to the versions or update levels of any protected resource.

5.5. Knowledge Base

5.5.1. The Supplier shall align with Authority "Knowledge Management Operating Model" policy including providing details to the Authority to assist with writing and updating knowledge articles within the Authority service management tooling.

5.5.2. Information provided to comply with section 5.1.16.1 shall include, but not be limited to:

- Knowledge articles on all support and maintenance of the Service
- Knowledge articles to aid the correct routing of Service Incidents
- Knowledge articles to assist with the Shift-Left of Service Incidents resolutions by other support teams
- OLAs required to run and integrate the service
- CI Support Documents, Operational Manuals and Playbooks describing the end to end managed service operations, interactions and handoffs between suppliers

5.5.3. The Supplier shall support the Authority in writing and updating architectural, design and service documentation.

5.6. Expansion

5.6.1. For any agreed expansion, the Supplier shall assist the Authority by producing a full set of Architectural Artefacts and engaging with the Authority and Authority third parties to define a delivery, implementation, test and acceptance plan. The updated architectural artefacts will be presented by the Supplier for Authority approval. Please refer to section 4.1 for the detailed implementation requirements for any expansion.

5.6.2. The Authority expects to expand the scale and scope of the Replacement Backup solution during the initial term of the contract. The Authority requires that any additional licences, software or hardware provided by the Supplier to facilitate such expansion to be co-terminus with the initial procurement.

5.6.3. Expansion may require a new implementation which would be separate from the initial solution, in effect providing the Authority with more than one implementation of the Replacement Backup solution.

5.7. Monitoring and Reporting requirements

5.7.1. General Monitoring requirements

5.7.1.1. The Authority currently utilises a range of Monitoring and alerting tooling. One of the key ambitions for the Authority is to improve the scope, depth and visualisation of its Monitoring and alerting tooling.

5.7.1.2. The Supplier shall be responsible for defining Monitoring and Alerting thresholds for implementation by the Authority within the Authority tooling for the Backup solution as part of their design responsibilities.

5.7.2. Tooling capability and metrics

5.7.2.1. Existing Monitoring capabilities and metrics will be maintained until replaced as part of the development of Authority Monitoring requirements. The Supplier shall assist the Authority in identifying gaps in Monitoring, suggesting improvements to the current Monitoring design and collaborating with the Authority Product Engineering team on the future Monitoring design. The proposed solution must be able to natively generate alerts which can be integrated with ServiceNow using a method agreed as acceptable by the Authority to generate a support ticket for action by support staff in the event of failure of a backup job etc. Integration with Dell DPA would be advantageous: The Authority may consider a change to the product used for this function, but the functionality is required.

5.7.3. Documentation and Artefacts

5.7.3.1. The Supplier shall ensure that all documented artefacts describing the service model and its architecture are up to date, accurate and available to the Authority throughout the Contract Period.

5.7.3.2. Notwithstanding any other provision of the Contract, the Supplier shall provide the following documentation within 30 Working Days of the Commencement Date:

- Business Continuity Plan
- Break-Fix RACI

5.7.3.3. Notwithstanding any other provision of the Contract, the Supplier shall provide the following documentation within 20 Working Days of the Commencement Date:

- Security Management Plan

5.8. Authority policies and procedures

5.8.1. The Supplier shall adhere to the principles and policies as defined in all Authority and Government policies, processes and procedures listed in Annex 6.

5.8.2. Copies of policies and procedures listed in Annex 6 can be found in the Data Library. The documents listed in Annex 6 are for use in undertaking the obligations as set out in the Contract and must not be used for any other purpose.

5.8.3. The documents listed in Annex 6 may only be used within the scope of the current engagement with the Authority. Except with the express prior written permission of the Authority, these documents and the information contained herein may not be further published, disclosed, or used for any other purpose.

5.9. Testing requirements

5.9.1. The Supplier shall comply with the relevant Authority Quality Assurance and Testing Strategy and Standards in Annex 6**.**

5.10. Training requirements

5.10.1. All on-boarded Supplier Personnel shall complete any mandatory Authority training and compliance reviews at the cost of the Supplier.

5.10.2. The Supplier shall carry out training, knowledge transfer and skills uplift to help the Authority embed expertise of the Backup solution.

5.10.3. The Supplier shall help the Authority identify gaps in the current skills and capabilities of the workforce.

Annexes

3

6. Annex 1 Sizing

6.1. Current Volumetrics

Production currently has 196 active DPA reported unique clients, Pre-production currently has 40 active DPA reported unique clients. Total of 236 currently active DPA reported unique clients.

Backup breakdown

Environment	VMware	Filesystem	Exchange DAGs	NetWorker DB	Totals	Notes
Production	188	9	1	2	200	Note: 4 VMs also have agent backups configured. Hence the +4 from the original stated total.
Pre-Production	38	1	1	2	42	Note: 2 VMs also have agent backups configured. Hence the +2 from the original stated total.
Totals	-	-	-	-	242	Note: 6 VMs also have agent backups configured. Hence the +6 from the original stated total.

Typical backup schedule/retention

By default all virtual servers are backed up according to the following schedule:

1. A snapshot is taken of the entire VM including all intrinsic disks
2. A daily incremental backup is kept for two weeks
3. A weekly full backup is kept for one month

4. A monthly full backup is kept for six months
5. A yearly full backup is kept for one year

6.2. Required Initial Sizing

- The current protected capacity is 79TB over 242 servers.
- Required initial sizing is 1.5x current capacity and number of servers.
- This equates to 119TB protected data over 363 servers

Using the above retention schedule, current capacities are as follows:

	Protected Capacity (TB)	**Daily % Change (for incr backups)**				
	79	10.00% (7.9TB)				
Retained Backups	**Weekly Full**	**Daily Incr**	**Monthly Full TB**	**Yearly Full TB**	**Total (TB)**	**Total x1.5 (TB)**
Occasions Retained	4	14	6	1	-	-
	316.00	110.6	474	79	979.60	1469.40

7. Annex 2 – Defined terms

Word	Acronym	Definition
Scale Unit		
Alert		A warning that a threshold has been reached, something has changed, or a failure has occurred. Alerts are often created and managed by system management tools and are managed by the Event Management process. In the case of the Authority's IT Service Management Tool, ServiceNow, Alerts are created from Raw Events based on pre-defined rules, Event mappings and Service mappings.
Automated Alert		An Alert created automatically by monitoring or service management tooling in response to the breach of pre-configured thresholds or behaviours.
Available and Availability		End Users accessing services hosted on HO-IaaS are able to perform all agreed functions correctly, as set out in the Contract, and access and utilise all the functions of the services hosted on HO-IaaS.
Blended Day Rate	BDR	A single day rate for DMR Engineering resources provided by the Supplier and derived from the average of the Supplier's SFIA rate card against the positions requested in the Engineering Team.
Break-Fix		The replacement of a failed component in an infrastructure item.
Business as Usual	BAU	Business as Usual Work is unplanned or planned work that can happen unexpectedly or regularly and is usually relatively small. BAU for example includes (but not limited too) tasks like generating a regular report, answering support enquiries or setting up a product for a Authority, firewall rule Changes, creating Virtual machines, ACI tenants, regular and emergency parching and undertaking Standard Changes BAU work: • Seeks to maintain the same action steps day-to-day, like daily routines and processes

Word	Acronym	Definition
		• Repeatedly produces products or deliverables as part of everyday operations, such as a factory which produces only one type of product • Aims to continue to improve the output produced by normal business operations • Delivers the same general output every day
Change Management System	CMS	A system used to manage the lifecycle of ITSM change.
Cleared Resources		Supplier Personnel which have and maintain the following clearance levels: • Home Office Security Cleared ("SC") this is a Mandatory requirement for all resources Supplier Personnel • Non-Police Personnel Vetting – Level 3 ("NPPV3") this is a Mandatory requirement for all resources Supplier Personnel • Developed Vetting ("DV") as requested by the Authority All Cleared Resources to be located within the United Kingdom
Configuration Item	CI	Any component that needs to be managed in order to deliver an IT Service. Information about each CI, for example its Status, is recorded in a configuration record within the Configuration Management System and is maintained throughout its lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as process documentation and Service Levels.
Configuration Management Database	CMDB	A database used to store Configuration Records throughout their Lifecycle. The Configuration Management System maintains one or more CMDBs and each CMDB stores Attributes of CIs, and Relationships with other CIs.
Configuration Management System	CMS	A set of tools and databases used to manage IT Service Configuration data. The CMS also includes information about Service Incidents, Problems, Known Errors, Changes and Releases and it may contain data about employees, suppliers, locations, Business Units, Authoritys and Users. The CMS includes

Word	Acronym	Definition
		tools for collecting, storing, managing, updating and presenting data about all Configuration Items and their relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management Processes.
Configuration Model		The Configuration Model includes design of three data types within ServiceNow: • CI Classes/Types (e.g. Server, Applications, Databases) • CI Relationships (e.g. Application "Depends on" Server) • CI Attributes (e.g. Server specific attributes such as Server Name, IP address)
Continual Service Improvements	CSI	Continual Service Improvements (CSIs) are methods to improve quality, reduce failures and implement lessons learned with objectives measured in the following key areas: • Service efficiency savings • Service Level improvements • Automation • Service agility • Service improvements
Cyber Security Operations Centre	CSOC	The Authority's Cyber Security Operations Centre which provides protective Monitoring for some elements of HODCx.
Data Centre		A secure facility designed to house computer systems and associated components, such as communication and storage.
DDaT	DDaT	Home Office Digital, Data and Technology.
Demand Management Requests	DMR	Demand Management Requests are outcome-based work packages will include project management, architecture, design, development build, deployment, development testing and Service Transition for HODCx Infrastructure.
DevOps	DevOps	DevOps (a clipped compound of "development" and "operations") is a software engineering culture and practice that aims at unifying software development (Dev) and software operation (Ops). The main characteristic of the DevOps movement is to strongly advocate automation and Monitoring at all steps of software construction, from integration, testing, releasing to deployment and infrastructure

Word	Acronym	Definition
		management. DevOps aims at shorter development cycles, increased deployment frequency, more dependable releases, in close alignment with business objectives.
Early Life Support		A preliminary period of live running where tuning of workload resources takes place to optimise the operation of the workloads and the hypervisor.
Emergency Maintenance		Means ad hoc and unplanned maintenance provided by the Supplier where: • the Authority reasonably suspects that Services, or any part of the Services, has or may have developed a Fault, and notifies the Supplier of the same; or • the Supplier reasonably suspects that Services, or any part the Services, has or may have developed a Fault.
End User		Any person authorised by the Authority to use the IT Environment and/or the Services.
Event (General Definition)		A change of state that has significance for the management of a Configuration Item or IT Service. The term Event is also used to mean an Alert or notification created by any IT service, Configuration Item or Monitoring tool. Events typically require IT Operations personnel to take actions and often lead to Service Incidents being logged.
Event Management		The process responsible for managing Events throughout their lifecycle. Event Management is one of the main activities of IT Operations.
Event Management Plan (EMP)		The Event Management Plan (EMP) documents how Event Monitoring and management will be provided for a specific service or set of services. It is the agreement between the ITOC and the portfolio owning the service on the Event Monitoring and Management services to be provided by the ITOC.
Fault		A condition that causes a component to fail to perform its required function.

Word	Acronym	Definition
Front Door		Enterprise Services Front Door is the process to manage all non-standard requests from the business.
Head Service Level		This is the Service Level required for the majority of the performance, e.g. 95% P1 Incidents Resolved ≤ 4 hours
High Level Design	HLD	High Level Design – Process flowchart depicting each of the processes at a high level containing organisational swim lanes, process inputs & outputs, process phases and activities. Underpinning document containing process objectives, common principles and a matrix of responsibilities with responsibility narrative.
High Priority Incident	HPI	Service Incident which is of Priority 1 (P1) or Priority 2 (P2).
High Priority Incident Report	HPIR	A HPIR is requested from the Incident resolver group for a P1 or P2 Service Incident once it is Resolved/Fixed. The HPIR provides an overview of how the Service Incident was Resolved and any lessons learned.
HODC1	HODC1	Home Office Data Centre South East.
HODC2	HODC2	Home Office Data Centre South West.
HODCx	HODCx	HODC1, HODC2 and a third party Data Centre where the Home Office are a tenant, are included in the scope of this Contract. Adding any other Home Office or third party Data Centres into the scope of this Contract, such as Police Data Centres, will be performed under Change Control Procedure and, once added into scope, these will be incorporated into the "HODCx" definition.
HO-IaaS	HO-IaaS	Home Office Infrastructure-as-a-Service. Topology defined in section 2.5.1.
Incident		Unplanned interruption to, or quality reduction of an IT Service.
Information Technology Operations Centre	ITOC	The Authority's Information Technology Operations Centre.
Infrastructure as Code	IaC	A method of writing and deploying machine readable definition files that generate service components.
IT Service Management	ITSM	A set of processes to manage the implementation and operation of IT Services.

Word	Acronym	Definition
Key Performance Indicators	KPIs	KPIs evaluate the success of the Supplier in accordance with measures set out at Annex 2.
Level 2 Support		The Supplier's 2nd line team which shall be the initial point of engagement for Service Incidents assigned to the Supplier. Service Incidents must be raised on-tool via ServiceNow and will not be raised to the Supplier by phone or email except in the following circumstances: • SSD to follow up on open Service Incidents and Service Requests • Service Management for service escalations and call out of the Duty Manager Level 2 Support resources shall be experienced and knowledgeable technicians in all aspects of the supplied solution and able to assess issues and provide solutions for problems.
Level 3 Support		The Supplier's 3rd line support team which shall receive escalations from the Supplier's 2nd line support team for network, server and storage Service Incidents for the Official domain and performs fault diagnosis and Service Incident resolution. Level 3 Support resources shall have access to the highest technical resources available for problem resolution or new feature creation within the Supplier provided materials. These resources shall attempt to duplicate problems and define root causes, using product designs, code, or specifications.
Level 4 Support		The Supplier's expert technical capability in the event that Service Incidents or Problems require escalation to this level. It also supports Continual Service Improvement (CSI) and project initiatives with the High Level Design and Low Level Design activities needed for robust solutions. The team works normal business hours, Monday to Friday 8am to 6pm excluding public holidays.
Low Level Design	LLD	Low Level Design- Process flowchart depicting each of the processes at a lower level containing organisational and role swim lanes and process phases and activities. Underpinning process description matrix spreadsheet containing process steps, activity,

Word	Acronym	Definition
		description, inputs, outputs, touch points and role-based RACI matrix.
Maximum Tolerable Downtime	MTD	The sum of RTO and WRT which defines the total amount of time that a business process can be disrupted without causing any unacceptable consequences.
Maintenance Change		An alteration in state or configuration of a controlled item within the Change Management System (CMS).
Monitoring		Repeated observation of a Configuration Item, IT Service or process to detect Events and to ensure that the current status is known.
NIST	NIST	National Institute of Standards and Technology
Non-Available		In relation to the IT Environment or the Services, that the IT Environment or the Services are not Available.
Non-Disclosure Agreement	NDA	A Non-Disclosure Agreement is a legally binding contract that establishes a confidential relationship. The party or parties signing the agreement agree that sensitive information they may obtain will not be made available to any others. An NDA may also be referred to as a confidentiality agreement.
Notification		An automated communication sent from the Service Management systems via authorised channel such as email or SMS.
Official domain	O*	Official is a HM Government security classification and covers the majority of routine business information that is created or processed by government. Some of this information, however, can have damaging consequences if lost, stolen or published in the media. An example would be the personal information of staff or Authoritys requiring protection under the Data Protection Act.

Word	Acronym	Definition
		Official information is unmarked, that is, it does not carry a visible classification
OGD	OGD	Other Government Department
Operational Level Agreement	OLA	An OLA supports the Supplier's delivery of IT services to the Authority. The OLA defines the goods and services to be provided and the responsibilities of both the parties.
Permitted Maintenance		Maintenance which is determined, solely by the Authority, as being excluded from the calculation of Availability Service Level.
Planned Maintenance		Preventative maintenance for applications and infrastructure components which is planned for a future date.
Priority 1 Service Incident	P1	when a Service is Unavailable to its users or where performance is so poor the service becomes unusable.
Priority 2 Service Incident	P2	When a Service is severely degraded to its users or there is a loss of resilience which, although not resulting in, significantly increases the risk of, a P1 Service Incident.
Priority 3 Service Incident	P3	A component failure that does not affect the performance or resilience of the Service.
Priority 4 Service Incident	P4	A Service Incident that is cosmetic in nature or has no or little effect on end-users.
Problem		The cause of one or more Service Incidents.
Product Catalogue		A catalogue of consumable information technology related products and services available to customers.
Project Work		Project work: • Introduces a new or changed product. For example, a company-wide rollout of new technology. • Produces the product in a finite, set time period. For example, the technology rollout has a completion deadline. • Is unique in plans, specifications and deadlines. • Creates Change, procedures for which involve creating new BAU activities. For

Word	Acronym	Definition
		example, the technology rollout needs to be completed by a deadline. • Delivers specific output once. For example, a single large-scale tech install only happens once.
RACI		A model used to help define roles and responsibilities. RACI stands for responsible, accountable, consulted and informed.
Recovery Point Objective	RPO	Determines the maximum acceptable amount of data loss measured in time.
Recovery Time Objective	RTO	Determines the maximum tolerable amount of time needed to bring all critical systems back online
Release		A set of authorised changes to a service or component.
Resolve/Fix/ Resolution		When the Service is returned to a working state by rectifying the issue that resulted in a Service Incident, the state can be set as Resolved. If the user is satisfied with the resolution, the user can close the Service Incident, or the Service Incident is auto-closed after a certain time based on the Service Incident auto-close properties. Resolution means in relation to a Service Incident, either: • The root cause of the Service Incident has been removed and the Services are being provided in accordance with the Services Description and Service Levels; or • The Authority has been provided with a workaround in relation to the Service Incident deemed acceptable by the Authority.
Replacement Backup solution		The combination of hardware and software from the Supplier for which these requirements are defined.
SACM	SACM	Service Asset and Configuration Management.
SADI	SADI	Service Architecture Design & Implementation.

Word	Acronym	Definition
Scale Down Period		The Supplier, at the request of the Authority, shall scale down (remove) any Authority specified Cleared Recourses within a maximum of 2 weeks following the Authority's formal request. This shall also include (but not limited too) • Removal of any associated Charges to the Authority for the resource • Any adjustment to the Blended Day Rate • Preparing and submitting the Change Authorisation Note to reflect the Change
Scale Up Period		The Supplier, at the request of the Authority, shall scale up (add) any Authority specified (SIFA Professional Skills and SIFA Levels) Cleared Recourses within a maximum of 6 weeks following the Authority's formal request. This shall also include (but not limited too) • The addition of any associated Charges to the Authority for the resource • Any adjustment to the Blended Day Rate • Preparing and submitting the Change Authorisation Note to reflect the Change
SCOM	SCOM	System Center Operations Manager.
Security Incident		An event when systems or data is compromised or threatened, or when measures put in place to protect them fail, for example by: • Phishing attack • Ransomware • DDoS • System misconfiguration • SQL injection
Service Availability		This is defined in section 4.7.1
Service Continuity Event		A Service Incident which the Authority considers significant enough to raise as a disaster-level Event. Such an Event might limit Availability to multiple critical services.

Word	Acronym	Definition
Service Incident		An occurrence of a failure to deliver any part of the Services in accordance with the requirements, or the Performance Indicators, whether reported or not, that can disrupt or cause a loss of operations, services or functions.
Service Operating Hours		In relation to any Service, the hours for which that Service is to be operational.
Service Readiness Review	SRR	A standard governance process which determines whether the processes, documentation and skills are available to commence support for the live Service.
Service Request	SR	A request from a user for information, advice, a standard change, or access to a service.
Shift-Left		Moving the person, process, or technology closer to the Authority and/or resolver team, resulting in a faster and more efficient and effective outcome. Implementing more self-service capabilities and deliver standardisation and repeatable solution patterns and Service Incident resolution through automation.
Statement of Work	SoW	A written statement that specifically describes the phases of work or services, major tasks, or areas of responsibility the Supplier is to perform at a particular site, or within a particular locale during a stated period of time, according to a schedule of delivery. It defines project-specific activities, deliverables and timelines.
Strategic Service Desk	SSD	The Authority's service desk to co-ordinate Service Providers and their services to achieve the end-to-end service levels needed to support Home Office's business functions.
Target Operating Model	TOM	A description of the desired state of the operating model of an organisation. When working on the operating model, it is normal to define the "as is" model and the "to be" model. The Target Operating Model is the "to be" model.
Technical Design Authority	TDA	The Authority's DMR process and Architectural Governance Boards for reviewing and approving authority for new and amended High-Level Designs. Peer review, advice and guidance to Technical Teams.

Word	Acronym	Definition
Total Cost of Ownership	TCO	A financial estimate intended to help Authoritys and owners determine the direct and indirect costs of a product or service. It is a management accounting concept that can be used in full cost accounting or even ecological economics where it includes social costs.
Unavailable/ Downtime		In relation to the IT Environment or the Services, that the IT Environment or the Services are not Available excluding any Permitted Maintenance.
Unplanned Maintenance		Maintenance carried out as a result of unexpected equipment failure.
Work Recovery Time	WRT	Determines the maximum tolerable amount of time that is needed to verify the system and/or data integrity post the RTO for example, checking the databases and logs for consistency.

- *Table 4 – Defined Terms*

8. Authority Policies

The Supplier shall follow and conform to all Authority and HM Government policies, processes and procedures listed below (copies can be found in the Data Library):

8.1. Government policies

- The Government Digital Service Standards:
- https://www.gov.uk/service-manual
- The Government Digital Service Manual
- https://www.gov.uk/service-manual
- Government Digital Service Technology Code of Practice
- https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice
- Government Digital Services Technology Code of Practice – Collection of Related Topics:
- https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice-related-guidance
- Government Security Classifications
- https://www.gov.uk/government/publications/government-security-classifications
- General Data Protection Regulations
- https://wwwhm.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

8.2. Authority Policies - Cyber security

8.2.1.1. Cyber security policies that apply from Commencement Date (can be found in Data Library)

- Firewall Policy
- Cyber Risk Management Policy
- Cyber Assurance Policy
- Password Policy
- Account Management Policy and Standard
- Backup and Restore Policy
-

8.2.1.2. Cyber security policies that may become applicable through the Contract Period (not currently in Data Library)

Appendix C – Technical Questionnaire

Home Office

Crown Commercial Service

Appendix C – Further Competition Questionnaire

C23462 – Backup Platform Enhancement

RM6068 Technology Products and Associated Services:

Further Competition

Contents

Introduction 68
A. Overview 68
B. Mandatory Instructions 68
C. Generic guidance 68
D. Marking 69
Technical Questions and Technical Response templates 71
1. Company Information 71
2. Subcontractors/ Licensors. 71
3. Mandatory (Pass/Fail) Questions 72
4. Technical Questionnaire 74

Introduction

A. Overview

A.1. Appendix C – Further Competition Questionnaire (this document) provides questions you must answer and the response template for your answers.

A.2. The following information has been provided in relation to each question:

A.3. Weighting – highlights the relative importance of the question

i) Specific Guidance – sets out information for you to consider when preparing a Quality Response to a Quality Question, in addition to the generic guidance given at section 3.

ii) Response Template – sets out the maximum number of words available to you for use in the Technical Response to a Technical Question.

iii) Marking Scheme – details the marks available to evaluators during evaluation.

B. Mandatory Instructions

1.1. Your Technical Response to a Technical Question must be made within the blue shaded boxes provided after the Quality Question.

1.2. Your Technical Responses must be in Arial font, size 11 points or larger.

1.3. Each of your Technical Responses must be within both the page limit and the word limit provided for each Technical Question.

1.4. You must not make any change to this Appendix C – Further Competition Questionnaire apart from providing your responses to questions.

C. Generic guidance

A.1. Your Technical Responses should be relevant, concise and clear.

A.2. Your Technical Response to each Technical Question must be self-sufficient. You should repeat content you have used in other Technical Responses to avoid reliance on other Technical Responses.

A.3. Your Technical Response must address each part of the Technical Question, providing relevant, clear and concise explanations and facts that could help someone outside your organisation to understand how you will perform the Call Off Contract.

A.4. You are advised to consider compatibility between your Technical Responses and information provided in the ITT.

D. Marking

A.1. Your Technical Response to a Technical Question will be evaluated on how well your Technical Response addresses the guidance for the Technical Question and how well your Technical Response addresses the Buyer's purpose as set out in Appendix B – Statement of Requirements. A person evaluating a Technical Response shall assign one of the Technical Response Marks given in the following table:

Marks	Criteria
0	**Not Demonstrated** • No positive evidence provided that the response meets any element of the requirements.
1	**Minimal Demonstration** • Limited positive evidence provided that the response meets elements of the requirement. • Concern in a high number of significant areas needing considerable attention. • Significant reservations due to insufficient evidence to demonstrate competence or understanding.
2	**Moderate Demonstration** • Moderate positive evidence provided that the response meets elements of the requirement. • Some significant areas of concern exist needing attention. • Some reservations exist which prevent the response from demonstrating an acceptable level of competence or understanding.
3	**Acceptable Demonstration (Minimum Score the Potential Provider must achieve)** • Adequate positive evidence provided that the response meets most of the requirements. • Some issues of concern may exist. • Shows an adequate understanding of the requirements. • Sufficient competence demonstrated through relevant evidence.
4	**Good Demonstration** • Substantive positive evidence provided that the response meets the expected requirements and shows a good understanding of the requirements. • No significant areas of concern. • Some limited minor issues may exist.
5	**Strong Demonstration** • Substantial positive evidence provided that the response fully meets the requirements, including some evidence of exceeding expectations. • Provides added value and value-for-money by doing so.

	• Shows a full understanding of the requirements and considerable insight into the relevant issues.
6	**Outstanding Demonstration** • Evidence provided wholly exceeds the expected requirements. • Provides a deep understanding of the requirements and additional value in several respects above that expected. • Provides significant added value and significant value-for-money by doing so. • Leaves the evaluators in no doubt as to the capability and commitment to deliver what is required, and beyond.

Evaluation Element	Questionnaire number	Questionnaire	Total score available	Element Score
Information	(1)	Company information Potential Provider contact information	Information only	Note scored
	(2)	Subcontractors / Licensors	Information only	
Mandatory Questionnaire	(3)	Mandatory questionnaire	Pass / Fail	
Technical	(4.1)	Expansion Capabilities	8%	70%
	(4.2)	Product features that minimise Operational Impact	11%	
	(4.3)	Implementation in complex organisations	4%	
	(4.4)	Immutability and Ransomware	18%	
	(4.5)	Administration of the replacement backup product	15%	
	(4.6)	Licencing of the replacement backup solution	6%	
	(4.7)	Commitment to backup recoverability	8%	
Pricing	(5)	Total Charges	30%	30%
		Total		100%

Technical Questions and Technical Response templates

1. Company Information		
1.1	Please state your full company name	[redacted]
1.2	Please state your company number	[redacted]
	Potential Provider Contact	
1.3	Please state the contact's name	[redacted]
1.4	Please state the contact's telephone number	0[redacted]
1.5	Please state the contact's e-mail address	[redacted]

2. Subcontractors/ Licensors.			
	Use of Subcontractors or Licensors (Please note this includes 'associates' or anyone not directly employed)		
2.1	**Will you be providing all the Services yourself without using Subcontractors/ Licensors? (delete as applicable)**	Yes	
2.2	**If using Subcontractors or licensors, please state below the role and expected percentage of charges likely to be allocated to each sub-contractor.**		
Name		**Role(s)**	**Expected Percentage**
Subcontractor 1			
Subcontractor 2			
Subcontractor n etc *(add extra rows as necessary)*			

3. Mandatory (Pass/Fail) Questions

- **Instructions**
  - Potential Providers are asked to populate column "Able to meet requirement?" in the table in section 2 with:
    - "Yes" if the Potential Provider is able to fully meet the requirement; or
    - "No" if the Potential Provider is unable to meet the requirement or only partially able to meet the requirement.
  - If a "No" is selected against a requirement, the Potential Provider is asked to submit a response to explain their inability to meet the requirement.
  - In the event that a Potential Provider does not comply with a mandatory requirement, they may provide an alternative approach or workaround within their response. The Buyer reserves the right to assess whether the alternative approach or workaround is acceptable and not to "fail" the Potential Provider against these requirements

Mandatory Questionnaire

Ref	Mandatory Questions (Pass/Fail)	Document Reference	Able to meet requirement? Yes/No	If "No", please elaborate
1	Is the Potential Provider able to supply staff who are currently Home Office Cleared Resources, or willing to undergo the required Home Office Clearance?	Appendix B Specification and Requirements Section 2.6.1	Yes	
2	Is the Potential Provider able to meet all current NCSC security principles for encryption in Cloud , Network and Device security?	Cloud security guidance - NCSC.GOV.UK Device Security Guidance - NCSC.GOV.UK	Yes	

3	Is the Potential Provider able to meet the required milestone timetables and overarching contractual requirements	Appendix B Specification and Requirements Section 2.6, 3.3, 4.1.13, 4.2.6	Yes	

4. Technical Questionnaire

Technical Questions Overview (total weighting 70%)				
Contract Component	**Question Category**	**Question**	**Specification and Requirements Reference**	**Weighting (%)**
	Q4.1. Expansion Capabilities	How will the Potential Provider address the requirement of the Authority to make use of infrastructure solutions that can support rapid and cost effective expansion?	Appendix B Specification and Requirements Section 5.2	8
	Q4.2. Product features that minimise Operational Impact	How does the Potential Provider solution assist the Authority with the continuing operation of the backup system in the event of significant disruption to the Authority logical IT infrastructure?	Appendix B Specification and Requirements Section 2.1.8	11
	Q4.3. Implementation in complex organisations	How does the Potential Provider operate in a customer environment where an incumbent third party operates the backup service and who will implement the Replacement Backup solution?	Appendix B Specification and Requirements Section 2.2.1	4
	Q4.4 Immutability and Ransomware	How will the Potential Provider solution provide the Authority with confidence in the continuing availability and efficacy of the Replacement Backup solution?	Appendix B Specification and Requirements Section 2.1	18
	Q4.5. Administration of the replacement backup product	How will the Potential Provider solution minimise the administration and training burden of the Replacement Backup Solution for the Authority?	Appendix B Specification and Requirements Section 2.1.17 & 5.6	15
	Q4.6. Licencing of the replacement backup solution	How does the Potential Providers proposed Replacement Backup solution provide the	Appendix B Specification and Requirements Section 2.1.6	6

Technical Questions Overview (total weighting 70%)				
Contract Component	**Question Category**	**Question**	**Specification and Requirements Reference**	**Weighting (%)**
		Authority with a cost effective solution?		
	Q4.7. Commitment to backup and recoverability	How does the Potential Provider Replacement Backup solution provide the Authority with confidence in the operation of their backups?	Appendix B Specification and Requirements Section 2.1.10	8
Total weighting (%)				**70**

All Technical Questions within this Further Competition are directly specific to the subject-matter of the required Services. As such, all Potential Providers' responses to all Technical Questions and Social Value Questions must be specific to the delivery of the required Services and must not include statements on the organisation's general experience and capabilities which are not directly specific to the subject-matter of the required services.

Q4.1. Expansion Capabilities
How will the Potential Provider address the requirement of the Authority to make use of infrastructure solutions that can support rapid and cost effective expansion?
Guidance:
Your solution shall scale both in the size and scope of backup targets that can be protected. The Authority will favour solutions that scale with minimal effort and with little or no change to the level of administration required to manage the expanded solution. 1. Explain how your Replacement Backup solution scales for expansion in the number of protected workloads or in the size of storage as a result of growth of required storage beyond the initial procurement to ensure continuing efficient operation. 2. Explain what additional effort is required from the Potential Provider and from the Authority within your solution both to implement and run as a result of increases in scale or scope. 3. If professional services engagement is required for expansion, you shall indicate how much person effort from your professional services would be required to double the capacity of the initial installation required by the Authority.
Rubrik clusters scale without limit for both performance and capacity and do so without introducing additional management points or burden. Expansion is performed by customers with no services requirement and take less than 1-hour to configure. Additional features and functionality, such as advanced security scanning and detection functionality for data governance can be added by a simple addition of a license. **1&2. Scaling for Expansion and Ease:** Rubrik meets this requirement by natively supporting the most demanding workloads out of the box. Adding workloads is simply done via an intuitive HTML SaaS based UI following a simple workflow. Linear scale is a key part of the Rubrik software defined platform, simply add new nodes to the existing cluster, automatically discover, and add the capacity to the cluster, again, all through the single management interface. Atlas is the foundation of our Cloud-Scale File System that can be deployed on-premises, in the cloud, or even within a virtual appliance. You can consider this layer to be the “glue” of cloud data management, providing cloud-scale distributed file, metadata, and a cluster management system that was purposefully built to store and manage versioned data regardless of the infrastructure selected. It is designed to be infinitely scalable, adaptive and self-healing, application aware, and data integrity focused. Simplicity at scale, Rubrik wipes out management complexity with just a few clicks. By adopting the same web-scale technologies used by Google, Facebook, and Amazon, users can easily handle rapidly increasing volumes of information with a linear-scale architecture. Rubrik supports a variety of different sized appliance capacities, starting at 12TB all the way up to 150TB, all in a 2U chassis. These different capacity appliances can all be mixed and matched in the same cluster, allowing the HO to start small, to protect just a subset of overall workloads, and then seamlessly scale and protect the whole of the organisation as and when required. Cluster expansion is a simple process that can be accomplished via the HTML5 UI in a few clicks. The expansion process is fully documented. As clusters grow and are expanded, we not only increase the overall capacity, but, as we are adding additional

appliances to the cluster, the performance of the cluster increases as well.

Rubrik Standard Flash Appliance Specifications

rubrik

	Rubrik r6304s Small Environments	Rubrik r6404s Growing Environments	Rubrik r6408s Enterprise Environments	Rubrik r6410s Large-scale Environments	Rubrik r6412s Large-scale Environments	Rubrik r6416s Large-scale Environments	Rubrik r6420s Large-scale Environments	Rubrik r6408f Higher Security Standards	Rubrik r6416f Higher Security Standards
APPLIANCE SPECIFICATIONS									
Model	r6304s[1]	r6404s[1]	r6408s[1]	r6410s[1]	r6412s[1]	r6416s[1]	r6420s[1]	r6408f	r6416f
CPU	3 × 10-Core x86 2.2 GHz	4 × 10-Core x86 2.2 GHz	4 × 10-Core x86 2.2 GHz	4 × 10-Core x86 2.2 GHz	4 × 10-Core x86 2.2 GHz	4 × 10-Core x86 2.2 GHz	4 × 10-Core x86 2.2 GHz	4 × 10-Core x86 2.2 GHz	4 × 10-Core x86 2.2 GHz
Memory	192GB DDR4	256GB DDR4	384GB DDR4	384GB DDR4	384GB DDR4	384GB DDR4	384GB DDR4	384GB DDR4	384GB DDR4
Storage	9 × 4TB HDD	12 × 4TB HDD	12 × 8TB HDD	12 × 10TB HDD	12 × 12TB HDD	12 × 16TB HDD	12 × 20TB HDD	12 × 8TB HDD[2]	12 × 16TB HDD[2]
	3 × 400GB SSD	4 × 400GB SSD	4 × 400GB SSD	4 × 400GB SSD	4 × 400GB SSD	4 × 400GB SSD	4 × 400GB SSD	4 × 400GB SSD[2]	4 × 400GB SSD[2]
Network Connections	3 Dual-Port x 10GbE/ 25GbE (data)[3]	4 Dual-Port x 10GbE/ 25GbE (data)[3]	4 Dual-Port x 10GbE/ 25GbE (data)[3]	4 Dual-Port x 10GbE/ 25GbE (data)[3]	4 Dual-Port x 10GbE/ 25GbE (data)[3]	4 Dual-Port x 10GbE/ 25GbE (data)[3]	4 Dual-Port x 10GbE/ 25GbE (data)[3]	4 Dual-Port x 10GbE/ 25GbE (data)[3]	4 Dual-Port x 10GbE/ 25GbE (data)[3]
	3 Dual-Port x 10GbE or 1GbE (mgmt)	4 Dual-Port x 10GbE or 1GbE (mgmt)	4 Dual-Port x 10GbE or 1GbE (mgmt)	4 Dual-Port x 10GbE or 1GbE (mgmt)	4 Dual-Port x 10GbE or 1GbE (mgmt)	4 Dual-Port x 10GbE or 1GbE (mgmt)	4 Dual-Port x 10GbE or 1GbE (mgmt)	4 Dual-Port x 10GbE or 1GbE (mgmt)	4 Dual-Port x 10GbE or 1GbE (mgmt)
	3 × 1GbE (IPMI)	4 × 1GbE (IPMI)	4 × 1GbE (IPMI)	4 × 1GbE (IPMI)	4 × 1GbE (IPMI)	4 × 1GbE (IPMI)	4 × 1GbE (IPMI)	4 × 1GbE (IPMI)	4 × 1GbE (IPMI)
Useable Capacity (TB)	11.2	30	60	75	90	120	150	60	120

[1]Software-based encryption included, [2]FIPS 140-2 Level 2 self-encrypting drive, [3]Available in SFP+ 10GbE/25GbE or 10GbE

PHYSICAL & ENVIRONMENTAL SPECIFICATIONS									
Model	r6304s	r6404s	r6408s	r6410s	r6412s	r6416s	r6420s	r6408f	r6416f
Dimensions	2U Rackmount Height: 3.5" (88mm) Width: 17.6" (447mm) Depth: 30.5" (775mm)								
Weight Net Weight includes HDD/ SSDs. Gross Weight includes packaging and rails.	Gross Weight: 102.0 lbs (46.2 kg)	Gross Weight: 113.0 lbs (51.3 kg)	Gross Weight: 115.0 lbs (52.0 kg)	Gross Weight: 115.0 lbs (52.0 kg)	Gross Weight: 116.0 lbs (53.0 kg)	Gross Weight: 116.0 lbs (53.0 kg)	Gross Weight: 116.0 lbs (53.0 kg)	Gross Weight: 115.0 lbs (52.0 kg)	Gross Weight: 116.0 lbs (53.0 kg)
	Net Weight: 75.0 lbs (34.0 kg)	Net Weight: 86.0 lbs (39.0 kg)	Net Weight: 88.0 lbs (39.9 kg)	Net Weight: 88.0 lbs (39.9 kg)	Net Weight: 89.0 lbs (40.7 kg)	Net Weight: 89.0 lbs (40.7 kg)	Net Weight: 89.0 lbs (40.7 kg)	Net Weight: 88.0 lbs (39.9 kg)	Net Weight: 89.0 lbs (40.7 kg)
System Cooling	4 × 8 cm heavy duty PWM fans with optimal fan speed control								
Operating Environment	Op Temp: 10°C to 35°C (50°F to 95°F), Non-Op Temp: -40°C to 70°C (-40°F to 158°F), Op Humidity (non-condensing): 8% to 90%, Non-Op Humidity (non-condensing): 5% to 95%								
Power Supply	1200-2090W @ 100-240V / 14-9.8A, 50-60Hz Dual Supply for Redundancy/Hot-Pluggable								
Max Power Consumption	836 Watts	1023 Watts	985 Watts	985 Watts	985 Watts	985 Watts	985 Watts	985 Watts	985 Watts
Max Thermal Dissipation	2853 BTU/hour	3490 BTU/hour	3361 BTU/hour	3361 BTU/hour	3361 BTU/hour	3361 BTU/hour	3361 BTU/hour	3361 BTU/hour	3361 BTU/hour
Operating Requirements	Input Voltage: 100-240V AC auto-range, Input Frequency: 50-60Hz								

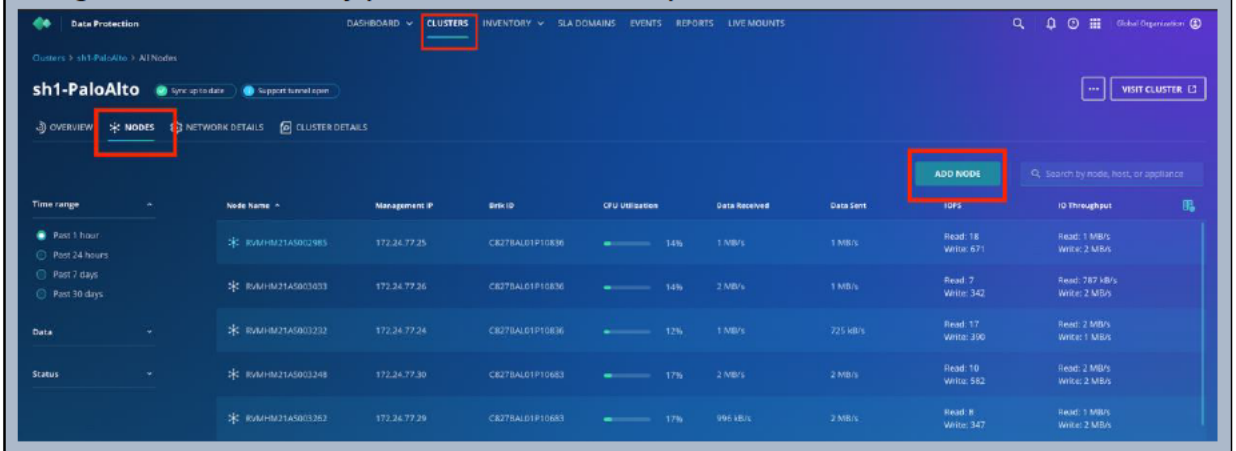
MODEL NAMING CONVENTION

r — 6 — 4 — 04

Rubrik | Product Family | # of Nodes | Disk Capacity

ss-r6000-standard-flash-appliance / 20221207

The Rubrik solution is a distributed, scale out, software defined platform that leverages commodity hardware for compute and storage resources. Expansion capabilities are achieved through software. By simply connecting new nodes to the Rubrik cluster network, a Rubrik service will discover the new hardware. An interface wizard will guide The Home Office (hereby HO) through specific network configuration requirements and then the additional storage and compute will seamlessly be available to the cluster. The whole process is completed via a UI wizard with an end-to-end process of 22 steps with 7 of those being clicks, 15 data entry points, 3 of which are optional.

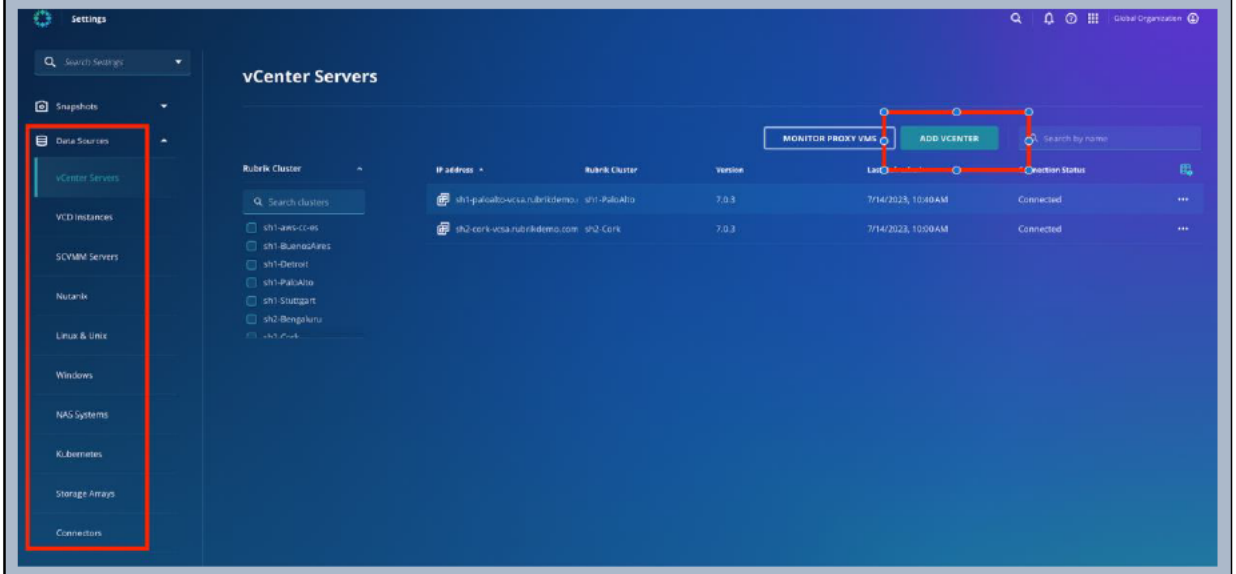


By adopting the same web-scale technologies used by Google, Facebook, and Amazon, The HO can easily handle rapidly increasing volumes of information with a linear-scale architecture. There is no hard limit to scale for a single Rubrik Cluster, we have customers with clusters containing over 190 nodes, protecting over 7PB of data across multi-appliance

clusters, scaling to protect hundreds of thousands of objects - virtual machines, databases, physical servers, NAS etc - who are reference customers and willing to openly discuss our solution.

Rubrik builds native 'snappable' integrations with many common backup sources using API and workload specific capabilities. This allows the very rapid addition of new workloads as a 'template' is used to onboard these new workloads. As everything is built in software, all this capability is included in the core platform. If you are initiating the backup migration starting with vSphere VMs, you can do that. As other workloads are migrated or adopted, you can add new data sources to the Rubrik platform and natively protect SQL, or Oracle workloads, M365 SaaS workloads, Cloud native workloads or even Kubernetes. The Rubrik platform scales as the HO and their services scale.

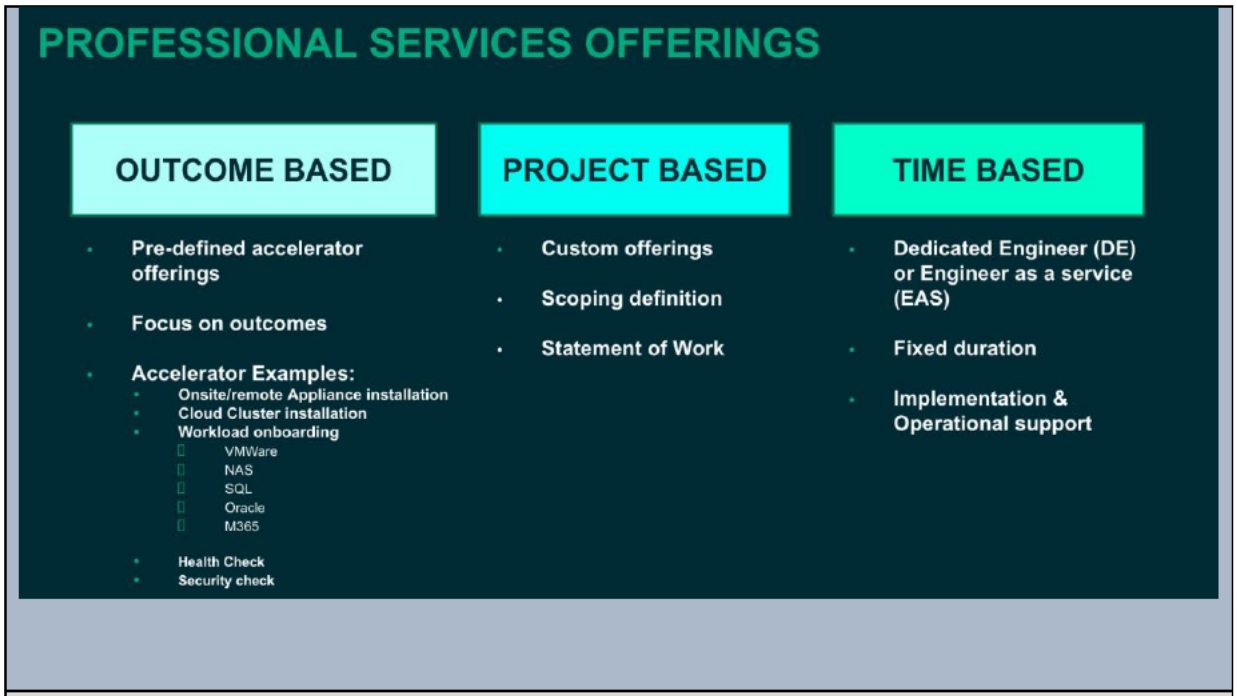
Unlike many other solutions, Rubrik does not utilise 3rd party technologies to facilitate protection of such other services, such as OEMing another technology to facilitate M365 protection alongside a traditional on-premise platform. This avoids multiple points of management, and inconsistency between policy and protection SLA's as data moves between repositories and consequently backup products. Whilst reduction of administration is an obvious benefit, it is the reduction of risk that benefits customers most by utilising a single technology across their estate.



3. Professional Services

There will be no requirement to engage Rubrik Support or Professional services to help an expansion, rapid or otherwise. Rubrik Support and professional services are available to assist or carry out work where appropriate, but as all our native integrations can be initiated via the UI, the process for the HO team, or designated third-party administrators, to complete this is very lightweight and quick and can be completed without any external assistance.

Rubrik Professional services are available and offer a wide range of services.



Marking Scheme:	
The following Marking Scheme will be used to assess the response provided to this question:	
0	Not demonstrated
1	Minimal Demonstration
2	Moderate Demonstration
3	Acceptable Demonstration (Minimum Score the Potential Provider must achieve)
4	Good Demonstration
5	Strong Demonstration
6	Outstanding Demonstration

Q4.2. Product features that minimise Operational Impact
How does the Potential Provider's solution enable the Authority in the continuing operation of the Authority backup service in the event of significant disruption to the Authority logical IT infrastructure?
Guidance:
The Authority requires a Replacement Backup solution which ensures that events which impact the Authority logical IT infrastructure are not disruptive to backup and recovery operations.

1. Indicate how the loss of Microsoft Active Directory authentication would limit the functionality of the proposed backup solution.
2. Indicate how your solution can operate in situations where the Authority required services to be backed up from or restored to a separate infrastructure deployed in response to disruption and what impacts licensing such a process may bring.
3. As part of the Authority's defence in depth strategy it is critical that the Replacement Backup solution integrates with the processes and procedures of the Authority teams that manage incident alert and response. You shall explain how your solution provides integration into customer environments in relation to security and health monitoring?
4. You shall highlight 3rd party products used in your solution that need to be separately secured, e.g., if the solution runs on a Windows OS and will require the OS to be secured separately.

Rubrik meets this requirement by delivering a highly resilient and secure platform. Removing any single point of failure and ensuring isolation of SSO (Single sign on) and local break class accounts as well as provisioning for service accounts.

1-Loss of Active Directory

Loss of Active Directory (AD) authentication mechanism would have no impact on your ability to continue ongoing backup and recovery operations.

Rubrik supports single sign-on (SSO) using the Security Assertion Markup Language (SAML) 2.0 standard. SSO allows the HO to log into RSC using credentials associated with an identity provider (IdP) of their choice such as ADFS, Azure AD, Okta, and OneLogin. SAML IdPs allow the HO to centrally manage identity, policy (password complexity, MFA requirements), and role mapping across their enterprise. This is the process you would normally use when your native authentication mechanism is operational. If you are using a centralised identity provider, it's recommended to grant access at a per-user level vs using group membership. That way, you can clearly see who has access and authorization to the Rubrik cluster.

In the event that your AD is unavailable or compromised, Rubrik's two-step MFA verification feature uses time-based one-time passwords in addition to the user login credentials to enforce multi-factor authentication on local, break glass user accounts. This is the most secure model for admins and critical accounts, with Time-based one time passwords (TOTP) and MFA enforced. Read-only and lower-privileged accounts can be sourced from AD or an Identity Provider. This will ensure that you have access even if your AD or Identity Provider is compromised.

This feature is an implementation of 2FA for Rubrik Security Cloud (RSC). You can enable Rubrik two-step verification to use 2FA mediated by time-based one-time password (TOTP), which provides an additional layer of authentication security. By using TOTP, Rubrik enforces multi-factor authentication (MFA) with the help of a single-use numeric code in addition to your login credentials. You can use an application running on your personal device, for example a smart phone, to generate the single-use numeric code. Rubrik two-step verification works with any TOTP application that complies with RFC 6238.

MFA enforcement is mandatory for all local RSC user accounts. Administrators must enforce Rubrik two-step verification for users at the global level. When enforced, each user must configure Rubrik two-step verification on an individual basis.

2- Restoration to Separate Infrastructure

Rubrik offers flexible licensing options designed for critical services companies. The program offers a cost-effective way to purchase Rubrik products and simplifies licence management with an easier solution to buy, consume, and manage Rubrik software. Key features include:

- Migrate Licence Anywhere, Anytime: Future-proof your Rubrik investment with licence portability across all Rubrik supported hardware platforms and the public cloud.
- Scale Predictably: Pay as you grow with flexible true forward model and on-demand capacity & planning.
- Maximise Cost Savings: Maximise discounts and savings by deploying a common IT platform across your organisation.

This licensing model allows the HO the flexibility to manage licensing as required.

Rubrik deploys a SaaS based centralised control plane, this is maintained by Rubrik and is accessible from anywhere. Cloud native solutions can be backed up without the requirement of physical storage on premises. Rubrik delivers the capability natively leveraging our own cloud storage.

In the instance where new physical infrastructure is deployed, Rubrik can support this in a number of ways;

- Additional clusters configured with replication from the primary site. This would see appliances in situ as part of a recovery/DR site that receives replicated backups and in the instance of any loss of the primary site, can directly take backups of other backup sources that might be running in the cloud or other physical locations.
- Appliances, physical and virtual that are deployed if/when and incident occurs. This would see the deployment of 'new' Rubrik appliances to backup and recover data in alternate locations as the HO decide.
- Cloud cluster - Rubrik software can be deployed in the cloud to support backup and recovery of cloud workloads.

Licenses are not tied to an appliance – you're not repurchasing licensing in the event of a disaster whereby new hardware is needed.

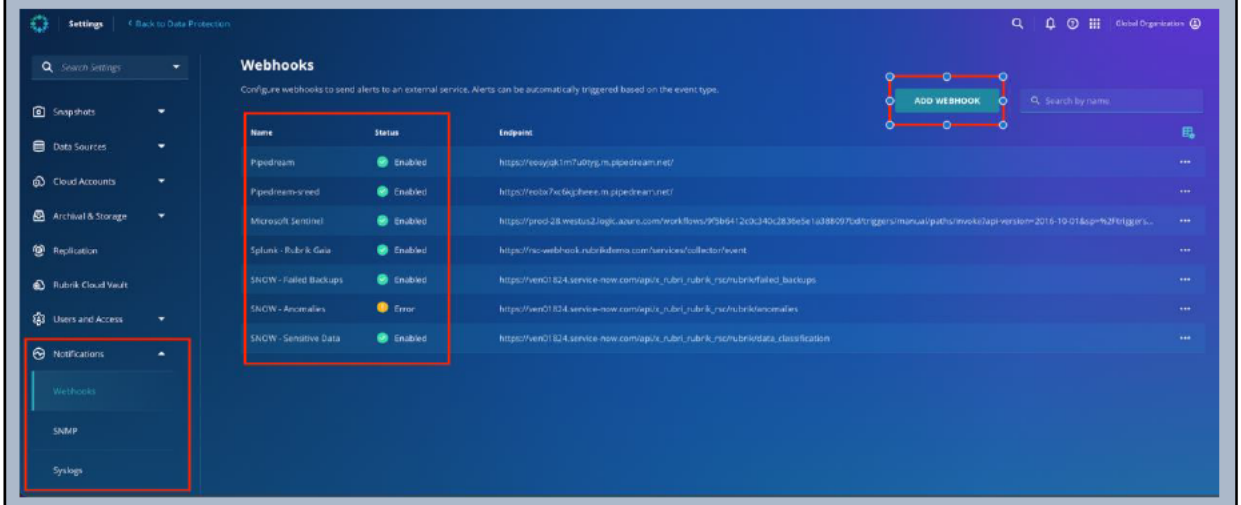
In all of these instances, Rubrik ingests backups and then indexes that data and supports it with metadata. This allows the connection of new clusters to the centralised control plane (RSC) and provides easy and quick recovery of data to new or different locations.

3- Backup Integration with Alerting and Response

All reporting, alerting and logging data can be easily integrated to other reporting systems via Rubrik RESTful API, with pre-built integrations already available out of the box for tools such as Splunk and ServiceNow. Rubrik supports SNMP v2, v3 and SNMP MIB-II queries and includes support for SNMP Traps for hardware events and Rubrik-specific MIBs to allow notifications about issues that may be occurring. The addition of these MIBs also allows integration of critical notifications with existing SNMP monitoring solutions, such as SolarWinds (or, indeed, any modern SIEM or other tool via Rubrik's open APIs).

Additional capabilities involve syslog and webhooks. The Rubrik cluster uses the standard syslog protocol for formatting and transmission of system notifications. By default, at the transport layer, the Rubrik cluster sets the syslog standard protocol and port (UDP/514). The transport layer protocol and port can be disabled or can be configured to use custom settings. At the application layer, the syslog transmissions use the HTTP protocol. When syslog support is enabled, the Rubrik cluster sends server messages to an external syslog server according to how the facility or severity levels are configured. The facility level represents the machine process that created the syslog event, for example, general system processes, such as the kernel, a user, mail. However, there are also facilities for Rubrik specific logs. The severity level determines how severe is the message that is displayed in syslog, for example, critical, warning, or purely informational. By default, Rubrik CDM sends all messages to syslog. The Activity Log displays all the messages.

Webhook integration enables sending data from RSC to external systems for monitoring and analysing the logs for any security incidents. When an event occurs matching the trigger conditions defined for the webhook, RSC makes an HTTP request to send the information to the specified webhook URL. You can use webhooks to store and manage all Rubrik log data at a centralised location and meet compliance requirements. You can also create roles to view and manage webhooks and assign them to users.



Rubrik provides full call home functionality and this monitors cluster performance, hardware health, and overall system information. Proactive alerts are triggered for a variety of different events. Not only does Rubrik offer an extensive suite of reporting, alerting and monitoring, we also monitor customer environments with a unique cloud-based "Sentry-AI" system. Sentry-AI automatically proactively alerts customers and Rubrik support of any issues with the environment and provides the tools necessary to help understand the cause and resolution for those issues.

4- Third Party Products to be Secured

The Rubrik platform runs on a custom, hardened Linux distribution that strips out all unused and unnecessary kernel modules and libraries, using the "JeOS" design paradigm. There is no backup data exposed over the network using standard protocols such as SMB/CIFS or NFS. When the Rubrik solution is upgraded, the underlying platform is automatically patched too. Meaning the HO don't have to be concerned with managing the OS vulnerabilities as you would with legacy 'appliance' platforms.

Rubrik does not use 3rd party apps as part of its customer facing solution. By using 3rd party tools, Rubrik believes we could introduce risk that is outside of its control. All software functionality is built and delivered by Rubrik.

The Rubrik platform complied with SOC 2 standards as well as SOC 3, FIPS 140 and CC as well as US federal regulations 'Department of Defence Information Network Approved Product List'.

Rubrik does have an internal vulnerability management program to manage vulnerabilities across its product, infrastructure, application and network ecosystem. The identification, analysis / prioritisation, remediation, tracking and reporting of vulnerabilities is managed through our vulnerability management program in line with our security policies. A dedicated security team is responsible for regular scanning of applications and infrastructure and vulnerabilities are assigned to the appropriate team (e.g., Engineering) and remediated based on internally defined SLAs. Tickets are tracked through to completion in our ticketing system and the program is audited by our independent SOC 2 and ISO auditors. Patches are tested before deployment and regular, independent penetration tests are conducted across all our products.

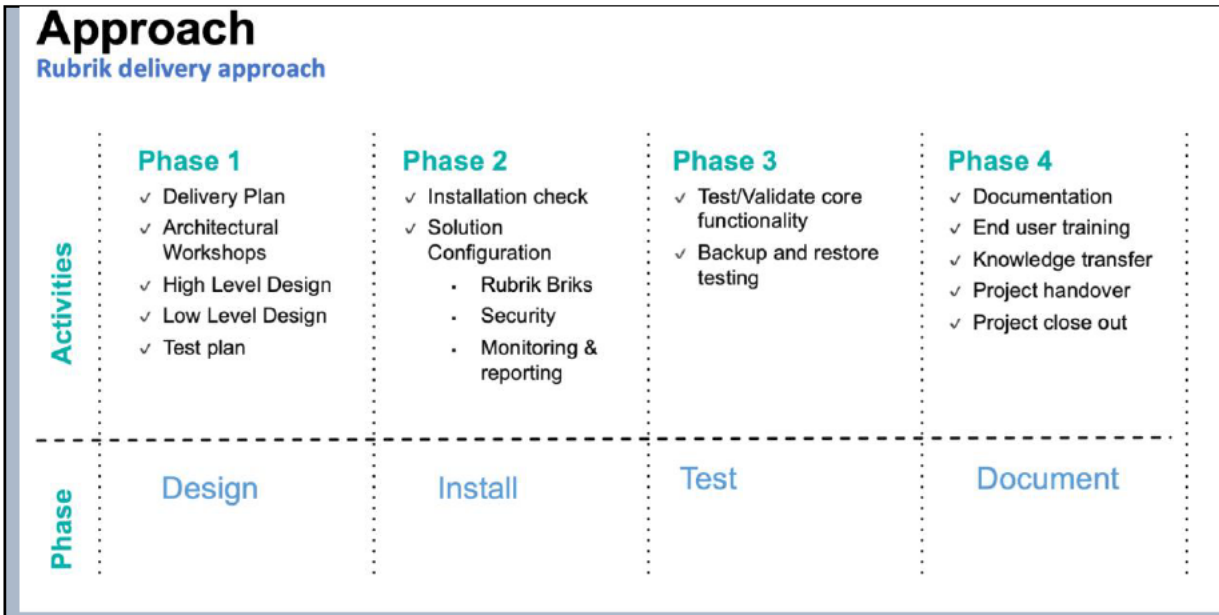
In addition to our internal vulnerability management and security testing program, Rubrik employs independent, third-party security experts to perform penetration tests prior to general availability (GA) of major product releases.

Marking Scheme:

The following Marking Scheme will be used to assess the response provided to this question:

0	Not demonstrated
1	Minimal Demonstration
2	Moderate Demonstration
3	Acceptable Demonstration (Minimum Score the Potential Provider must achieve)
4	Good Demonstration
5	Strong Demonstration
6	Outstanding Demonstration

Q4.3. Implementation in complex organisations
How does the Potential Provider operate in a customer environment where an incumbent third party operates the backup service and who will implement the Replacement Backup solution?
Guidance:
It is intended that the Potential Provider of the replacement backup will primarily engage with that third party to ensure continuity of service and provide information to that third party for their implementation of the Replacement Backup solution. 1) Explain how your processes and documentation will assist the Authority and its third parties with the implementation of the proposed solution. 2) Explain how you will work with multiple Authority third parties in the replacement of the Authority backup solution? 3) Explain any separation that exists inside the Potential Providers organisation for government customers, including any additional security measures placed on these separate teams. The authority wishes to ensure data sovereignty both in the use and administration of the solution. 4) Explain what features exist in the proposed solution to reduce storage volumes and data transmission volumes across the Authority network. Include details of any deduplication features and details of client to client, client to server and server to client communication flows.
Rubrik meets this requirement having deployed its platform in nearly 6000 global customers. Rubrik deals with customers directly, via partners, Global service integrators and Managed service providers on a daily basis, working collaboratively to successfully deploy, up-skill and operate the Rubrik platform. **1- How do Processes and Documentation assist** During the onboarding/procurement process, Rubrik provides a project manager and engineer to undertake the successful rollout of the Rubrik solution. We realise that every customer and environment is different and requires varying areas of focus, however at a high level, the process typically follows a 4 step process;



Throughout these stages, both the authority and 3rd party can be involved closely to shadow and collaborate with Rubrik to fully understand the implementation. Softcat can additionally provide engineering, architecture and assurance support if other technologies are identified as being within scope, e.g. if networking switches required reconfiguration or similar.

Continuing support is provided in the form of the Rubrik support portal allowing the authority and administrators access to all published documentation from Rubrik relating to platform configuration, upgrades, support and escalation processes, RFE processes etc.

Furthermore, the Rubrik university and training team can provide learning material in the form of self-paced courses or instructor led training, both virtual and physical.

The intention of the Rubrik services is to provide the authority with a fully deployed Rubrik platform with operators who are fully educated in the setup, configuration and operation of the solution; the project signoff will not be completed if these are not met.

Please refer to the attached 'Rubrik Professional Services Proposal' for more information.

As part of the implementation, Rubrik will ensure business and service continuity are at the forefront of delivery. In similar situations where Rubrik has replaced an incumbent backup provider, we propose the side by side operation of both the incumbent and Rubrik for a period of time until there are sufficient recovery points available in Rubrik, typically 1 month. This allows Rubrik to ingest the initial fulls and incrementals for that period. If anything needs to be recovered from the incumbent that can also be achieved.

After that initial period we would recommend powering off the incumbent but leaving it in situ. Experience tells us that any recovery after that period will most likely be a compliance or regulatory requirement, as in most cases, you would not recover data that old into production. If there is such a regulatory requirement, simple power up the system and recover. This also ensures the incumbent provider is isolated from any potential malicious activities that could risk the integrity of the backups, as it is often that in these situations the

licensing of the incumbent has lapsed and security patches are not supplied. Once a year has passed (Maximum retention period) and the Rubrik has a yearly full, the incumbent can be fully decommissioned.

2- Working with multiple third parties

As part of the project phase 1, Rubrik will work with all invested parties to properly understand the scope of the project. This will be in the form of physical and virtual meetings where appropriate, with the aim to define roles and responsibilities throughout the entirety of the project. Upon definition, where relevant individuals or parties are required to be involved in the phases of the rollout, Rubrik will plan accordingly to mutually agreed times where we can all engage in the successful outcome of the project.

Rubrik has nearly 6000 customers worldwide, with many of them leveraging service providers or 3rd party operators to manage the Rubrik platform. All projects have successfully engaged all relevant parties and delivered a completed rollout.

Please refer to the attached 'Rubrik Professional Services Proposal'

3- Separation for Security of Government Customers

Rubrik Security Cloud (RSC) is a centralised management console to manage all Rubrik deployments. RSC is a SaaS application maintained by Rubrik and hosted in GCP (Google Cloud Platform). The HO have their own isolated tenant for security. This will be hosted in a UK based region ensuring data sovereignty.

Within the operation of the Platform, Rubrik does not have access to customers' data.

The proposed solution includes on premises appliances that are controlled by security measures mentioned above, that would be located in your own secure data centres. Additionally as the rollout scales the Rubrik solution would include cloud native protection, M365 protection and Rubrik Cloud Vault. (See architecture diagram attached) In all of these instances, the HO can define granular access rights, data is airgapped, logically or physically as well as having credential isolation. Access to the data is controlled entirely by the HO and where cloud services are used they would be in the specific region the HO chooses to ensure data sovereignty.

4- Data Reduction Functionality

Rubrik supports both deduplication and compression. Data is compressed and deduplicated globally across each of the supported workloads. Deduplication is always on and is part of the base performance profile, in other words it has no impact on performance of the Rubrik cluster. Unlike traditional storage-centric platforms Rubrik is application aware and intelligent with regards to selecting the appropriate data reduction techniques to apply to different workloads. Hence, this helps provide the most efficient method of reducing data without placing the onus on skilled administrators to ensure they select the correct "mix" of storage optimization settings to get the best level of efficiency on storing backups.

Rubrik is purpose- built for backup and recovery. Rubrik has intentionally set out to architect its own distributed file system to meet this requirement. As a scale-out file system this removes the traditional issues of deduplication silos or having to implement additional hardware / dedicated resources to perform efficiency operations such as deduplication and compression. Due to the highly distributed, master-less, web-scale architecture of the Rubrik platform each cluster node can cooperate in storage optimization of the underlying backup data - this in combination with the design hardware streamlined to only run the required

services to operate (versus backup software installed on traditional off the shelf operating systems) means the system is secure and optimised to perform data optimization without the need for proprietary or additional hardware. Since Rubrik is a converged solution, the platform scans data at ingestion and can make intelligent decisions on what workloads to compare to (hash based method) in order to obtain the most efficient data reduction possible. Additionally, all incoming workloads are compressed. Deduplication ratios vary based on the data type and whether it is pre-compressed and/or encrypted. Overall deduplication rates are reported for the user to view in the Rubrik GUI.

Rubrik offers an automated, intelligent approach for data reduction, designed to minimise performance penalties of traditional deduplication techniques. Rubrik leverages host-side change block tracking (when available) for source-side data reduction such as VMware CBT. Rubrik also uses target deduplication to complement the incremental forever backup approach. while also deduplicating and compressing data globally across a cluster. This is performed after (post-process) the full backup and during (in-line) each subsequent backup. Additionally, all archived data is stored in a compressed, deduplicated format on the archival repository whether that is on premises or in the cloud.

Rubrik leverages LZ4, ZSTD and Gzip to provide compression to data.

Additionally Rubrik uses Erasure Coding (4,2) with a specific implementation of Reed-Solomon algorithms to improve performance, provide resiliency, and use space efficiently.

Rubrik delivers an incremental forever policy, where native integration to data sources allows identification and request of changed data only. This approach results in extremely fast backups after the initial full backup with multiple recovery options and greatly reduces the amount of traffic traversing the HO networks.

For example, the HO requires 1.5PB from the sizing in Appendix B §6.2 which calculates due to the Full backups required for weekly, monthly, and yearly recovery points:

6.2. Required Initial Sizing

- The current protected capacity is 79TB over 242 servers.
- Required initial sizing is 1.5x current capacity and number of servers.
- This equates to 119TB protected data over 363 servers

Using the above retention schedule, current capacities are as follows:

	Protected Capacity (TB)	Daily % Change (for incr backups)				
	79	10.00% (7.9TB)				
Retained Backups	Weekly Full	Daily Incr	Monthly Full TB	Yearly Full TB	Total (TB)	Total x1.5 (TB)
Occasions Retained	4	14	6	1	-	-
	316.00	110.6	474	79	979.60	1469.40

Rubrik produces synthetic full backups by chaining incremental snapshots, thus negating the need to actually store duplicate data. This does not affect restoration performance as it does with many technologies. Using the above metrics the sizing required for HO is as follows, and this has been reflected in our offering.

Summary of Data Center Workloads
Site - HO1

Reserve Capacity : 10%

Dataset	Usable Capacity Required (TB)	Reserve Capacity (TB)	Total Capacity Required (TB)	Seeding Bandwidth (Gb/s)	Incremental Bandwidth (Gb/s)
VM	144.5	16.06	160.56	-	-
ORACLE	30.49	3.39	33.88	-	-
Total	174.99	19.45	194.44	0	0

Estimate of Required Capacity from Year 0-5

Yearly Growth Rate (in %) : 10

Required Capacity	Year0	Year1	Year2	Year3	Year4	Year5
Usable Capacity Required	174.99	192.49	211.74	232.91	256.2	281.82
Reserve Space	19.44	21.39	23.53	25.88	28.47	31.31
Total Capacity Required	194.43	213.88	235.27	258.79	284.67	313.13

When it comes to replication of data in the case of a DR or secondary site, Rubrik supports throttling of traffic between Rubrik Clusters and between Rubrik Cluster and an Archive target and it will report if replication/archiving jobs are not complete. Replication and archive throttling overrides can be scheduled to specify how much bandwidth can be used for replication during specified days and times. Multiple throttle schedules can be set. For example, bandwidth can be more limited during business hours and increased during non-business hours. The bandwidth limits for archiving and replication are configured separately and are independent of each other. The bandwidth limits are configured at the Rubrik cluster level and available bandwidth is distributed dynamically between the nodes based on the load.

Marking Scheme:

The following Marking Scheme will be used to assess the response provided to this question:

0	Not demonstrated
1	Minimal Demonstration
2	Moderate Demonstration
3	Acceptable Demonstration (Minimum Score the Potential Provider must achieve)
4	Good Demonstration
5	Strong Demonstration
6	Outstanding Demonstration

Q4.4. Immutability and Ransomware

How will the Potential Provider solution provide the Authority with confidence in the continuing availability and efficacy of the Replacement Backup solution?

Guidance:

The Authority wishes to acquire a solution that is robust and responsive in the constantly adapting threat landscape.

1. Describe how your product achieves these aims and ensures that as threats develop that the product remains robust against them. You shall include any action that the Authority has to take in order to take advantage of such measures. You shall also indicate if any of these features require downtime within the solution in order to be implemented.
2. Describe how your product implements immutability of backups and what features exist in the product to ensure that your implementation of immutability cannot be compromised.

3. Describe the aspects of the solution which are designed to resist malicious attempts to modify or interrupt the functionality of the backup product by reference to the technical or software architecture of the solution.
4. Explain the attributes of the Potential Provider solution that do not support immutable storage, and any 3rd party functionality that is utilised to achieve this requirement. You shall further list any elements of the solution which cannot provide immutability of backups.
5. Detail any known chain of events which would compromise the restorability of any existing backup created by this solution.
6. Indicate your Replacement Backup solutions alignment to appropriate security guidance from NCSC and other recognised authorities such as NIST. You shall include specific reference to NCSC GPG13 in your response.
7. Identify all encryption used within the proposed solution both during data transfer and at rest. Detail any aspect of the solution which transmits or stores unencrypted data and provide an explanation of why encryption is not available for that aspect.

Rubrik meets this requirement by delivering a software defined platform built with a resilient, secure first design. Removing single points of failure and a self healing ecosystem. Delivering native, always on immutability, ransomware detection, sensitive data discovery, threat hunting and automated recovery.

1- The Rubrik solution was built upon a security first principle, aligning to one of the HO key themes. This solution is built upon a 'bunker in a box' mentality, meaning, by default Rubrik delivers;

- A hardened OS with all non-essential and vulnerable services removed and no root/shell access.
- All updates and patching are performed by Rubrik, incurring zero downtime.
- Natively immutable and air gapped proprietary file system
- Encryption at rest and in transit
- MFA and RBAC - SAML integration, local break glass accounts and roles ensuring no unauthorised or unauthenticated access.
- Retention lock with monotonic clock - NTP bypass is not viable on Rubrik.
- Insider threats are nullified by the Rubrik 2-person rule with support intervention.
- Services including ransomware investigation and sensitive data discovery are natively built into the software stack. There's no need to expose yourself to risk by using 3rd party services or marketplaces to 'bolt on' services.
- Rubrik is a software defined platform, any updates/upgrades are included with any valid support contract and can be applied through non-disrupting, rolling upgrades.

Rubrik Data Vault (Bunker in a Box)

- Retention Lock & NTP Protection
- External MFA & RBAC
- Always On Built-in MFA
- End-to-End Encryption
- No 3rd Party Applications
- Air Gapped & Immutable File System

Secure Hardened Linux
Vendor Patched & No Shell/OS Access
No Downtime Automated Upgrades

1. True End-to-End Encryption
- Client to Rubrik & node to node with no perf impact (mandatory DoD mode)
- In-flight TLS 1.2 SHA-512 hash & at-rest FIPS 140-2 L2 RSA 2048-bit key
- Key mgmt using TPM or KMIP for key rotation

2. Always On Built-in MFA
- Globally enforced using TOTP, no insecure email reset option
- Scan QR code with smartphone, secure any local or AD account in seconds
- Local account for recovery in event of attack (AD compromised)

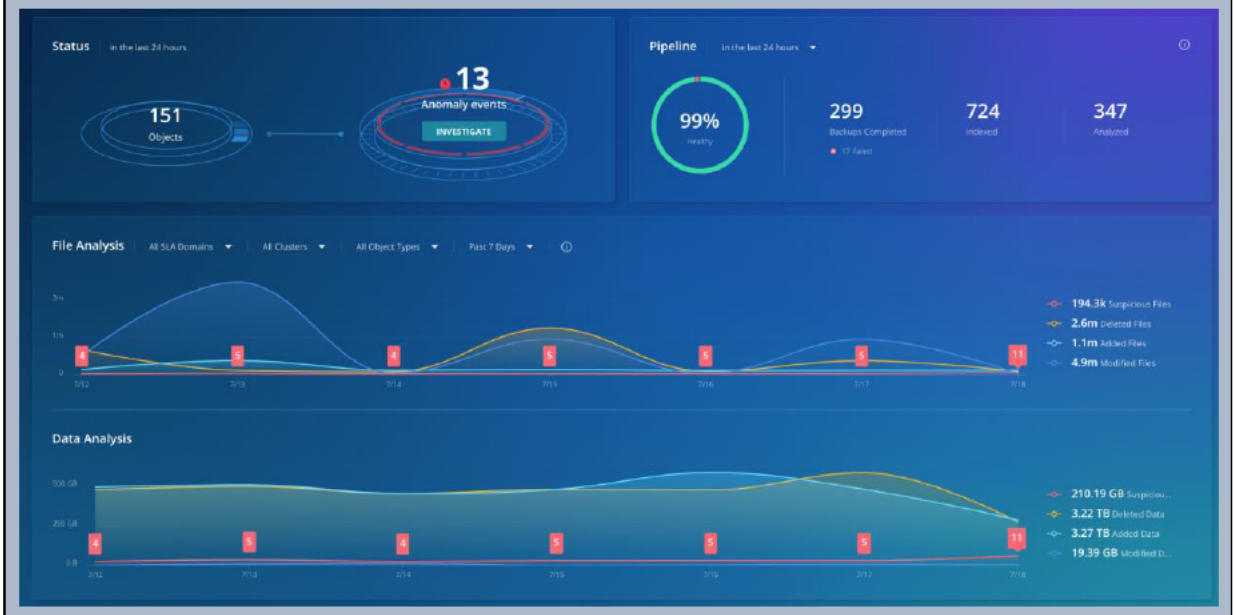
3. Secure AD User/Group Logins & RBAC
- Integrate into RSASecurID, Duo, anything SAML2.0 compliant
- Multi-factor on all AD integrated logins, alerts/syslog for failed logins
- RBAC, read-only admins, least privilege access & API tokens
- No login to backup without MFA, local or AD, also applies to SSH

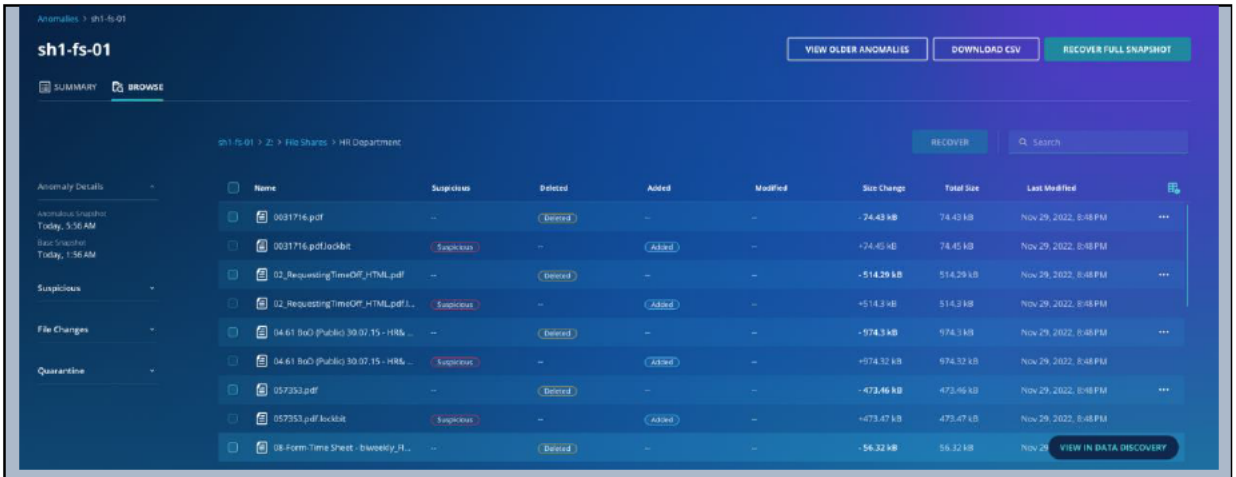
4. Retention Lock (with 3rd external verification)
- Prohibits backup admin from premature expiration, no storage impact
- 2-person rules for cluster configuration changes

5. NTP Protection
- Monotonic clock to prevent time jumps & NTP poisoning
- Cohasset validated - SEC 17a-4(f) & FINRA 4511(c) compliant

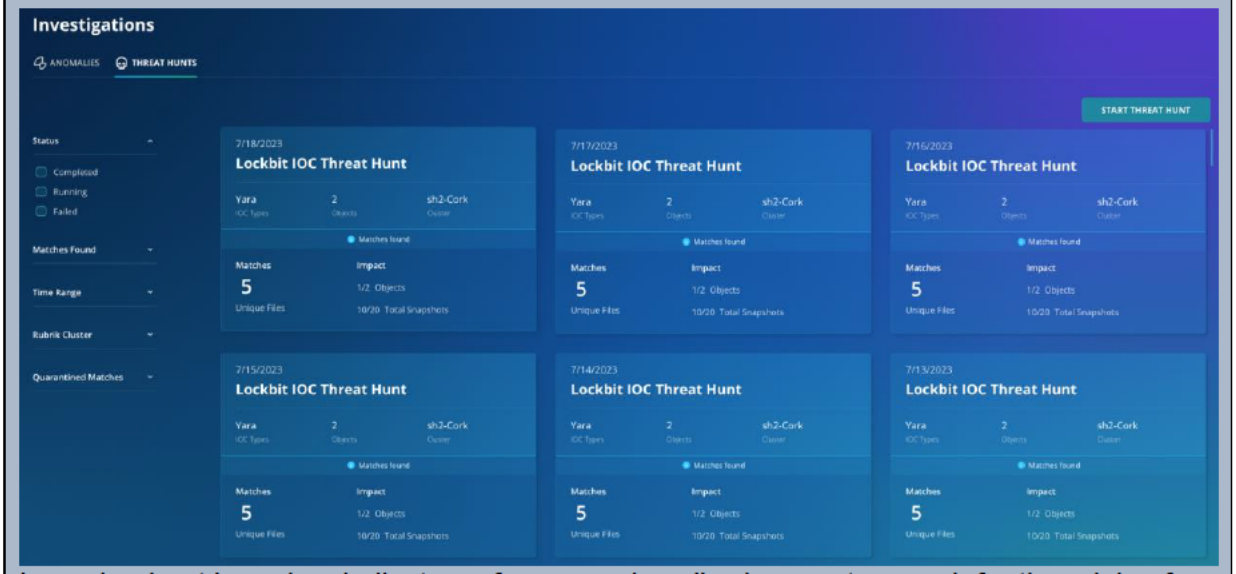
Air Gap + Immutable Filesystem + Encryption + Always On MFA + Retention Lock + NTP Protection
= Impenetrable From Inside or Ransomware Attacker & Truly Immutable

Rubrik provides ransomware investigation, threat hunting, sensitive data discovery and orchestrated recovery to help in the event of an incident. Rubrik analyses data, to identify anomalous behaviours across the entire time series of backups. Using encryption detection and AI/ML, Rubrik identifies ransomware events.

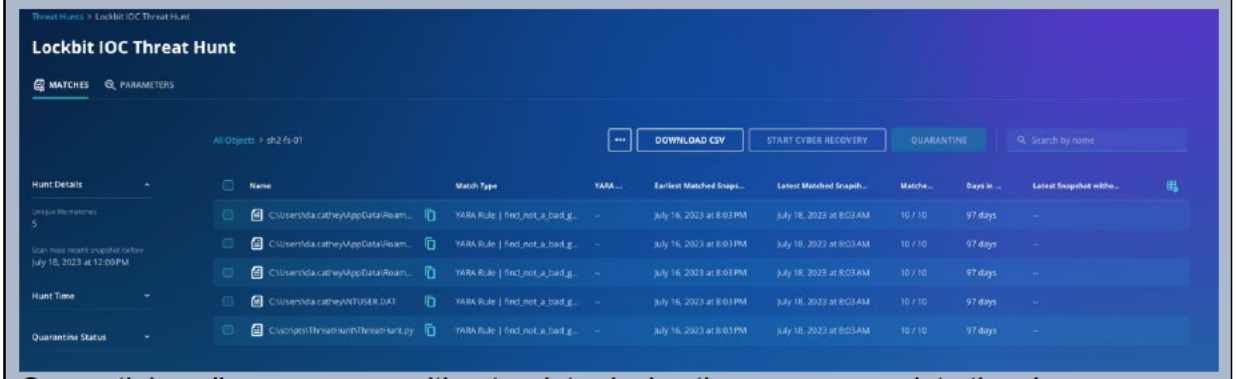




This allows you to understand the blast radius of an attack, identifying what needs to be recovered. But to ensure you don't bring back the malware, you need to threat hunt and find the source.

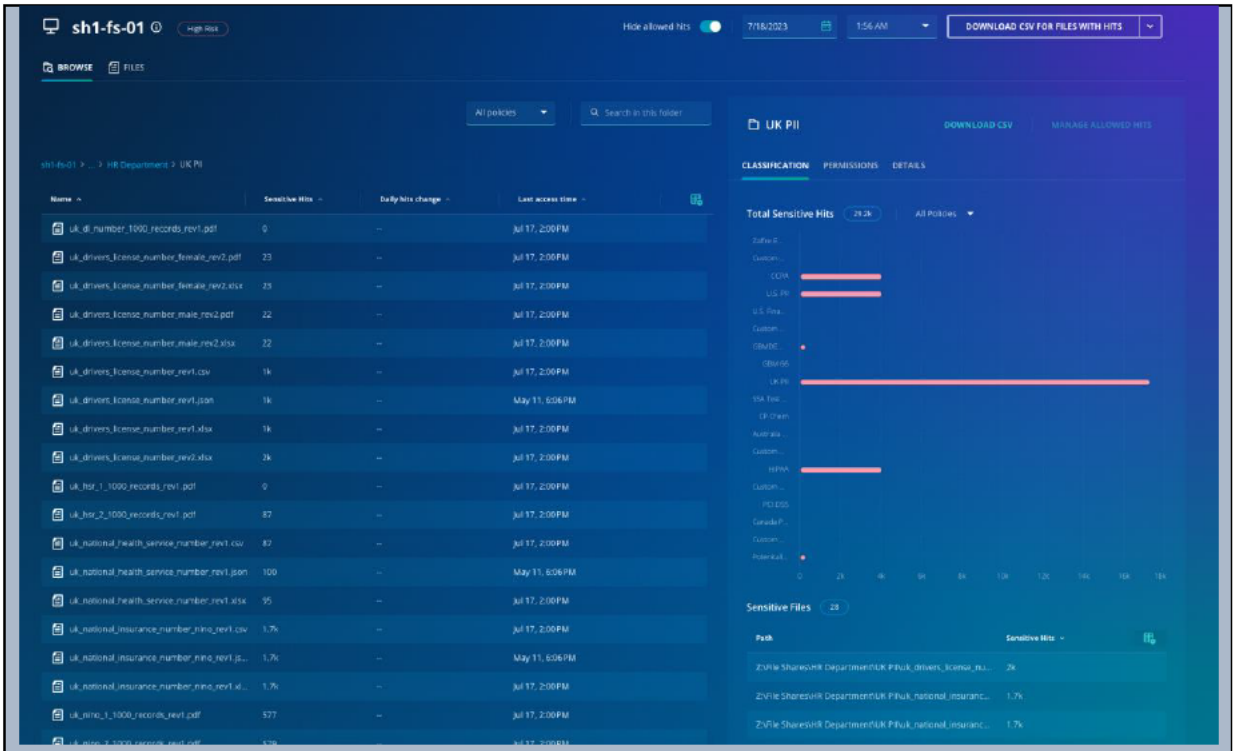


Launch a hunt based on indicators of compromise allowing you to search for the origin of the infection.



Quarantining allows recovery without re-introducing the ransomware into the clean environment.

Define search criteria to understand where sensitive data resides and if it was in the scope of an attack. Additionally, understand permissions assigned to files allowing you to deliver a more stringent least privilege access model, both important in regulatory matters.



2- Rubrik combines an immutable filesystem with a zero-trust cluster design in which operations can only be performed through authenticated APIs ensuring;

- Data is never exposed to external clients through insecure methods or protocols such as NFS or SMB. All operations have to be authenticated.
- All writes are out-of-place, meaning that new writes will never touch data written earlier.
- Data is fingerprinted at ingest and the fingerprints stored along with data to ensure that once written, the data is never changed.
- Cluster communications are secured using the TLS 1.2 protocol with certificate-based mutual authentication.

Rubrik constructed an immutable Filesystem (Atlas). This provides tight controls over which applications can exchange information, how each data exchange is transacted, and how data is arranged across physical and logical devices. Atlas is custom designed to be a distributed and immutable file system for writing and reading data for other Rubrik services.

Immutability is provided across two layers: the logical layer and the physical layer.

All data brought into the system is written into a proprietary Patch File. These are append-only files (AOFs), meaning that your data can only be added to the Patch File while it is open. All snapshot and journal data is held within Atlas, which enforces the use of Patch Files in the directory structure. The filesystem will refuse writes at the API level that are not append-only. Atlas has total control over how and where data is written. If your backup data has been modified, then it's essentially worthless. We solved this by ensuring that checksums are generated for each Patch Block within a Patch File. These checksums are computed and written to a Fingerprint File stored alongside the Patch File. Rubrik always does a fingerprint check before committing any data transformations. This ensures that the original file remains intact with forced validation during read operations.

To counter a ransomware attack, the original, validated data must be restored from backup. Rubrik routinely verifies the Patch Blocks against their checksums to ensure data integrity at the logical Patch Block level. Patch Files are not exposed to any external systems or customer administrator accounts. This ensures that meticulous care is taken to restore exactly what you originally stored in a backup.

While the logical layer focuses on data integrity at the file level, the physical layer focuses on writing data across the immutable cluster to achieve data integrity and data resiliency. Patch Files are logically divided into segments called Stripes. As Stripes are written, the AOF computes a Stripe level checksum, which it stores within each Stripe Metadata.

Stripes are further divided into physical Chunks stored on physical disks held within the cluster. Replication and erasure coding occur at the Chunk level. Similar to Patch Files, as each Chunk is written a checksum is computed and stored in the Stripe Metadata alongside the list of chunks. These checksums are periodically recomputed as part of Atlas' background scan by reading the physical Chunks and comparing against the checksums.

Rubrik delivers MFA, granular RBAC, end to end encryption, monotonic clock and retention lock, ensuring complete protection of the HO data and removes any threat of compromising the system.

Immutability and end to end encryption are always on.

3- Business continuity is a big part of ensuring you can recover from an incident. As described above, once data is in the Rubrik platform it cannot be changed. Built-in MFA and TOTP ensures that users are authenticated in a proper manner to restrict unwanted users. RBAC allows the configuration of access to users to follow the least privilege methodology allowing the HO to define roles for specific job functions relating to backup and recovery. This can be integrated with any SAML compliant directory service.

Rubrik's flexible deployment options allow for multiple Rubrik clusters, both physical and virtual, on premises and cloud based. This enables replication and backup and archive to the cloud providers. In the event of an emergency, recovery of data can be initiated to alternative sites. The platform natively includes DR, Isolated and in-place recovery plans with testing, ensuring recoverability and providing proof where auditors/regulators are concerned.

4- Rubrik natively provides immutability in its platforms as described above. As part of the flexible deployment options Rubrik can leverage public cloud platforms both in protection and also storage. Where this is carried out, Rubrik are reliant on the public cloud providers capabilities e.g. Microsoft Retention Lock and AWS S3 Object Lock.

5- Once a successful backup has been completed recoverability is always achievable. Rubrik performs integrity checks, described later in this document, along with the aforementioned security features to ensure recoverability is achievable even when data is across public cloud.

The circumstances in which this wouldn't be the case would be in the event such as the following;

- Lack of access to the platform (i.e. power outage, no network connectivity, DC

damage) this includes access to the SaaS based control plane AND lack of access to the local management instance running locally on the nodes.

- Lack of permissions on the user

6- Rubrik products and services are regularly independently verified for compliance, security, and privacy. Our continued investments are illustrated by the certifications and attestations of compliance below.

- GDPR
- Privacy Shield
- CCPA Compliance
- ISO 27001, 27017, 27018
- SOC2 Type II
- SOC3
- HIPAA
- DoDIN APL
- FIPS 140
- Common Criteria.

Rubrik follows guidance from recognised organisations such as NIST and NCSC. For example, modelled after the Zero Trust Implementation Model from NIST, Rubrik implements the following, providing maximum protection against attacks.

- ∉ MFA
- ∉ Least privilege access
- ∉ RBAC
- ∉ Encryption
- ∉ Immutability
- ∉ Sensitive data discovery

Proactive monitoring is critical when it comes to overseeing how systems are used or misused and the user accountability that goes along with that. There are general principles around how Rubrik deals with proactive monitoring.

- Strategy - Integrate into SEIM, SOAR platforms.
- Policy - User defined to support investigation
- Value - Provide actionable information bringing immediate value in the case of cost, recovery and reputation
- Provide - Deliver native capabilities to realise the above value
- Resource - Deliver knowledge, training and ongoing education
- Document - Intuitive user documentation and support portal
- Review - Ongoing management and customisation of policies.

7- Data-at-rest and data-in-transit are always encrypted. Rubrik clusters have the option to use software-based encryption or self-encrypting disks for data-at-rest. One of these options must be enabled to ensure that data within the system is safe and encrypted. Data must also be encrypted during transmission via TLS

certificates. Rubrik supports the import and export of TLS certificates signed by a Certificate Signing Request (CSR) or a key phrase, as well as wildcard certificates. Encrypting data-in-transit ensures that data cannot be copied ------- EXCEEDED WORD COUNT -30 WORDS HAVE BEEN REMOVED

Marking Scheme:	
The following Marking Scheme will be used to assess the response provided to this question:	
0	Not demonstrated
1	Minimal Demonstration
2	Moderate Demonstration
3	Acceptable Demonstration (Minimum Score the Potential Provider must achieve)
4	Good Demonstration
5	Strong Demonstration
6	Outstanding Demonstration

Q4.5. Administration of the replacement backup product
How will the Potential Provider solution minimise the administration and training burden of the Replacement Backup Solution for the Authority?
Guidance:
The Authority wishes to "shift left" common IT tasks, i.e., bring them into the organisation, and requires easy to manage applications to assist in that desire. The Replacement Backup solution shall ease the administrative burden for the Authority and its third parties in order to assist the Authority in this endeavour. 1. You shall indicate how many different applications and interfaces are used in the full administration of your Replacement Backup solution. 2. You shall estimate the expected administration burden (in terms of FTE) based on the Authority's requirements and supplied details of existing backup targets. Indicate which aspects of the proposed solution reduce the administration burden for the Authority and how these reductions are achieved. 3. You shall provide time estimates for the training required to become competent with the operation of your proposed Replacement Backup solution. It can be assumed that the candidate is competent with the existing backup product. 4. You shall explain how your solution will assist the Authority in upskilling staff who will be required to work with the solution. 5. Explain what default reporting is available within the proposed solution. 6. Explain any functionality within the proposed solution for automation of backups. For example, where a hypervisor or containerised solution is being protected is the addition of backups for any new virtual workloads automated by the proposed solution. 7. Where an agent application is required provide details of how the agent can be deployed using automation or installed by "push" technologies. Detail what permissions are required for these operations and whether the installation of an agent requires the agent target to be rebooted prior to the agent being used.
1- Rubrik Security Cloud (RSC) is a single-pane-of-glass management replaces all current backup software and secondary storage with a simple to set up, simple to use and simple to scale system. There are no requirements to licence any additional storage or software for the solution to work. RSC is a centralised control plane and is maintained by Rubrik and hosted in GCP (Google Cloud Platform), no additional infrastructure is required. Each individual customer has their own isolated tenant for security. Rubrik's simple to use interface will greatly reduce the administrative overhead of operating the environment. A basic understanding of backup and recovery is all that is needed to configure and operate Rubrik, reducing the number of staff hours wasted managing the environment. There is one update for the system. Administrators do not have to patch hardware, OS and software individually and don't have to worry about potential version conflicts between each layer. The Rubrik Backup Service, where needed, gets upgraded automatically when the system is upgraded, and no reboots are required. This ensures that no administrative time

is used to keep client systems up to date.

RSC provides a single touchpoint for global management of on-premises, at the edge, and in the cloud. This allows businesses to streamline operational costs and free up administrative time.

Key capabilities include:

• Global inventory: RSC aggregates the discovered environments of each Rubrik cluster. This provides users with a single global inventory of objects across the enterprise. With Global Object Search, users can search by object name to easily locate data regardless of location, providing full visibility and control over all applications and data.

• Global monitoring and reporting: RSC delivers a single easy-to-use dashboard to view global metrics on SLA compliance, infrastructure health, and performance.

• Global SLA policy management: A Rubrik SLA domain is a declarative policy that captures the core objectives for data protection and lifecycle management. The basic components of an SLA domain are - Backup frequency and retention, Continuous Data Protection (CDP), Snapshot window, Archive & Replication location. SLA Domains unify data protection policies under a single policy engine within RSC. Users can effectively centralise management across the entire enterprise with a single pane of glass across on-prem, edge, and cloud applications running in AWS, GCP and Azure.

2- As stated above, all administration is achieved through RSC. The amount of time spent administering, upgrading, patching multiple platforms and interfaces will reduce greatly.

Furthermore, having a single audit trail and monitoring and alerting platform significantly eases the effort in troubleshooting and MTTR in terms of incidents.

The SLA domains that Rubrik employs are a dramatic change to the current legacy approach of backups. The Rubrik SLA domains remove the burden of managing multiple backup schedules and windows and can provide the following benefits for The HO;

1. Save time - You only need to create a single Global SLA to use on any cluster
2. Reduce risk - if you need to change an SLA to align to new business requirements, you only need to edit a GSLA once instead of doing it multiple times reducing the risk of misconfiguration.
3. Centralised visibility - easily create reports that span across the environment.

Service Level Agreements (SLAs) unify data protection policies through a single policy engine.

Policy	Description
Snapshot and backup frequency and retention	Directs the Rubrik cluster when to create point-in-time snapshots or backups of data sources and how long to keep the data.
Replication	Directs the Rubrik cluster to send replicas of source snapshots or backups to a target Rubrik cluster and defines the maximum time to keep the replica on each cluster.
Archiving	Directs the Rubrik cluster to move snapshot or backup data to a separate data storage system for long-term retention.

As you can see the only required input for a SLA domain is frequency and retention. by defining these to align with business RPO and RTO's, the Rubrik solution will automatically ensure backups are taken to ensure you remain in compliance with the business needs. Native API integration to the data sources allow us to monitor the source hosts/data and identify the appropriate times to make the backup call without interfering with production performance. This simple declarative policy-based approach can reduce management time by up to 75%.

Typically, there are 2 major version updates per year, a summer release and a winter release. With incremental patches in between for interim product enhancements, bug fixes and security patches. Upcoming and available updates, along with the severity and priority information are communicated to our customers via regular updates from Rubrik support and are also visible from the Rubrik Security Cloud dashboard. A popular feature within the upgrade process is the version release table, allowing Rubrik customers to see the adoption rate and trend of versions, and the days since the last minor patch was released.With each release, Rubrik provides release notes and an updated compatibility matrix, to ensure our customers can check for version (e.g. Hypervisor, OS, DB, RMAN etc) compatibility before any upgrade. Should the HO have any questions or concerns, Rubrik support and the account team would be happy to assist.

Rubrik support can also undertake the upgrades for The HO if required, or be on hand (via the support tunnel) to support the HO. Upgrades use a dual partition methodology. With dual-partition upgrades, the new software is provisioned in the second partition. The first partition retains the original version and can be used in the event of an upgrade failure. The dual partition system reduces downtime in the event of an upgrade failure by rolling back the Rubrik node to the pre-upgrade status.

Once the Rubrik platform is upgraded, Rubrik software clients will automatically and non-disruptively upgrade themselves upon next contact with RSC. So there is nothing the admins need to do when upgrades are competed removing the need for manual agent upgrades which is a common behaviour of legacy backup solutions.

3- The Rubrik solution is centrally managed through the Rubrik console and is highly intuitive. Expectations based on what Rubrik will be offering/delivering, you can expect an operator to be competent within 1 week.

4- Rubrik offers various training and certification programs to help enable individuals effectively deploy, operate, and troubleshoot Rubrik solutions.

Training includes a combination of online courses, hands-on labs, and assessments to validate knowledge and skills.

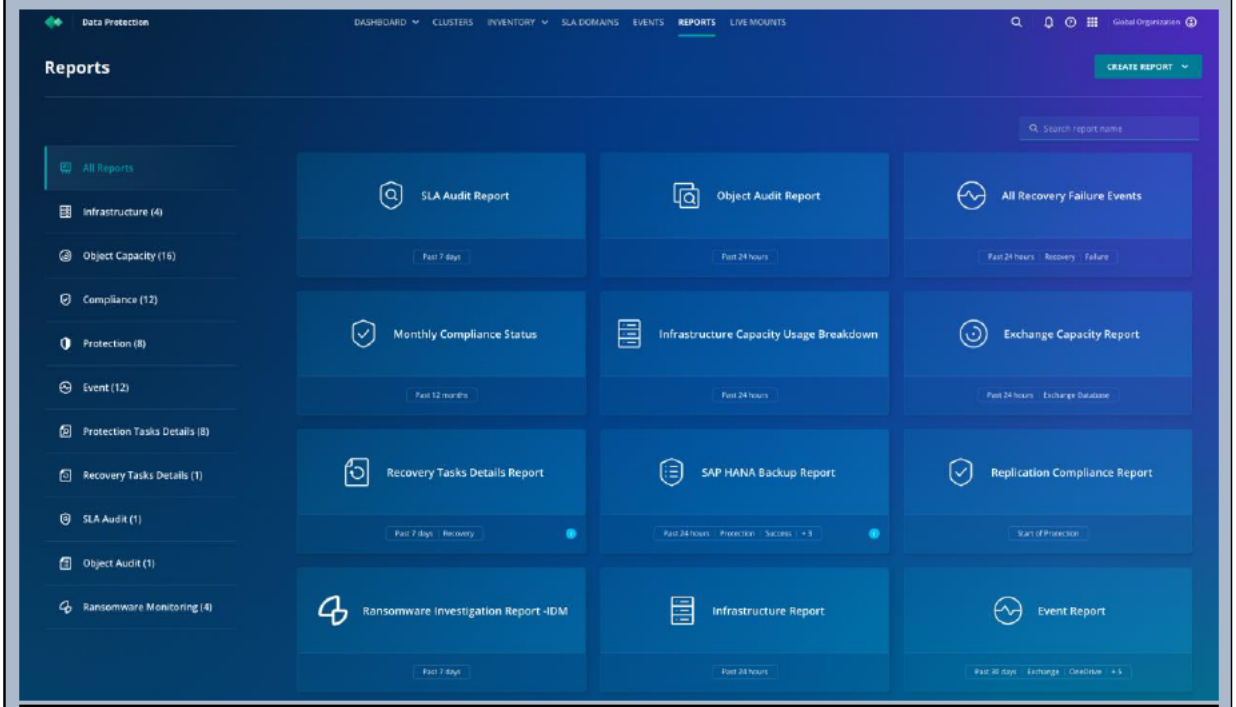
As part of the engagement Rubrik will also deliver a knowledge transfer during project completion and can also include official training as well as access to the Rubrik university.

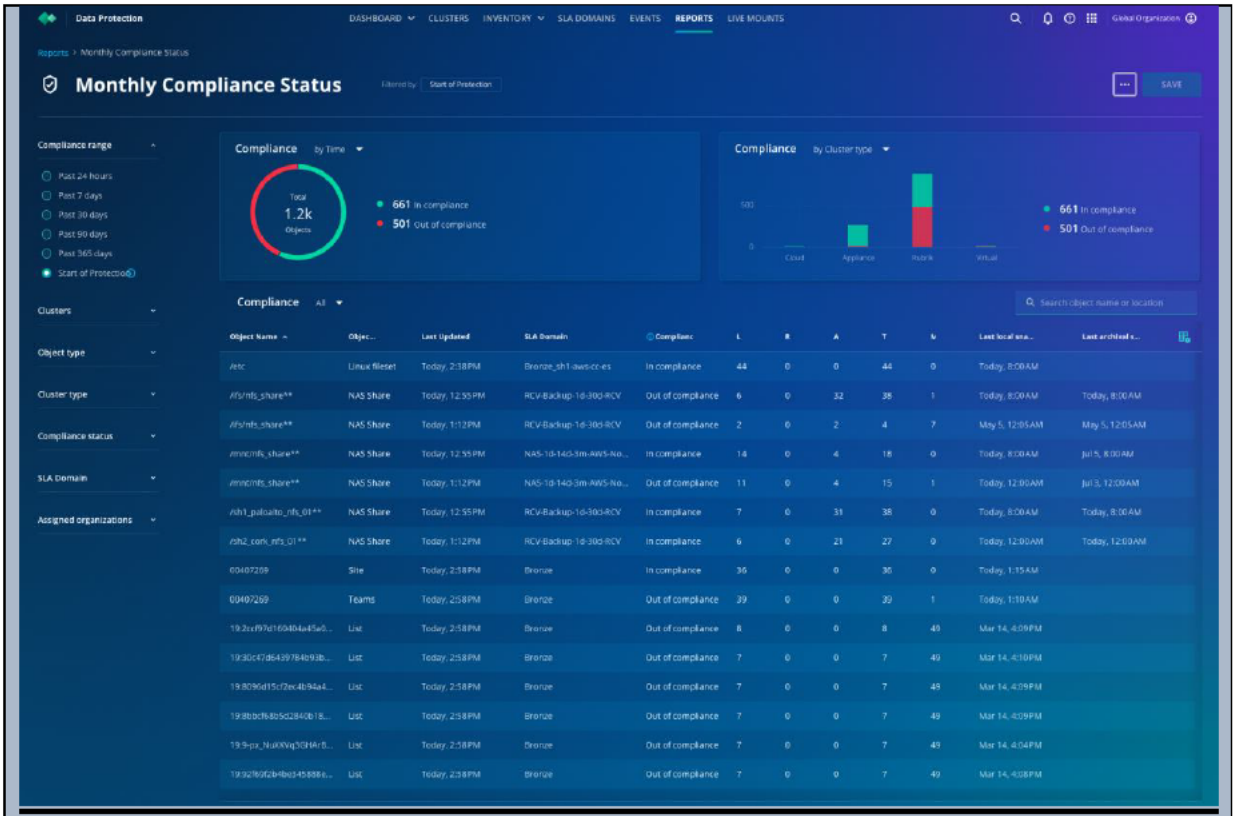
5- Rubrik includes a variety of pre-built dashboards and report templates optimised by use case, such as capacity growth, SLA compliance, and protection status. Administrators can drill-down for granular metrics across application, time, location, status, etc. Views can be filtered and applied to multiple data sources. Export and schedule them as needed. We simplify building custom reports using the report template wizard.

The key dashboards for backup status are:

- Monitoring, which provides detailed information on
  - Jobs in Progress
  - Failed Jobs
  - Cancelled Jobs
  - Completed Jobs
  - Scheduled Jobs
- Compliance, which provides detailed information on
  - Total Protected Objects
  - Objects In Compliance
  - Objects Out of Compliance

For global reporting across all on-premises, edge and cloud-native workloads, RSC provides a unified management and reporting portal. Events, Alerts and Logs are provided on dynamic dashboards which provide fast access to required information coupled with the ability to dynamically filter and/or download in other formats as required.





All reporting data can also be easily integrated to other reporting systems via Rubrik RESTful API, with pre-built integrations already available out of the box for tools such as Splunk and ServiceNow.

6- Automated backups can be achieved in a number of ways with Rubrik. As part of the SLA domains referenced earlier, Rubrik automatically discovers any new workloads that get added i.e., vCenter, SQL, Oracle. As a new workload is added, Rubrik will poll the host and identify the new source. You can Apply an SLA to any level within the hierarchy of a system, for example,

DataCenter → Cluster → Host → VM

You can apply a catch all SLA at the Cluster level, and then any VM that is created in that cluster will automatically inherit the same SLA, ensuring it is protected automatically. If you want to apply a different SLA, you can apply a direct SLA to the VM or DB.

Rubrik delivers an API first platform. Everything that is available in the UI is available via our API. Rubrik has comprehensive and native Rest-based and Graph API support.

Rubrik's native APIs allows automation of data management services such as initiating on-demand backups, applying SLA's, automating recovery plans etc. with granular control. Rubrik is built on an API-first architecture and consumes the same APIs that are published to users.

SDKs are available (Terraform, Puppet etc.)

7- The Rubrik Backup Service (RBS) provides enhanced integration with protected resources and host systems. The RBS software can be downloaded directly from the Rubrik cluster, or the software can be downloaded once and pushed to hosts as needed. Providing software directly from the Rubrik cluster enables the Rubrik

cluster and a hosted deployment of the RBS to reliably authenticate to each other. Rubrik provides automatic upgrade of the RBS software as part of a general upgrade of the Rubrik platform as described in this document. After upgrading the Rubrik version, the Rubrik cluster automatically upgrades the RBS software at the next backup of a protected ------- EXCEEDED WORD COUNT -1 WORDS HAVE BEEN REMOVED

Marking Scheme:	
The following Marking Scheme will be used to assess the response provided to this question:	
0	Not demonstrated
1	Minimal Demonstration
2	Moderate Demonstration
3	Acceptable Demonstration (Minimum Score the Potential Provider must achieve)
4	Good Demonstration
5	Strong Demonstration
6	Outstanding Demonstration

Q4.6. Licencing of the replacement backup solution
How does the Potential Providers proposed Replacement Backup solution provide the Authority with a cost effective solution?
Guidance:
1. You shall describe how the proposed licencing/cost model for the Replacement Backup solution assists the Authority in that aim *As the implementation of the Replacement Backup solution will be performed by the Authority there will be a gap between the procurement of the required software and hardware and its entry into usage by the Authority.* 2. You shall explain how you will work with the Authority to communicate progress during this time before entering into live service.
Rubrik provides the Home Office (HO) with a cost effective solution due to a number of reasons: Rubrik offers predictable Support and Subscription renewal costs. This means that the HO can comfortably enter a 3-year agreement with Rubrik, without any concern of large price hikes in years 4 and 5. Predictability beyond an initial 3-year agreement can be achieved by including the option for an additional term at no uplift in cost. **Portable Licensing** Rubrik has a simple "data under management" pricing model, where a single **$ per usable BETB/FETB** metric is used across all licensing components. Based upon the stated requirements within the pricing model (Appendix D) Rubrik has included a total of: • 300 TB of Foundation Edition • 477 TB NAS Cloud Direct • 3,300 TB of M365 (66,000 units at 50Gb each) • 337 TB of UCL (Universal Cloud License) In the future, as the Home Office migrates on-premise workloads to Cloud-Native (AWS, Azure, GCP), licensing can be ported across without the requirement of purchasing additional licensing. As Cloud-Native uses storage within the same snapshot management

as the same platform, as well as cloud storage for retention, a choice of frequency, replication and retention is defined by the assigned SLA Domain policy, and can cater for cross-region or cross-cloud replication dependant on configuration. Not only is this approach infinitely scalable to meet growth demands, but also will scale down when utilisation is reduced, in turn reducing the cost to the Home Office.

Phased Licensing with Volume Discounting Applied

We are conscious of the fact that the Home Office will not deploy all of the software on Day 1. As such, our pricing reflects the intended deployment schedule as outlined with Appendix D - pricing model.

However, to provide the Home Office with the best value for money, the volume discount for the overall software requirement has been applied and will be available from Day 1.

Reduced Backup and Security Administration Effort

Rubrik customers report a **95% reduction** in administrative effort to backup, secure and maintain systems. This gives HO Engineers and Help Desk staff time back to focus on higher value activities which help advance the organisation.

Rubrik is known within the data protection market for being a true innovator in terms of modernisation, automation and simplicity. Rubrik's architecture is a complete overhaul to the traditional legacy backup and data management platforms with significant siloed infrastructure requirements, software and configuration complexities, and inherent lack of security to deal with today's threats of cyber-attacks and ransomware.

Rubrik provides a **single unified platform** to manage the entirety of the data management across HO's systems and applications, wherever they are situated (on-premises/cloud-native/SaaS). Rubrik's approach is focussed on removing all complexities within the traditional approach to manage data and infrastructure and replacing it with a 'consume it' style data management fabric that automates tasks and manages itself in the most effective way possible. The focus can then be shifted to the important elements within the organisations such as systems and applications, and their respective SLA within the business.

The Rubrik platform consolidates many of the functions of a traditional backup infrastructure such as proxies, catalogue, search, command/control, dedicated backup storage array(s), reporting and monitoring which is consumed as a single software fabric. This means that configuration and management is dramatically simplified using the native HTML5 and REST API interfaces.

Rubrik's Security Cloud automates HO's entire data management environment, with a policy driven Set-and-forget approach to protecting all the systems and services within the HO. With this automation, HO will reduce operational administration significantly, removing reliance for individualised and bespoke roles focussed on backup and data protection, and allow for a shared responsibility across all the team providing greater function resiliency and

allowing the time traditionally spent to be reinvested into innovation and other areas of focus across the HO.

For simplicity, the SLA Domain policy concept is the key concept that is required to be learnt by HO staff, as this defines the schedule, frequency, location of data, and retention of an object, and Rubrik will then automate all the data management services required to adhere to the SLA Domain Policy. If the HO standardises on a single set of policies (e.g., the frequency and retention specified in C7), that single policy can be applied to all objects within HO's environment, and can be locked with Retention Lock, so this cannot be changed. This combined with assigning policies at the highest level, means that objects already assigned will follow the automation provided by Rubrik, with zero administrative effort to perform this data movement, and newly created objects will automatically inherit the top-level SLA Domain, with zero administrative effort from HO teams to 'assign a policy'.

Once the platform, policies and objects have been assigned, with our set-and-forget approach the only reason HO's IT teams would be required to log into the platform would be to perform one of the following tasks:

1. Perform a Recovery
2. Generate Ad-hoc Reports
3. Other miscellaneous system administration

This approach has allowed Rubrik customers to reduce their time spent on backup by up to **95%**.

Archiving

As outlined throughout the response, Rubrik offers a cost effective data management mechanism through Archiving. Due to Rubrik's metadata indexing, the platform (through a defined SLA) can automatically archive data to low-cost, long-term storage in the cloud – without compromising the ability to rapidly recover (RTO Near-0). This aligns directly to the HO key operating model theme of redued TCO.

Cost vs Risk Avoidance

Rubrik guarantees the protection and fast recovery of data, therefore when considering the balance of cost vs risk, our Platform offers significant value when considering return on investment, especially if the HO were to be targeted with a Ransomware attack. To support this, Rubrik offers the HO with a ransomware recovery warranty of $10m. The ransomware recovery warranty covers the expenses related to the recovery and restoration of data protected by Rubrik in the event that data cannot be recovered following a ransomware attack.

By means of illustration, using the Hiscox assessment suggests that if the HO were hit with a Ransomware attack the financial impact could be up to £398.4 Million. The Hiscox calculator makes assumptions about your Sector, geographic location and revenue. Customisable inputs which match your organisation's capabilities can be compared to your Sector's standard and UAL understand better where improvements can be made. The calculation was based upon a DEL of £13.7 Billion (as stated for 2021/22) and a Threat profile of significantly above average.

Your estimated cyber exposure value

£398.4 M

Breakdown of your cyber exposure

We have defined four distinct loss categories that cover the major potential forms of cyber misuse.

Type of Cyber exposure

Business interruption
Costs incurred due to business and/or IT systems being unavailable (e.g. a ransomware attack encrypting all computer systems)

Personally identifiable information
Costs incurred due to exposure of information that can distinguish or is linked to an individual (e.g. name, health/employment/financial info, etc.)

Intangible assets
Costs associated with theft of resources that bring value to an organisation and are not physical in nature (e.g. licenses, copyrights, patents, trademarks, etc.)

Financial loss
Direct or indirect costs resulting in financial fraud, claims, fines, additional reporting, etc.

As the implementation of the Replacement Backup solution will be performed by the Authority there will be a gap between the procurement of the required software and hardware and its entry into usage by the Authority.

Currently, the lead times for the proposed hardware is 2-4 weeks (this is subject to change and should be reviewed at the time of placing an order).

The Rubrik Professional Services team & Softcat will work side by side with the HO delivery team to communicate progress against the project plan. In addition, the Softcat & Rubrik account managers will ensure that any commercial orders are expedited e.g., hardware delivery

Marking Scheme:

The following Marking Scheme will be used to assess the response provided to this question:

0	Not demonstrated
1	Minimal Demonstration
2	Moderate Demonstration
3	Acceptable Demonstration (Minimum Score the Potential Provider must achieve)
4	Good Demonstration
5	Strong Demonstration
6	Outstanding Demonstration

Q4.7. Commitment to backup and recoverability

How does the Potential Provider Replacement Backup solution provide the Authority with confidence in the operation of their backups?

Guidance:

The Authority places importance on the success of backup and restore operations

1. State the percentage of initial success your product achieves on workloads of a type similar to those presented in the supplied workload detail.
2. Explain which factors influence the success of backup and restore operations in your solution
3. Explain how the elements of your solution are maintained and what work is required to implement updates to the solution.
4. Include details of any downtime or further impact to the operation of backups during upgrade activities.
5. Does the Potential Provider solution offer any facility to test the restorability of the backups within the solution to ensure the recoverability of successful backups. Indicate whether such functionality is done autonomously or if Authority interaction is required.

1- Rubrik is dedicated to delivering a backup and security platform that achieves all requirements of the customer. All platforms deployed will meet with a 100% success of workload protection based on what has been scoped and agreed upon before project completion sign off.

If a Backup fails or is interrupted, the automated task manager 'quicksilver' will automatically retry

Rubrik has 5,000+ global customers across 3 regions, 57 countries and 22 industries. This includes over 150 UK Public Sector organisations, including other central government departments & agencies. Collectively Rubrik has been entrusted to protect 28 Exabytes of customer data.

One of these customers with similar workloads and in a similar industry, is the DWP (Department of Work and Pensions). The DWP have been a customer for almost 4 years and are still growing as we onboard new workloads and support their cloud adoption strategy.

2- Simply put, a successful backup will require network connectivity to the backup source, adequate time to ingest the backup and a source target that is not short on resources. Rubrik will automatically check for resource utilisation on the backup source, such as CPU load, disk latency and datastore latency (for virtual) before initiating backups. If thresholds are exceeded Rubrik automatically re-aligns and re-tries, but eventually warns the administrator if a successful backup is not possible due to the source being over the limits all the time. This functionality ("Adaptive Backup") is optional to use. Other limits within the system (e.g., maximum of simultaneous parallel streams per source) make sure that production is not overloaded by the automatic scheduler of Rubrik.

Once a successful backup has been completed, alerting can allow you to have visibility of successful or failed jobs, recovery of the backup can be activated. Rubrik delivers various methods of recovery based upon the workload we are recovering.

Factors to take into account to assure a successful recovery are;

Access to the interface

A successful backup

The Rubrik management platform is managed by the Rubrik Security Cloud, which is a SaaS based UI. This simplifies management as well as consolidating functionality such as

ransomware detection and investigation and sensitive data discovery under one roof. If for whatever reason connectivity was lost to the RSC, it would still be able to be managed via local CDM interface which forms part of the Rubrik distributed, web-scale architecture. All nodes in the cluster have the ability to run the local management interface so this is not a risk.

3- It's important to note, the Rubrik platform is protected by Rubrik Support services. This allows you access to the Service reliability engineers who will help and support The HO with any issues that might arise from normal BAU operations as well as with hardware or software issues. Additionally access to extra personnel aid in the ongoing maintenance of the Rubrik solution. The flexible options we offer here are as below.

Premium & P-Plus Add-On Support Offerings

	Premium Support	Premium-Plus Support Services		
		Customer Experience Specialist (CES)	Customer Experience Manager (CEM)	CEM + ASE Assigned Support Engineer (PAC)
		SMB	Med/Large Accts	Large Accts
Phone/Email/Web Access to Support	✓	✓	✓	✓
Enterprise SLA	✓	✓	✓	✓
Product Updates & Fixes	✓	✓	✓	✓
Post-Sales Relationship Manager		✓	✓	✓
QBRs and Regular Syncs on Support Efforts, RFEs, Defects		✓	✓	✓
Qualification for Rubrik Ransomware Warranty Program			✓	✓
Global Account Coverage (24x7 when required)			✓	✓
Technical Environment Intimacy				✓
Prioritized Case Handling				✓

White Glove Support Through the Entire Customer Lifecycle

	Onboard	Adopt	Expand	Renew
Customer Experience Manager **Customer Experience Specialist**	• Accelerate product adoption, time to value, and product comfort via structured onboarding sessions. • Coordinate the implementation of Security Hardening and other product Best Practices • Understand, Align-with, and Drive Customer's Goals and Business Objectives	• Own the Customer Life Cycle & Account Management, build a Relationship of Trust & Transparency • Conduct collaborative strategic planning to achieve customer business outcomes via weekly scheduled calls, product roadmap reviews, QBRs, health checks • Proactively monitor feature adoption, identify pain points and expansion opportunities to drive upsell/cross-sell • Post Sales Relationship Manager - Escalation Management, Case Monitoring & Reviews	• Ensure optimal performance while minimizing risks. • Accelerate time to proficiency of additional deployment as needed • Assist sales with renewals, usage analytics and relationship management	
Customer Experience Specialist		• Reduced frequency of touch points with the customer (Monthly) • Coverage during Customer's Local Business Hours • Cannot qualify the account for Ransomware Recovery Warranty		
Assigned Support Engineer	• Develop intimate knowledge of the customer's environment and workloads • Oversee the Technical Support cases and drive critical issues to resolution. • Work closely with CEM to Jointly develop & report on success plans, proactively impart best practices, drive time to value, conduct technical training, and assist with feature enhancements			

rubrik

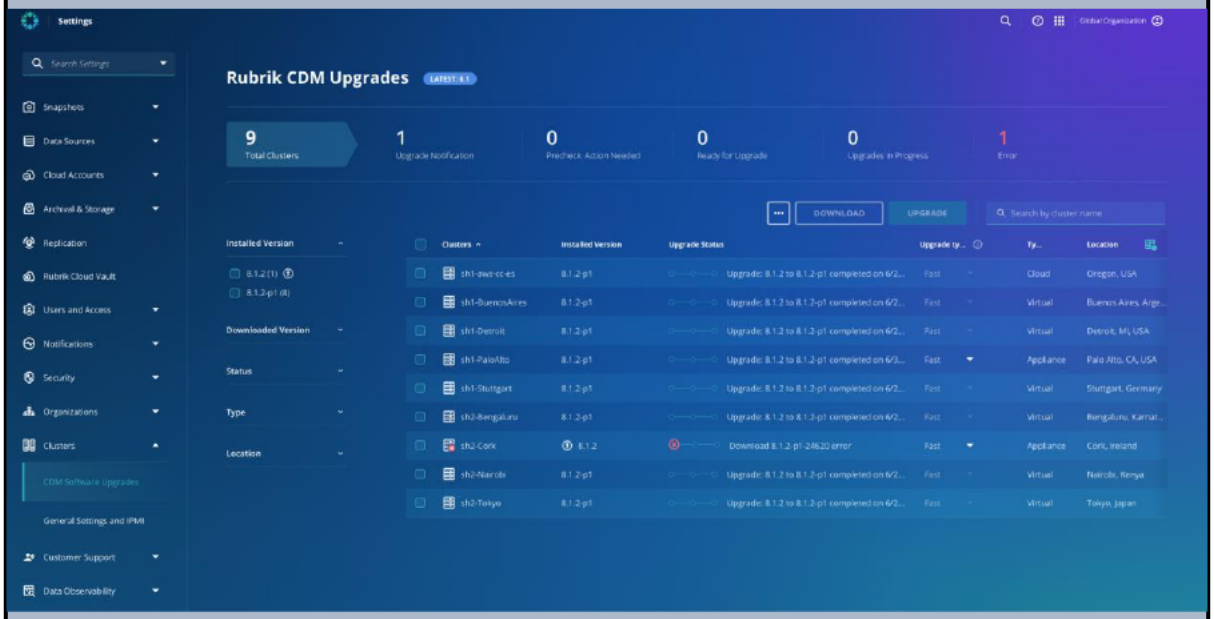
Ongoing upkeep for the platform is very low maintenance. The Rubrik solution is very simple to upgrade. The SaaS based management interface is automatically maintained and upgraded by Rubrik. For on premises equipment/software, there is one update for the system. Administrators do not have to patch hardware, OS and software individually and don't have to worry about potential version conflicts between each layer. The Rubrik Backup Service, where needed, gets upgraded automatically when the system is upgraded, and no reboots are required. This ensures that no administrative time is used to keep client systems up to date.

As per the below, you can see the platform will alert you to when an upgrade is available. This is accessible from the settings section, Clusters, Upgrade. Once an upgrade is initiated the process applies the upgrade to all nodes of a Rubrik cluster in a single operation.

The upgrade process uses a dual partition methodology to upgrade Rubrik. With dual-partition upgrades, the new software is provisioned in the second partition. The first partition retains the original Rubrik CDM files and can be used in the event of an upgrade failure. The dual partition system reduces downtime in the event of an upgrade failure by rolling back the Rubrik CDM node to the pre-upgrade status.

Dual partition upgrades also allow the upgrade process to resume easily after an initial failure.

This operates in a rolling fashion with zero downtime.



4- Due to the distributed nature of the Rubrik web scale software, there is no reason to incur any downtime when running upgrades. It's important to note that any backup or recovery operations that are happening will continue as the task will be passed to another node to complete.

5- There are two aspects to explore when talking about testing the recoverability of backup data:

1) Data Integrity of data transferred and stored during backup

2) Verifying data/backups stored are recoverable

Data Integrity is core to the Rubrik architecture. Given the various facets of Rubrik and in particular the way that Rubrik is used as the "storage of last resort" for backup and recovery, there are multiple methods to ensure data integrity — all of which are transparent to our customers.

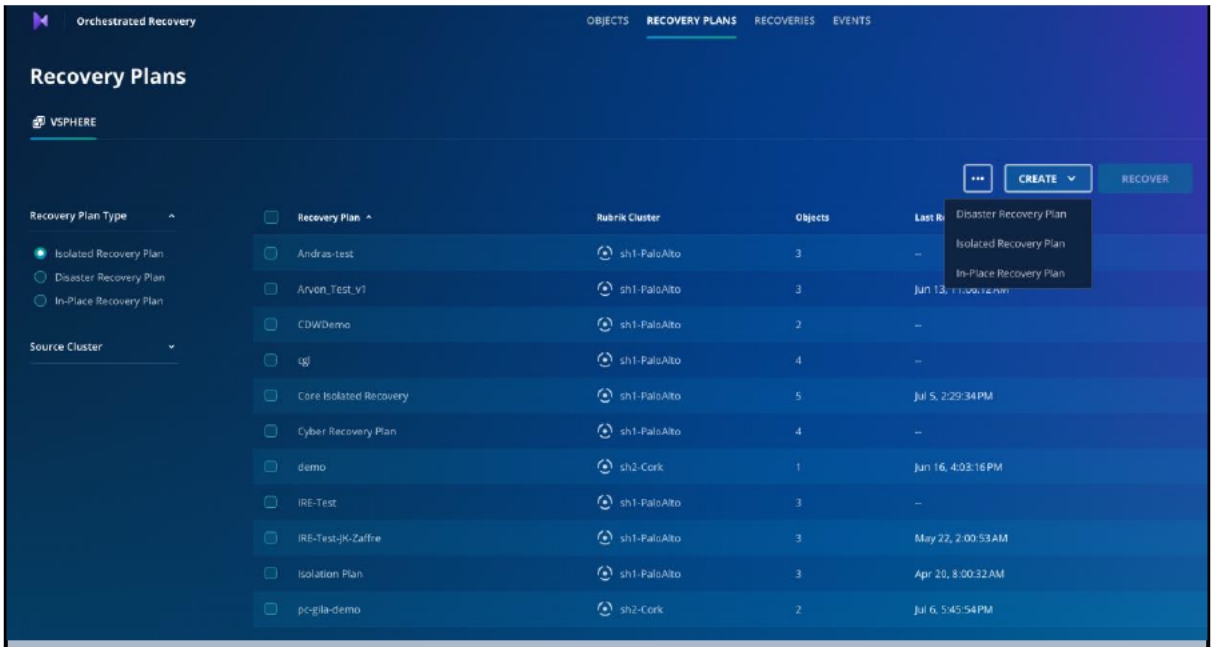
Rubrik is engineered to be a self-healing software system that is resilient to multiple node and disk failures as well as chassis failure at scale. Data ingest and management tasks – backup, replication, archival, reporting, etc. are distributed throughout the cluster. Each node within the cluster acts autonomously as it executes its task assignments. Any data management platform requires multiple lines of defence to ensure data integrity. From end-to-end continuous checks for data and metadata to a self-healing software system that weathers node/disk failure to an architecture that minimises dependence on hardware, Rubrik utilises a multifaceted system of checks to validate the accuracy and consistency of data throughout its lifecycle. As a next-generation solution designed to support data management across multiple locations, Rubrik ensures data integrity even when data is stored in the public cloud and data recoverability even when local data is destroyed or corrupted.

For testing, Rubrik recommends using Live mounts. Rubrik live mount enables the ability to easily and instantly recover from any snapshot backup, with just a few mouse clicks and without having to transfer data over the wire by utilising Rubrik's own storage.

This feature will bring up a selected recovery point in parallel with your live environment for a quick test, confirmation, or more extensive functionality test, and then finally a tear down without having to allocate any additional storage.

A further differentiator is the performance Rubrik is able to obtain during the live mount process. Not only is the live mount near instantaneous but the live mounted volume, VM or application is hot locked into the Rubrik flash tier. This enables Rubrik to provide near to production performance on live mounted applications, VMs, DB's etc.

Rubrik also delivers orchestrated recovery of applications, workloads or services. Recovery Plans manage recovery specifications for three types of recovery: disaster recovery, isolated recovery, and in-place recovery.



Rubrik's Orchestrated Recovery solution is a powerful feature that enables The HO to streamline and automate the recovery of their critical applications and systems. This functionality, including the creation of recovery plans, testing and failover activities, as well as detailed reporting are fully built into RSC; no separate interface required.

With Orchestrated Recovery, Rubrik simplifies the complex task of recovering multi-tier applications by automating the sequence and dependencies of the recovery steps (i.e., what order should systems come online, what host and datastore to fail over to, what IP should be assigned, any post failover scripts that need to run, etc...). The HO can define recovery workflows, specifying the order in which different application components should be restored and the dependencies among them. This allows for consistent and reliable recoveries, reducing the risk of errors and ensuring a faster recovery time.

Rubrik Orchestrated Recovery not only allows for Disaster Recovery, but this same technology can be used to create Isolated Recovery Environments (IREs) on the fly. This capability gives The HO the ability to quickly and seamlessly test their Cyber Recovery Readiness and report on it to the business.

Orchestrated Recovery integrates with Rubrik's other data management features, such as backup, replication, and snapshot technologies. This enables seamless transitions between backup and recovery operations, providing a unified experience for data protection and recovery.

Furthermore, Orchestrated Recovery supports different recovery options, including full restores, granular file-level recoveries, and application-consistent recoveries. The HO has the flexibility to choose the most suitable recovery method based on their specific needs.

You can optionally configure a post-failover script when you create a Recovery Plan. Post-failover scripts can be used to perform custom activities such as automated testing, DB consistency check etc.

A sample report of an application test recovery to an isolated environment.

rubrik

IRE-Test_2023-06-20_001

Recovery Plan: **IRE-Test**

Recovery Overview

Success
Outcome
Recovered **3 virtual machines** via live mount

00:23:44
Recovery Time
Started on 06/20/2023 10:29:05 AM
Ended on 06/20/2023 11:02:34 AM

0
Errors Occurred

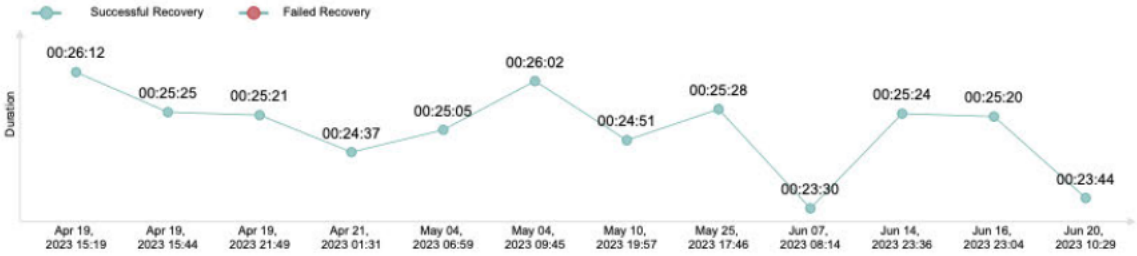
Recovery History

You've completed 15 isolated recoveries using the IRE-Test recovery plan.

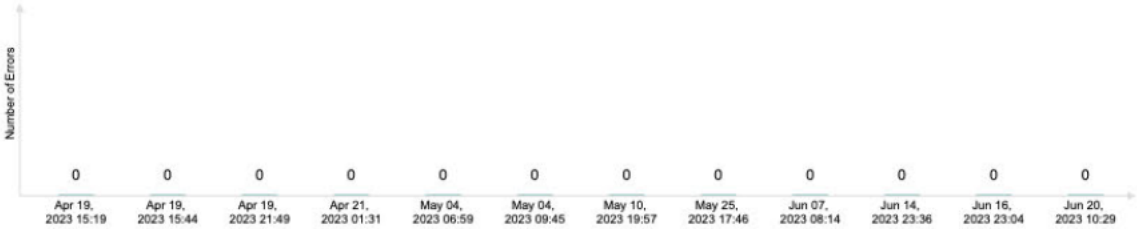
100.00% Success Rate
15 out of 15 recoveries succeeded

20 min, 07 s
average duration of successful recoveries

Trend in Recovery Duration (Last 12 Recoveries)



Trend in Number of Errors (Last 12 Recoveries)



Objects

Object	Immutable Snapshot	Recovery Outcome	Post-Recovery Script
sh1-haverford-db-01	06/20/2023 8:04:41 AM	Success	Not Available
sh1-haverford-fs-01	06/20/2023 8:07:19 AM	Success	Not Available
sh1-haverford-webapp-01	06/20/2023 8:18:09 AM	Success	Not Available

Target Resources

Compute Resource: sh1-paloalto-vcsa.rubrikdemo.com/sh1-PaloAlto Datacenter/sh1-PaloAlto Cluster
Target Networks: LabLan, LabLan, LabLan,
Network Preservation: Preserve entire network settings

Marking Scheme:
The following Marking Scheme will be used to assess the response provided to this question:

0	Not demonstrated
1	Minimal Demonstration
2	Moderate Demonstration
3	Acceptable Demonstration (Minimum Score the Potential Provider must achieve)
4	Good Demonstration
5	Strong Demonstration
6	Outstanding Demonstration

© Crown copyright 2020

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.