Request for Proposals

Enterprise Backup, Recovery & Disaster Recovery Solution

Questions and Answers

This document consolidates the vendor questions submitted for the ARC Backup, Recovery & Disaster Recovery (BRDR) RFP. The original compilation contained roughly 140 individual entries; duplicate and near-duplicate questions from different contributors have been merged into a single question, organized by topic. The consolidated list below contains 91 distinct questions across 17 topic areas.

1. Proposal Process & Timing

1. Are the Professional Services items described on RFP page 8 (e.g., Discovery and Assessment) requirements before award — with findings included in the proposal response — or after award, to finalize the full scope and implementation plan?

   The RFP provides initial sizing information for inclusion in the proposed solution. The discovery and assessment step is intended to occur following award to address any potential changes to the environment since RFP posting and to confirm that the proposed solution remains the best fit.

2. Environment Sizing & Scope Discrepancies

2. Appendix A lists 47 virtualized servers (~55 TB on-prem) plus a 95 TB cloud-hosted SMB share, while the Scope of Work references a broader range of 50–70 VMs across 50–200 TB of usable data. Which figures are authoritative for sizing — are the ranges overlapping or separate — and should proposals be priced to the upper bound of the Scope of Work range or to the Appendix A figures (~47 VMs / ~177 TB)?

   The current workload consists of 47 virtualized servers. The 50-70 virtual machine figure is provided as a range the selected provider should be able to fulfill to accommodate potential future compute requirements either in on-premises virtualization or through cloud services. Similarly, the 50-200 TB figure is provided as a potential requirement across current and future block storage requirements for all potential workloads. The 95 TB hosted in cloud is distinctly separate from the virtual environment and consists primarily of SMB file shares.

3. The Scope of Work states that additional cloud workloads and databases will be defined during discovery. Please provide the current number and size of these workloads and databases, or state what vendors should assume for initial pricing.

   The RFP provides initial sizing information for inclusion in the proposed solution. The discovery process is intended to address any potential changes for the environment following RFP posting and to confirm no adjustments are required for the proposed solution. No changes are currently anticipated from the previously provided information.

4. Is this a single-site environment or are there multiple ARC physical locations each needing on-prem backup infrastructure?

   This is a single site environment.

5. How many years should the solution be sized for, and what is the expected annual data growth rate and approximate daily change rate?

As listed in the RFP, the solution should be sized for baseline of 3 years with a potential of up to 5 years. The solution should assume a growth rate of 3% yearly.

3. Current Infrastructure & Storage Platforms

6. What is the current primary storage platform supporting the virtualized infrastructure and physical servers (asked to confirm the solution will fully support hardware snapshot management as required)?

   The virtualized environment is operating on a TrueNAS M40 storage appliance by iX Systems.

7. Are the "6 virtual hosts" listed in Appendix A the physical hypervisor servers hosting the 47 VMs, or are they themselves VMs already counted in the 47 total? What hypervisor/OS do they run (VMware vSphere, Hyper-V, or both), and how many VMs run on each platform? Should they be licensed/protected as separate nodes?

   The 6 virtual hosts are the physical hypervisors operating VMware ESXi. The selected solution should support migration onto alternate hypervisors with the appropriate licensing requirements.

8. Are dedicated backup networks, VLANs, or Fiber Channel connections currently available, and is there a Gbit LAN infrastructure in place?

   A separate backup VLAN is available with Gbit LAN connectivity.

9. What network connectivity is available between the primary environment and the cloud/DR location — is the 10GbE connection dedicated to backup/replication traffic, or shared with production?

   The current DR replication is conducted over a shared 10GbE circuit. However, submissions should include a forward-looking best practices approach to the solution for reliability, security, and ease of operation. Therefore, solutions may or may not include the current operational configuration.

10. Does ARC prefer backup-management components to run physically, virtually, or is either acceptable?

    Either is acceptable.

4. Cloud Workloads, SaaS & Databases

11. Approximately how many cloud-hosted compute instances/VMs and workloads exist in AWS and Azure, what is their combined data volume (separate from the 95 TB SMB share), and are there additional cloud, database, or SaaS workloads that should be considered?

    ARC currently has less than 10 cloud-hosted compute instances active. Two instances of PostgreSQL are deployed as cloud hosted databases. The combined data volume of these instances is less than 5 TB.

12. Are cloud-native managed databases (e.g., RDS, Azure SQL) in scope for protection, and what versions of Microsoft SQL Server and PostgreSQL are currently deployed?

    To support future systems development, the selected platform should support both Microsoft SQL server and PostgreSQL. Two instances of PostgreSQL are currently deployed and operating at version 16.

13. Does ARC currently maintain AWS GovCloud, Azure Government, or commercial cloud accounts?

ARC currently maintains AWS commercial and Microsoft GCC.

14. Can ARC provide a current list of SaaS applications beyond Microsoft 365 (e.g., Salesforce, ServiceNow, Dynamics 365, or anything beyond Exchange Online/SharePoint Online/OneDrive for Business/Teams) that may require backup coverage, and should such coverage be priced as a per-application add-on or included in the base proposal?

    At this time, no other SaaS applications are within scope.

15. How do you protect SaaS applications today, which SaaS platforms are business-critical, and what are the recovery expectations for them?

    ARC is seeking to implement a best practices approach for data protection across all systems and platforms. Therefore, proposal submissions should demonstrate the capabilities of the solution and potential recovery objectives above that of any current methodology.

16. How many Microsoft 365 users require protection, and which M365 services and approximate data volumes are in scope?

    ARC maintains 280 licenses for M365. All M365 services and data are within scope.

5. The 95 TB Cloud-Hosted SMB Share

17. Is the 95 TB cloud-hosted SMB share fully in scope for backup/recovery under this contract, or is it managed separately — and where/on what platform is it currently hosted (e.g., Azure Files)?

    Proposals should be inclusive of protection options for the SMB shares hosted on cloud. Hosting of these shares is currently maintained on AWS. However, the selected platform should support alternate locations should migration be necessary for any portion of the object storage based shares as noted.

18. What is the required protection method, RTO/RPO tier, and retention period for the 95 TB SMB share — does the 90-day minimum retention requirement apply specifically to this dataset?

    The 95 TB SMB shares have differing RTO/RPO requirements by data classification, use, and location. Therefore, the proposed solution should provide best practices designs for protection of all object storage data while allowing flexible retention and RTO/RPO objectives by data classification, use, and location.

6. Workload Tiering & RTO/RPO

19. How does ARC classify Tier 1, Tier 2, and Tier 3 workloads, and can ARC provide a workload tiering matrix (or at minimum the approximate number/type of Tier 1 VMs, physical servers, and databases) to allow accurate RTO/RPO architecture design?

    ARC classifies Tier 1 applications as workloads critical to the overall operation of the agency IT environment. Tiers 2 and 3 are applications which are important but do not necessarily carry operational dependencies. There are currently ten (10) Tier 1, eight (8) Tier 2, and fifteen (15) Tier 3 applications. All listed are virtual machines.

20. What is the front-end data size of the Tier 1 workloads, and are they running on VMware, Hyper-V, physical servers, or cloud platforms?

Each is currently operating on VMware with a front-end data size of approximately 8 TB.

21. Is the sub-5-minute RTO/RPO a strictly binding requirement, or an acceptable target for full marks under the evaluation criterion — and is it intended for every Tier 1 workload or only selected applications?

    The Tier 1 RTO/RPO is a desired target to demonstrate resilience in the agency's ability to rapidly recover from an event.

22. What RTO/RPO targets apply to non-Tier-1 (Tier 2/3) workloads?

    ARC seeks to recover Tier 2 within 4 hours and Tier 3 within 8 hours.

7. Disaster Recovery Site & Replication

23. Does ARC have an existing secondary data center, colocation facility, or DR topology to serve as a DR target, or is cloud-based failover the sole intended DR destination — and if a secondary site exists, what's currently working versus not?

    ARC has no colocation or secondary data center. Proposed solutions should be flexible towards recovery in cloud and failback to on premises, if desired.

24. If a vendor-hosted or vendor-facilitated DR/emergency hosting site is required, are there geographic or data-residency constraints (e.g., within the U.S. or a specific region)?

    ARC's security policies restrict access to locations within the United States and Canada. Subsequently, all sites included in the solution should adhere to this geographic restriction.

25. Is a "warm standby" environment expected for any workload tier, or is recovery from cloud backup copies sufficient for non-Tier-1 systems?

    Recovery from cloud backup is sufficient.

26. Is there a designated or preferred cloud replication target platform, or is this left to vendor recommendation?

    ARC has no preferred designated target. The selected vendor shall provide recommendation.

27. For cloud replication, is the backup/DR application itself expected to perform the replication, or should replication be handled natively by the target cloud platform? Does ARC plan to replicate to a DR site under the proposed solution?

    The backup DR application should provide visibility and management of the replication and recovery processes. This may or may not include native integration with the target platform. Once implemented, ARC plans to replicate to the solution site.

28. The current DR solution is believed to be LTO tape shipped to Iron Mountain — can a secure, isolated cloud vault (AWS or Azure) replace the tape copy for DR, and does ARC still plan to create tapes even if backup-to-disk is implemented?

    ARC has no plans to include tape in any future backup processes. The proposed solution should be a forward-looking best practice solution that is resilient on-premises and cloud enabled with the storage necessary to attain the RTO/RPO performance and immutability requirements.

8. Compliance & Regulatory

Which ISO 27001 Annex A control domains are most relevant/in scope for this engagement and is ARC currently certified or working toward certification?

ARC is not currently seeking certification for ISO 27001. However, ARC does consistently review agency systems and processes to ensure adherence to best practices guidance for security and operational stability. The following controls are relevant to this engagement with relation to ISO 27001 Annex A.

- *Information Security Policies (A.5.1-A.5.2)*
- *Information Classification and Asset Management (A.5.8-A.5.14)*
- *Information Logging and Monitoring (A.8.15-A.8.16)*
- *Network Security and Backup (A.8.7, A.8.14)*

29. Will a NIST SP 800-53 Rev. 5 control mapping be considered sufficient to demonstrate ISO 27001 alignment, given the overlap between the frameworks?

    A control mapping will be sufficient as demonstration of this requirement.

30. For vendors proposing a "path to compliance" for FedRAMP/StateRAMP rather than existing authorization: what minimum evidence will ARC accept (e.g., initiated assessment, designated 3PAO, ATO in process); is there a required timeline for achieving full authorization after award; and will such proposals be scored equivalently to those with existing authorization? Relatedly, does the entire solution need to be FedRAMP-authorized end-to-end (on-prem, SaaS, and cloud) within the single pane of glass?

    Vendors proposing a path to compliance for FedRAMP/StateRAMP should provide the current status and anticipated timeline of attainment. A valid demonstration of path to compliance will be scored similarly to existing authorization. Any portion of the solution not meeting the authorization should be noted in the proposal.

31. Beyond the Area Agency on Aging PHI systems noted in the RFP, are there other in-scope systems/datasets subject to HIPAA or other regulatory data-handling requirements, and which regulations/frameworks (HIPAA, PCI, SOX, NIST, ISO, etc.) drive ARC's data protection needs generally?

    Other areas with PHI/PII include Human Resources and the Workforce Services department.

9. Encryption, Immutability & Identity

32. Are there specific encryption key management requirements for data at rest in cloud storage (e.g., customer-managed keys, HSM, ARC-controlled key custody), and does ARC encrypt or compress backups today?

    Backups are currently compressed. ARC is open to recommendations for cryptographic approaches within the proposed solution.

33. Does ARC require the immutability/dual-authorization model to integrate with a specific identity provider, or a physically separate approval workflow (e.g., a second admin outside the primary AD/Entra ID domain)?

    ARC uses AD/Entra ID integrated with Cisco Duo. The proposed solution should provide ability to integrate with the current identity solutions. The proposed solution should also provide the ability for break glass recoverability in the event the identify provider is impacted. This break glass may require dual authorization for security purposes.

34. Regarding the WORM storage requirement under Core Functional Requirements: will immutable copies of backups satisfy this requirement — i.e., can the initial disk-to-disk backup reside on non-WORM storage with a secondary copy on immutable storage?

    The proposed solution should demonstrate immutability capable of protecting all data while attaining the stated RTO/RPO objectives. Alternate approaches to WORM may be proposed if there is no impact to RTO/RPO achievability and immutability can be demonstrated.

35. What identity, MFA, and privileged-access systems are currently in use, and does ARC use on-premises Active Directory, Entra ID, or both together?

    ARC uses AD/Entra ID integrated with Cisco Duo

10. Current / Incumbent Backup Environment

36. What is ARC's current backup/DR platform and vendor (if any), is this RFP a full replacement or are there components ARC intends to keep, and what are the primary challenges with the current solution?

    The current platform uses Commvault and AWS Elastic Disaster Recovery. ARC seeking proposals for a full replacement which integrates all processes for management, reporting, security, and testing.

37. Is migration of historical backups from the existing platform expected, and is decommissioning of the current backup environment included in the project scope?

    Migration of the current backup is not expected. Similarly, decommissioning of the current backup environment is not included in the project scope.

38. Are existing backup policies, retention schedules, and disaster-recovery runbooks available for vendor review?

    Current policies and schedules are available. However, given that this is a full replacement of the existing environment, ARC would prefer all schedules and policies be setup in the new system according to workload requirement, vendor best practices and current security guidance.

11. Support SLA & Timeline

39. How does ARC define Severity 1/2/3 incidents for purposes of the 24x7x365 support SLA and are there associated response/resolution time commitments vendors should propose against?

    ARC defines incidents according to operational impact as indicated below.

- *Severity 1 (Critical) – Core Business Impact – Target SLA 2-4 hours*
- *Severity 2 (High/Major) – Degradation of Primary Applications – Target SLA 4-12 hours*
- *Severity 3 (Minor) – Minor loss of performance – Target SLA 24-48 hours*

40. Is there a target start date or expected contract execution date, and does ARC have a preferred implementation completion date, fiscal-year constraint, or other upcoming milestones/deadlines?

    The selected vendor should anticipate a start date within 60 days of award. All required hardware and services must be delivered, installed, and complete by December 2026. Additionally, the system must

demonstrate the required performance during this timeframe.

41. Will ARC's IT staff be available for structured discovery sessions within a defined window after award, or should the timeline assume vendor-led discovery with limited ARC staff availability?

    ARC staff will be available to assist with any discovery requirements.

12. Cost & Commercial Terms

42. Exhibit B-1 lists five cost categories (Hardware, Licensing/Support, Cloud Services/Immutable Storage, Onboarding/Training, Implementation) with a single total — should Year 2–5 maintenance/renewal costs be broken out by year within this format, or presented as a separate schedule?

    Costs should be broken out by the requirements for implementation in year 1 and renewal costs in subsequent years 2-3, with option for the optional extension through years 4-5. Due to budgetary requirements, all costs must be annualized as anticipated for the solution.

43. Does ARC have a stated budget range or funding ceiling for this project?

    The financial range for this project are undisclosed to encourage independent cost proposals.

44. Is ARC open to a subscription/consumption-based licensing model in addition to the stated hardware-and-software purchase with annual maintenance structure, or is capital purchase mandatory?

    ARC is open to review of recommendations within the submitted proposal.

45. Are there anticipated data egress or cloud API charges (e.g., for DR testing or failover events) that should be itemized separately from base cloud storage costs, and what are ARC's top cost drivers today (licensing, storage, egress, maintenance)?

    ARC would recommend notation of any egress and API charges for the proposed solution as storage and egress are current cost drivers.

46. Can multiple vendors be awarded portions of this contract (e.g., one for on-premises hardware/software, another for the cloud replication target), or is ARC expecting a single prime vendor for the full solution?

    For contract management reasons, ARC prefers a single prime vendor but is not opposed to joint venture proposals.

13. Proposal Format

47. Given the 20-page proposal limit (excluding product data sheets, budget exhibits, and cover material), do topology diagrams and RTO/RPO workload mapping tables submitted under “Technical Approach” count toward the page limit, or are they treated as excluded product details?

    Submitters should include items such as technical detail or topology diagrams within the proposal appendices as these are excluded from the page limitations.

48. Will ARC accept sub-page or condensed formatting (e.g., tables, appendices) for the required reference list, or should each reference be a full narrative entry within the page count?

Condensed formatting or reference submissions is acceptable.

14. Retention

49. Appendix A states a retention period of 90 days minimum and 6 months desired, while the Scope of Work separately lists daily, weekly, monthly, and yearly retention tiers — please confirm the required retention period for each tier and clarify whether weekly/daily backups should be full or incremental.

    The proposed solution should provide flexibility to review data by day, week, or month as appropriate. The minimum required retention for all system data is 90 days with a desired goal of 6 months as stated. In certain instances, where extended retention may be required, a yearly should be available. ARC is requesting that providers provide recommendations based on best practices and solution capability towards the frequency and type of backup jobs as this may vary by solution type.

50. Does ARC have legal hold, eDiscovery, or long-term retention policies that must be satisfied, and are retention policies expected to be applied consistently across all data types?

    As a publicly funded organization, ARC is subject to legal hold, eDiscovery, and long-term retention requirements. These requirements do not uniformly apply across all data types.

15. Training & Operations

51. How many ARC IT staff need hands-on administrator training and must training happen on-site or is remote training acceptable?

    The training will consist of 6 IT staff. On-site is preferred but may be conducted remotely if on-site is not available.

52. Will ARC administrators operate the solution entirely in-house after implementation?

    The solution will be managed in-house following implementation.

16. Monitoring, Security Integration & Recovery Validation

53. What ITSM and SIEM platforms are currently in use (to validate the REST API/SIEM integration requirement), and should backup/security alerts be sent to a specific SIEM or monitoring platform? Are security operations (SOC) integrated with backup/recovery events and telemetry today?

    ARC maintains an instance of Desk365 as the primary ITSM and Graylog as the primary SIEM. There is no current SOC integration.

54. How do you detect anomalous activity in backup metadata or repositories, and how is backup integrity verified to reduce the risk of restoring compromised data?

    The current platform alerts the ITSM to changes in the backup baseline.

55. Does ARC require recovery playbooks to orchestrate people, process, and technology during recovery efforts?

    Recovery playbooks should be inclusive of all dependencies for a recovery event.

17. General Discovery & Qualifying Questions

56. What prompted you to look at data protection now — a recent incident, audit finding, or upcoming change?

    ARC conducted a review of backup and disaster recovery processes. The findings within the review suggested the current environment be replaced to facilitate a higher degree of resilience and manageability.

57. Which workloads or business services are most critical to protect today, and why?

    The most critical services are those with immediate operational impact on the agency. These include IAM, database, PKI, and financial systems.

58. Do you have an active initiative or budget set aside for backup, recovery, or cyber resilience this quarter?

    Yes. However, the financial range for this project are undisclosed to encourage independent cost proposals.

59. Who else besides IT is involved in decisions on data protection (security, compliance, app owners)?

    ARC's Office of Information Technology works will data owners and departments to oversee and maintain all areas of data protection.

60. What platforms are in scope (virtualization, databases, file/object, Kubernetes, mainframe, endpoints)?

    All areas as listed in the provided inventory including virtual machines, databases, SMB shares, and cloud hosted workloads.

61. Where does your data live today (on prem, cloud, edge), and how fast is that changing?

    As noted in the provided inventory, the bulk of agency data is cloud hosted.

62. Which applications have unique protection needs (mission-critical databases, healthcare/financial systems, AI/analytics)?

    Unique protection requirements remain undisclosed beyond the provided inventory. The specifics of any unique protection scenarios will be provided following award to the selected vendor.

63. How are RPO and RTO targets set today? Are they measured and reported regularly?

    ARC's Office of Information Technology regularly evaluates risk and requirements to establish RPO and RTO targets.

64. Have you experienced backup failures, slow recoveries, or missed SLAs in the last 6–12 months?

    There have been no missed SLAs or backup/recovery failures.

65. What's your plan for large-scale recovery (e.g., recovering hundreds of TBs quickly)?

    The focus of the RFP is implementation of a replacement platform and not on current processes or procedures. ARC is open to recommendations within the proposed solutions for how to best achieve RTO/RPO objectives at scale.

66. Do you test recovery (tabletop or technical) on a schedule? What were the last test outcomes?

    ARC conducts a minimum of two tabletop exercises annually along with technical evaluation of backup and recovery processes. ARC is open to recommendations within the proposed solution for validation of backup, recovery, and DR processes.

67. Have you seen ransomware or destructive attacks impact backups or snapshots?

    No.

68. Do you maintain an isolated/air-gapped copy or vault for clean recovery?

    An isolated copy is currently maintained. The selected vendor shall include isolation in the proposed solution.

69. How do you detect, isolate, and validate data before bringing it back online?

    The focus of the RFP is implementation of a replacement platform and not on current processes or procedures. ARC is open to recommendations within the proposed solution for how to best achieve validation of data prior to recovery.

70. Do you need certified workflows for incident response and clean-room recovery?

    As noted in the RFP, the selected vendor should anticipate providing validated playbook/runbooks scoped for the proposed solution for all workflows involving a recovery event.

71. What's your approach to protecting cloud workloads (IaaS, PaaS, containers)?

    The proposed solution should provide flexibility to protect cloud workloads.

72. How do you manage cost and performance for cloud backups and long-term retention?

    ARC continually evaluates cloud spend and retention requirements to balance operational needs and available budget.

73. Do you move data between on prem and cloud for DR, archival, or analytics?

    Yes. As noted, ARC currently replicates on prem systems to cloud for DR.

74. Are there regions or sovereign requirements affecting where protected data can reside?

    ARC's security policies restrict access to locations within the United States and Canada. Subsequently, all sites included in the solution should adhere to this geographic restriction.

75. How are audit trails and evidence of compliance produced today?

    The focus of the current RFP is not on current processes or procedures. ARC is open to recommendations within the proposed solutions for auditing and compliance reporting.

76. Where are you seeing gaps in governance or policy enforcement?

The majority of gaps consist of system limitations for the current backup environment. The proposed solution should demonstrate a best practices approach toward governance and policy enforcement.

77. How many people manage backup/recovery day to day, and what are the pain points?

Three people manage the current process. Current pain points include manual interaction requirements, LTO management, and platform limitations.

78. Which tasks consume the most time (policy management, agents, upgrades, troubleshooting)?

Tasks which consume a higher degree of time include management, troubleshooting, and software updates.

79. Do you need as-a-service models, managed services, or automation to reduce overhead?

As listed in the RFP, ARC is not seeking managed services as part of this engagement.

80. What metrics or dashboards do leadership care about (success rates, time to recover, risk posture)?

The dashboard of a backup, recovery, and disaster recovery system should not be limited to executive metrics. All performance metrics are important towards providing confidence in the reliability, dependability, and risk reduction capabilities of the solution.

81. Are you considering a pilot or POC for a specific workload or recovery scenario?

The RFP is for implementation of a comprehensive solution. While a pilot or POC may be suggested as part of the proposal, the submission should focus on the goal of implementation and performance demonstration of the complete solution by end of calendar year.

82. What would make a solution "must have" for your team (faster recovery, cyber vault, automation)?

As noted in the RFP, must have items for the proposed solution include immutability and RTO/RPO objectives that are rapidly achievable.

83. What's your preferred buying motion (direct, partner-led, managed service)?

ARC is not seeking a managed service solution. Direct and partner-led are both acceptable proposal directions.

84. If we identify fit, what's the best next step — technical workshop, sizing, or solution overview?

The provided inventory is the sizing scope for this engagement. The selected vendor should anticipate implementation and demonstration of performance as logical next steps following award.

85. Where do backup jobs fail most often, and why?

Traditionally, backup jobs most commonly fail due an event external to the backup platform such as an agent being offline or a hardware fault.

86. How long do restores take for your top applications under real conditions?

    The focus of the RFP is implementation of a replacement platform and not on current processes or procedures. The proposed solution should demonstrate the ability to meet define RTO/RPO objectives under real conditions.

87. Which platforms are hardest to protect or automate (databases, containers, NAS/object)?

    The focus of the RFP is implementation of a replacement platform and not on current processes or procedures. The proposed solution should demonstrate the ability to automate protection throughout a variety of workloads.

88. Do you assume backups can be targeted by adversaries? How do you mitigate that?

    Yes. Backups are stored on a separate network segment to reduce potential targeting.

89. What is your confidence level in recovering a clean, known-good state after an attack?

    The focus of the RFP is implementation of a replacement platform and not on current processes or procedures. The proposed solution should demonstrate confidence inspiring data protection and recoverability.

90. What reports do auditors ask for, and how quickly can you generate them?

    While ARC has traditionally not been required to provide audit reports for backup/recovery or disaster recovery processes, the proposed solution should include the ability to report performance and validation for all processes under management.