ARC-IT Business Solutions Ltd
12 Gleneagles Court
Brighton Road
CRAWLEY
West Sussex
RH10 6AD

01444 817506
enquiries@aibs.co.uk
www.arcitbusinesssolutions.com

Arc Backup and BCDR Service Definition

1. Service Overview

Arc Backup and Business Continuity and Disaster Recovery (BCDR) is a managed backup, business continuity and disaster recovery service. The service protects on-premises servers and virtual machines, and Microsoft Azure virtual machines, using an image-based backup approach. It provides immutable backup copies, off-site replication, automated verification and a range of restore and virtualisation options to support rapid recovery after outages, accidents or cyber events.

Arc delivers onboarding, configuration, monitoring, alerting, reporting and regular service reviews.

2. Service Features (What's included)

2.1. Backup

Backup features focus on ensuring you always have recent, recoverable restore points that are protected from deletion and ransomware. Arc configures and manages backup schedules, retention, replication and verification based on your critical systems and agreed recovery objectives.

- Image-based backups. We take image-based backups that capture the operating system, applications, configuration and data.
- Immutable backup snapshots. Each incremental backup is stored as a standalone snapshot that cannot be altered. If one snapshot is removed, other restore points remain usable.
- Cloud Deletion Defence. Deleted backup data is held in a recoverable state (like the recycle bin), protecting against accidental or malicious deletion.
- Encryption in transit and at rest. Backup data is encrypted during synchronization, storage and replication. Data is also encrypted at rest using hardware encryption in the cloud platform.
- Backup verification. Automated verification runs after backups to confirm protected volumes are included and restore points are bootable. Daily screenshot verification boots a recovery point and captures the boot/login screen. Application checks can validate key services (e.g., SQL, DHCP, AD, DNS) and can be customised per VM.
- Ransomware detection on backups. The platform monitors for early indicators of ransomware activity impacting protected systems and backup data.
- Replication and geo-redundancy. Backups are replicated off-site to secure cloud locations. The service supports geo-replication to secondary sites. Data centres are located across multiple geographies, including UK, Germany, Iceland, USA, Canada, Australia and Singapore.
- Multi-volume support. Supports workloads with multiple disks/volumes. The platform can protect up to 6TB of virtual disk capacity per protected system subscription; multiple subscriptions can be used where needed.

- Initial cloud synchronisation options. Where initial cloud synchronisation would take too long across the internet, a “round-trip” device can be used to seed the first off-site copy. Synchronisation can also be throttled to reduce impact on business connectivity.
- Restore Options

Restore Method	Summary	Benefit
File and folder restore	Recover individual files and folders to the original or alternate location.	Fast recovery from accidental deletion or corruption.
Volume restores (iSCSI)	Expose protected volumes as an iSCSI target for recovery.	Granular recovery without full server rebuild.
Bare metal restores	Restore back to physical or virtual hardware.	Recover entire systems after major failure.
Local virtualisation	Boot protected systems locally on the backup device.	Rapid continuity for critical systems during on-site outages.
Cloud virtualisation (Datto Cloud)	Boot systems in the Datto Cloud for DR.	Continue operations even if the primary site or Azure is unavailable.
Virtualise via hypervisor / ESX upload	Boot in your hypervisor environment or upload restore points to ESX host.	Flexible recovery for virtualised estates.
Export image	Export recovery points as VHD/VHDX/VMDK.	Portability for audit, migration or specialist recovery scenarios.

2.4. Business Continuity

Business continuity features are designed to keep the organisation operating while full restoration is completed. The aim is to maintain key services for a core set of users and functions during an outage.

- Local virtualisation. Where a local backup device (physical or virtual) forms part of the service, Arc can virtualise a protected system locally on the device to provide rapid access during incidents where primary infrastructure is unavailable.
- Cloud virtualisation (Datto Cloud). Arc can boot protected workloads in the cloud to maintain service during a site-wide outage. Cloud virtualisation is available under fair use during an active recovery, with an open support ticket and agreed restoration plan updates. In practice, you can continue to operate from the Datto cloud all the time you can provide an updated plan with timescales to fully recover.
- Business-critical workload scope. During onboarding Arc works with you to identify which systems are “critical” for continuity and should be prioritised in recovery. We will also agree who the core set of users are. Backups will cover all agreed systems, but continuity and DR runbooks will prioritise critical services.

2.5. Disaster Recovery

Disaster recovery features support structured, repeatable recovery when there is a major incident. Arc documents the recovery approach, tests it and helps you demonstrate readiness.

- Recovery objectives (RPO and RTO). Target Recovery Point Objective (RPO) is 4 hours, and target Recovery Time Objective (RTO) is 4 hours, excluding recovery time associated with a security event where systems must be validated as clean before return to service.
- DR runbook and orchestration. Arc produces a DR runbook documenting recovery order, configuration, resource allocation and network requirements for recovery. This includes agreed priority systems for DR activation.

- DR testing. Arc includes one DR test per year. Tests validate orchestration, configuration and recoverability.

2.6. Service Management

- Structured onboarding with an Arc Implementation Lead and agreed communications plan.
- Ongoing monitoring of backup job health, replication status and verification results.
- Quarterly service reviews covering KPIs, restore activity, storage utilisation, risk items and improvement actions.
- Optional access to customer portal.

2.7. Retention

- Standard retention is 1 year.
- Retention settings apply to both local and off-site copies.

2.8. Service Hours

- Backup operations and platform monitoring run 24x7 according to the agreed schedule.
- Arc service desk contact and standard communications and notifications are provided during Business Hours, defined as Mon–Fri, 09:00–17:30, excluding UK Bank Holidays.

You may contact us by telephone during Business Hours on: -

+44 (0)1444 817506

or you may report an issue or make a request by emailing: -

SecurityDesk@aibs.co.uk

Optionally, you may request access to your own Arc-IT Web Support page, where you can submit and track the progress of your incident and request tickets.

3. Service Implementation (How we onboard you)

3.4. Initiation and Access

- Assign Arc Implementation Lead and confirm stakeholders, change windows and communications.
- Establish secure remote access, data sharing and permissions.
- Confirm workloads in scope (on-prem servers/VMs and/or Azure VMs) and agreed RPO/RTO targets.

3.5. Design and Readiness

- Define critical systems for continuity and DR sequencing.
- Confirm retention requirements and replication locations (where applicable).

3.6. Deploy and Configure

- Deploy Windows/Linux agents as required and configure protection sets.
- For Azure VM protection, configure Datto Azure Backup access (requires Azure admin credentials).
- Configure schedules, verification and replication settings.

3.7. Validation and Go Live

- Run initial backup and verification cycles.
- Confirm screenshot verification

- Confirm application checks for critical workloads.
- Complete a test restore (file/folder or VM) to validate operational readiness.
- Transition to steady-state monitoring, reporting and service review cadence.

4. Customer Responsibilities and Dependencies

- Provide administrative access to protected systems and, where applicable, Azure admin credentials to enable Azure VM protection.
- Provide and maintain network connectivity required for backup, replication and management (including outbound internet access where needed).
- Provide named contacts for operational notifications and service reviews.
- Inform Arc of material changes to protected workloads (new servers, decommissioned systems, major application changes) to keep protection aligned.
- Approve and support agreed change windows for agent deployment and recovery testing.
- Confirmation of accepted risk where our recommendations are declined by you.

5. Exclusions

- Emergency recovery assistance and incident response activity is excluded from this service.
- Cross-cloud recovery into cloud platforms outside Datto Cloud and Microsoft Azure is excluded.
- End-user device backup (laptops/desktops) and SaaS application backup (e.g., Microsoft 365 mailboxes).
- On-site services are excluded; the service is delivered remotely.

6. Operational Service Levels and Targets

6.1. Service Levels

Severity	Impact	Description	Response Target	SLA KPI
Severity 1	Critical	Backup failed 3 consecutive runs; replication stopped for critical workload; verified restore point unavailable for critical system	2 hours	95% of all events/incidents responded to within target (measured on a quarterly basis)
Severity 2	Major	Backup failed 2 consecutive runs; storage near capacity; verification failures for critical system	4 hours	
Severity 3	Minor	Backup failed once; warnings; non-critical verification issues	1 business day	
Severity 4	Info	Informational alerts; reports; planned maintenance notifications	As scheduled	

Response = time from when Arc receives or generates an alert to when initial advice and next steps are provided to you.

6.2. Escalation

- The Customer may request that the severity of their event or incident be expedited by contacting the Customer Service Manager using the contact details in section 2.

6.3. Service Availability

- 99.9% availability for all SaaS components of the service

6.4. Reporting

The following KPI's will be reported to you on a quarterly basis:

- RPO and RTO targets and any exceptions.
- Backup success rate.
- Storage utilisation and capacity headroom.
- Recent restores and recovery activity.
- SLA response performance.

7. Technical Standards and Compliance

- Datacentre and platform controls include ISO 27001 and SOC 1 and 2 aligned assurance.
- Data is protected using AES-256 encryption and is encrypted throughout synchronisation, storage and replication.
- Physical access controls include 24x7 guarded facilities with dual biometric and RFID access controls and logged access to secure areas.