

G-Cloud 15

Service Definition

Backup as a Service, Disaster Recovery (DR) as a Service

NG-IT

Lot 2a: Infrastructure Software as a Service (iSaaS)

1. Introduction	3
Company Overview	3
Social Value	3
Overview of the G-Cloud Service	6
Associated Services	9
2. Data Protection	10
Information Assurance	10
Data Back-Up and Restoration	10
Business continuity statement/plan	11
Privacy by Design	12
3. Using the service	13
Ordering and Invoicing	13
Availability of Trial Service	13
On-Boarding, Off-Boarding, Service Migration, Scope etc.	13
Training	14
Service Management	15
Service Constraints	15
Service Levels	16
Outage and Maintenance Management	17
Financial Recompense Model for not Meeting Service Levels	17
4. Provision of the service	19
Customer Responsibilities	19
Technical Requirements and Client-Side Requirements	20
After-sales Account Management	20
Termination Process	20
5. Our experience	22
Case Study	22
Clients	23
Contact Details	24

1. Introduction

Company Overview

NG-IT are the UK's leading provider of next generation Private Cloud, Hybrid Cloud and Cyber Security services. We make digital innovation a reality by delivering flexible, always available, highly agile IT services using innovative, next generation technology solutions.

As a multi award winning business, NG-IT is dedicated to meeting the demands of today's business environment. Instead of taking legacy ideas, systems, processes, and technologies, we deliver an exceptional experience around the understanding, design, deployment, and management of next generation data centric and cyber security solutions.

It is critical to stay head of attackers, and our solutions work to identify both new technologies and new and emerging threats. At NG-IT, we understand how important these steps are to ensure that your business is secure against old and new Cyber security threats. This way we can improve your security posture, reduce the risk to your business and keep you where you should be - ahead of the cyber attackers.

NG-IT have deployed over 400 private cloud, hybrid cloud or cyber security solutions including migrating more than 60,000 applications and 32,000 TBs of data. Our professional services capability allows us to provide a full end to end service for our customers, to ensure a seamless working relationship from the initial engagement to the delivery of the chosen solution.

We continually review and assess leading and emerging technology vendors, and our expertise lends us to consider the best options for our customers. We've invested heavily in our people to bring you the very best working relationship and technical consultancy there is to offer.

Social Value

In an increasingly digital and fast-paced world, our Social Value Strategy reflects a deep commitment to people, communities, and the planet. We believe that technology should not only drive innovation but also foster trust, inclusion, and long-term wellbeing. Our legacy is built on a human approach, listening, guiding, and delivering solutions that leave lasting confidence.

Our mission is to be a trusted advisor and supplier of hybrid cloud, security, and data protection services. Our vision is to help businesses prosper through innovative technology, and our values centre on a customer-first culture powered by quality people.

Kickstart Economic Growth

Commitment:

We support inclusive economic growth by investing in SMEs and VCSEs, promoting fair pay, and enabling local innovation through ethical procurement.

Initiatives & SMART Objectives:

- SME & VCSE Spend Growth: Audit current spend and increase by 15% over 3 years, aligned with local authority targets.
- Fair Payment Code: Ensure 100% of suppliers are paid within agreed terms by Q4 2026.
- Metrics & Monitoring:
 - Regular audits
 - Supplier satisfaction surveys
 - Spend tracking via finance systems

Governance & Ownership:

- Led by our Finance Department
- Reviewed annually

Make Britain a Clean Energy Superpower

Commitment:

We reduce our environmental footprint and promote sustainable digital practices that support the UK's Net Zero ambitions.

Initiatives & SMART Objectives:

- Carbon Reduction Plan: We are currently gathering baseline data on our operational emissions to inform a measurable reduction strategy. Our goal is to identify key areas for improvement and set a science-based emissions reduction target by the end of 2026, with a focus on energy-efficient infrastructure and remote-first working practices
- Net Zero Roadmap: We are currently in the process of gathering baseline data on our carbon emissions across Scope 1, 2, and relevant Scope 3 categories. This data will inform the development of a science-based Net Zero strategy. Our aim is to set a formal Net Zero target by the end of 2026, including plans for verified offsetting of any residual emissions.
- ISO14001 Certification: Maintain certification through annual audits and continuous improvement.
- Metrics & Monitoring:
 - Carbon accounting via Scope 1–3 reporting tools
 - Annual sustainability reports
 - Internal audits and external verification

Governance & Ownership:

- Led by our Operations Manager
- Reported to the Board

Break Down Barriers to Opportunity

Commitment:

We foster inclusion through education, skills development, and fair employment practices, empowering underserved groups and future talent.

Initiatives & SMART Objectives:

- Digital Skills Outreach: Deliver workshops annually in underserved regions via charity partnerships.
- Careers Advice Programme: Provide virtual careers advice and mentoring to students from diverse backgrounds.
- Volunteering Leave: Provide 2 paid days per employee annually, with 80% uptake by 2026.
- Gender Pay Gap Transparency: Publish annual reports, regardless of company size.

Metrics & Monitoring:

- Diversity metrics tracked via HR
- Workshop attendance and feedback forms
- Careers advice session participation and feedback
- Volunteering uptake reports

Governance & Ownership:

- Led by Finance and HR and Management
- Supported by Management

Build an NHS Fit for the Future

Commitment:

We contribute to a healthier workforce and community through mental health support, wellbeing initiatives, and responsible leadership.

Initiatives & SMART Objectives:

- Able Futures Promotion: Increase internal awareness and usage by 30% over 12 months.
- MHFA Training: Train 10% of staff as Mental Health First Aiders by 2026.
- Wellbeing Surveys: Maintain 90% response rate and use feedback to shape quarterly wellbeing actions.

Metrics & Monitoring:

- Programme usage analytics
- Training completion rates
- Survey dashboards and action logs

Governance & Ownership:

- Led by our Wellbeing Lead and HR Manager
- Reviewed quarterly by the Employee Engagement Committee

This strategy aligns with:

- PPN 06/20: Delivering social value in procurement

- PPN 02/23: Carbon reduction plans and Net Zero
- PPN 09/21: Modern slavery risk assessments
- PPN 03/23: SME-friendly procurement practices

We ensure proportionality to contract size and maintain flexibility to tailor initiatives to specific project needs.

Overview of the G-Cloud Service

NG-IT take great care in selecting our service provider partners. We undertake a rigorous selection process that affords us the confidence to promote and justify Assured Data Protection (ADP) as our key partner for Backup as a Service, Disaster Recover as a Service, 365 Backup as a Service and Clean Room as a Service.

ADP provides essential insights and expertise across all types of environments and infrastructure, making them the ideal partner for our customers to engage and trust as the service provider for this proposed platform.

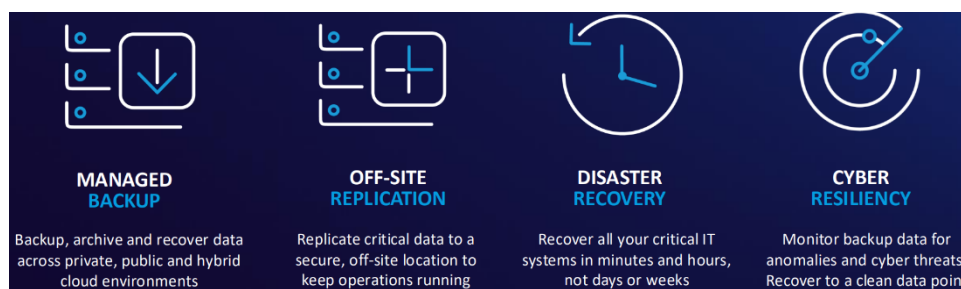
ADP eliminates the complexity, expense, and management of backup and data protection. We have teamed up with Rubrik to offer ground-breaking technology to make backup, disaster recovery and business continuity simple.

They have over 200 years of industry experience in the senior leadership team in delivering backup, disaster recovery, and business continuity as a service. As Rubrik's leading Managed Service Provider (MSP) they offer solutions as managed services tailored to individual business needs, making it affordable and achievable.

NG-IT and ADP's clients receive a fully managed service from design and implementation through to recovery and daily proactive support.

ADP is Rubrik's first and largest MSP, and fully Rubrik Authorised Support Partner (RASP) and has exclusively been a Rubrik provider since inception and is the only dedicated Rubrik service provider in the world. This unique relationship enables ADP to offer unrivalled support and case escalation, as well as fast track feature requests directly to Rubrik. ADP worked closely with Rubrik to design the Remote Office Branch Office (ROBO) deployment which is widely used by multi-national customers today.

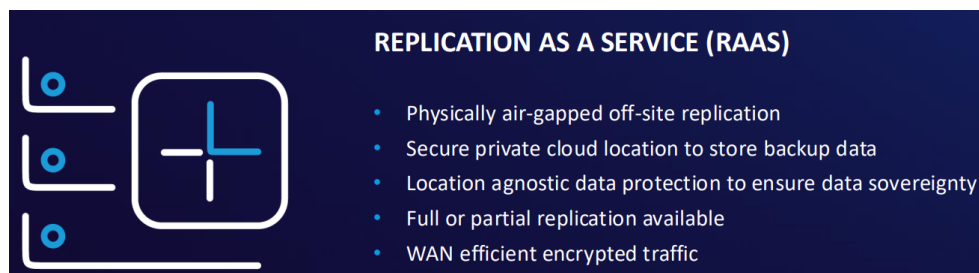
ADP protect over 150 petabytes of data for their 500+ global customers, ranging from single site to large multi-national deployments. Customers leverage backup or full disaster recovery as a service, consumed as an operation or capital cost.



Backup as a Service using Rubrik Technology to deliver the service. In all cases Rubrik will deploy a physical Rubrik appliance at customers site/data centre. ADP will provide your organisation with a local backup appliance with a predefined and agreed usable capacity. This is based on years of experience working with Rubrik, applying the average deduplication and compression ratio we achieve across our 450+ customers and 150PBs+ of Rubrik data under protection. We are always conservative with the compression and deduplication ratios, to ensure no under sizing and always extra room for growth.



Replication as a Service where ADP managed Rubrik solution provides secure replication from the on premises Rubrik cluster to a secure Rubrik cluster hosted inside ADP's UK data centre. This will enhance resiliency and provide business continuity. It is a reliable recovery method that provides recent copies of your data that can be quickly restored, reducing Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), when compared to on-site backups alone. Downtime and data loss reduction is one of the benefits of this service.



Disaster Recovery (DR) as a Service using Rubrik Technology to deliver the service. The ADP managed Rubrik DR solution provides a secure hosted DR platform with periodic DR testing and invocation. Your organisation's encrypted backup data can be replicated to ADP's UK Rubrik data centres. Rubrik's replication is incremental forever and WAN efficient. Data transfer speeds can be throttled, although this functionality is typically only required for the initial replication process. The solution will leverage the existing internet connection; no new internet connectivity will be required.

The Rubrik cluster and live mount functionality are used for the majority of the VM recoveries in the event of a DR. Live mount rapidly presents data for multiple VMs at the same time. If ADP's is DRaaS is taken, production flash storage is provided for applications and services requiring high performance storage. Data can also be migrated from the Rubrik cluster to production storage without affecting the performance or user experience. ADP provide 1:1 compute (Production:DR).

ADP's DRaaS team ensures networking is as agreed in the DR workshop. Networking is the most important part of the process and where we will really collaborate to ensure it is documented and

tested. All connectivity is provided by ADP. There is no limit to bandwidth and no ingress or egress charges.

ADP's DR team will conduct a fully documented and timed test each year. Typically, the DR test is performed relatively quickly after the service has been implemented. The DR document can be used for auditing and compliance.

DR can be invoked at any time. The DR and support teams operate 24/7/365. Once DR is invoked and operational, ADP will back up the data in line with your backup requirements. Essentially it is now the production data.



DISASTER RECOVERY AS A SERVICE (DRAAS)

- Fully-managed data recovery service for IT failure
- Ensures near-zero server recovery time on and off site
- Less cost than operating a secondary data center
- Tested annually to prove recoverability of all data
- Keep business operations running with minimum disruption

Backup for Office 365 backup service that backs up a customer office 365 environment from the Microsoft cloud to ADP using Rubrik platform. This backup includes email, teams and One Drive/SharePoint. M365 backup solution is a cloud-to-cloud product designed to back up data held in Microsoft's Exchange Online, OneDrive, SharePoint Online, and Teams Online. It is fully managed from Rubrik's centralised management platform, Rubrik Security Cloud (RSC). RSC provides customers with a simple, homogenous data management experience across all platforms that reduces the overhead associated with legacy tooling and point solutions. Access control to RSC is provided using 2FA and granular RBAC.

M365 backups are stored in a Rubrik owned Azure Tenancy called Rubrik Cloud Vault (RCV) providing an isolated immutable copy of data, away from your production environment. Backup data and indexes are stored in Azure Blob and table stores, using AES 256-bit encryption. CUSTOMER can select the region to match their data location requirements. Master encryption keys are stored in Azure Key Vault. Access credentials to storage and Key Vaults are unique per customer.

The backup data is also replicated via zone-redundant storage (ZRS)¹ which copies data synchronously three times to physically separated data centres in the same geographic region to comply with NCSC 3-2-1 backup guidelines.



Rubrik Enterprise Edition is a unified data protection platform that enables organisations to protect, manage and recover critical data whether it resides in on premisses data centre or across cloud environments. It provides consistent set of capabilities across both physical and virtual infrastructure and cloud workloads, supporting hybrid and multi-cloud strategies under a single operational model. These characteristics provide you consistent data protection, help improve your operational efficiency, enhance security against cyber threats and gives you a flexible recovery option.

Entra ID is a managed backup service of Microsoft Entra ID cloud identity and access management.

Why Backup Entra ID?

- Soft delete only (30 days retention for users, emails, etc.)
- No full rollback for settings, policies, and configurations
- No automatic point-in-time recovery
- Limited audit logs and retention

Rubrik Cloud Vault is a fully managed off-site cloud archive for backup data. It provides an additional layer of resilience against data-loss, cyber threats and operational disruption. Key benefits include improved cyber resilience and, simplified operations.

Identity Recovery for 365 is a capability that focuses on protecting and restoring critical identity systems. Identity Recovery ensures that these core services are restored in a reliable and efficient manner. It builds immutable backups of identity that are stored in an isolated environment. These backups cannot be accessed nor deleted, which means that they can be trusted as a clean source for recovery. Key benefits are reduction of operational complexity and protection against security threats.

Associated Services

NG-IT can provide Professional Services to install and configure the proposed solution. Data migration services are available if required.

2. Data Protection

Information Assurance

- Cyber Essentials Plus
- We are certified under the Cyber Plus scheme, demonstrating our commitment to protecting against common cyber threats across our remote working environment.
- ISO 9001 – Quality Management
- This certification ensures our virtual service delivery is consistent, customer-focused, and continuously improving.
- ISO 14001 – Environmental Management
- Reflects our commitment to sustainability through digital-first operations, reduced travel, and energy-efficient cloud-based tools
- Information Management Process:
- Secure Cloud Platforms: All internal and client communications are conducted via encrypted cloud-based systems with strict access controls.
- Remote Access Security: Employees use multi-factor authentication, VPNs, and endpoint protection to securely access company resources.
- Data Handling Policies: We comply with GDPR and the Data Protection Act 2018, ensuring lawful and transparent data processing.
- Incident Response: We maintain documented procedures for breach detection, escalation, and resolution, aligned with industry best practices.
- Supplier Vetting: All third-party vendors are assessed for compliance with security, ethical, and sustainability standards

Data Back-Up and Restoration

NG-IT Limited recognises that the efficient management of its data and records is necessary to support its core business functions, to comply with its legal, statutory, and regulatory obligations, to ensure the protection of personal information and to enable the effective operation and management of the organisation.

To guarantee that, we have a Data Backup Policy that applies to all staff within the Company with a purpose of safeguarding information belonging to us, any third parties and clients. We do not hold business critical data within a traditional on-premise network or managed data centre, all line of business application data and unstructured file data is located within cloud storage, owned and managed by the relevant application vendor the data is specific to.

This business systems technology model allows for continuous replication of data from production cloud platform to secondary storage or an alternative cloud platform, effectively providing always available, fully comprehensive, granular backup with quick restore capabilities.

Backup

- Full backups of all data are performed weekly. Full backups are retained for 3 months before being overwritten.
- Backups are stored in secure locations. A limited number of authorised personnel have

- Backup of data held within Database Systems have data backup routines which ensures database integrity is retained

NG-IT adopts the best security practices by defining security controls applicable to the entire organisation. Additional security measures identified through risk analysis, legal, regulatory, and/or contractual concerns, and/or specific standards -shall be addressed accordingly. Security controls and best practices are be considered and implemented as appropriate to the risk level.

Business continuity statement/plan

Business continuity is not simply a matter of contingency, it is a core component of delivering consistent, reliable service in a competitive and fast-evolving industry. As an IT reseller/security and service provider operating with a fully remote workforce and reliant on only on cloud-based systems with no corporate network, NG-IT Ltd recognises the importance of being prepared for unforeseen disruptions, whether technical, operational, or external.

We have a Business Continuity Plan that outlines measures to ensure that our operations remain stable and responsive during periods of disruption. It defines the procedures, responsibilities, and safeguards that enable us to continue supporting our clients, maintain supplier relationships, and uphold our professional standards. The plan reflects our commitment to resilience and readiness, and will be reviewed regularly to ensure it remains aligned with our business needs and the expectations of those we serve

This Business Continuity Plan sets out the procedures and responsibilities required to ensure the continued operation of NG-IT Ltd in the event of a disruption. It applies to all employees and covers both the reselling of IT services, hardware and software distribution. The plan is designed to safeguard client relationships, maintain service delivery, and protect the company's reputation.

The key aims of this plan are to:

- Ensure continuity of service provision to clients.
- Minimise delays in hardware fulfilment and vendor coordination.
- Maintain secure and effective communication with customers and suppliers.
- Uphold contractual obligations and regulatory compliance.

The following functions are considered critical to the business and must be maintained during any disruption:

- Vendor liaison and procurement
- Order processing and fulfilment
- Customer support and issue resolution
- Financial operations including invoicing and payments
- Internal communication and collaboration

All our staff members have defined roles in the event of a disruption. The Managing Director is responsible for overseeing the implementation and maintenance of this plan. The Operations

Manager and Finance Manager manages supplier relationships and hardware sourcing. The Technical Director and Cyber Lead ensure access to systems and data security. The Account Managers handles customer communications, and the Finance Officer ensures continuity of financial operations

All our business systems are cloud-based and configured for daily automated backups. Access is controlled via multi-factor authentication and role-based permissions. A centralised password manager is used across the organisation. Security audits are conducted quarterly to ensure compliance with data protection regulations and best practice.

Internal communications during a disruption will be conducted via internal messages and email, with SMS or telephone used for urgent alerts. External communications with clients and suppliers will be managed via email and telephone.

In the event of a disruption, recovery procedures will be activated immediately. Alternative suppliers may be engaged to maintain service continuity. Clients will be informed of any delays or changes to service provision. Staff availability will be managed through cross-training and flexible working arrangements. Any cybersecurity incidents will be addressed by isolating affected systems, restoring data from backups, and notifying relevant stakeholders.

This plan will be tested annually through structured exercises. Supplier performance and supply chain reliability will be reviewed in line with our ISO management system. Contact lists and standard operating procedures will be updated accordingly. Following any real disruption, a post-incident review will be conducted to identify areas for improvement.

Privacy by Design

We are committed to embedding privacy into every aspect of our service delivery. As an IT reseller, we do not process personal data directly through proprietary platforms, but we ensure that all technologies we recommend, resell, or support meet GDPR standards and respect user privacy from the outset.

- **Privacy by Design:** We assess privacy risks during the initial selection and onboarding of any suppliers. This includes reviewing data handling practices, encryption standards, and access controls before recommending solutions to clients.
- **Supplier Vetting:** All vendors we work with are evaluated for GDPR compliance, including their use of data processors, sub-processors, and data residency policies.
- **Minimal Data Handling:** We store minimal personal data (e.g., names and email addresses) solely for communication and support purposes. This data is handled securely, in line with GDPR principles, and is never used for profiling, marketing, or shared with third parties without consent.

3. Using the service

Ordering and Invoicing

To order services from our organisation, you can simply send an email to gcloud@ng-it.co.uk to discuss your requirements in more detail and initiate the process. We recommend including key information in your email such as your organisation name, a brief description of the services needed, preferred start date, expected outcomes, and any relevant procurement references. Once we have reviewed your request, we will assist you in completing the Order Form, which formalises the agreement under the framework and becomes the Call-off Contract. This includes support with service scope, pricing, and terms to ensure everything aligns with your expectations. Our fees are invoiced monthly in arrears, and payment terms are 30 days net from the date of invoice receipt.

Availability of Trial Service

At the present, complimentary trial of the Backup as a Service, Disaster Recovery (DR) as a Service Solution cannot be offered, as the nature of the Service involves fully managed security operations that cannot be replicated in a short period and standalone trial environment. As an option to the trial and upon request, we can offer a product demo and a Proof of Concept (POC). The POC will give you a good view of the Product capabilities and how the service aligns within your environment, allowing an applied assessment, and the demo can provide an overview of core functionalities.

On-Boarding, Off-Boarding, Service Migration, Scope etc.

Once the Managed Service Contract is signed and we have the confirmation of your order, the onboarding process begins, and a designated team is assigned within the Service Provider to coordinate all aspects of your contract and provide a smooth onboarding process. As your IT Service Reseller, we will also have a dedicated Service Delivery Coordinator looking after your contract and leasing periodically with the Service Provider during the whole lifetime of your contract. At this point, your dedicated Service Delivery Coordinator will make sure that the Service Provider will follow the steps outlined in their onboarding process.

As a starting point, you will receive a Welcome Email from the Service Provider and an invitation to schedule a kick off call. This serves as a formal starting point and you will be introduced to the team that will work with you during the implementation period. During the kick off call, it is expected that the Service Provider walks through the initial scope of the service, get a mutual understanding of what is included and outline next steps.

Moving forward towards the Service implementation, you will work with the Service Provider Implementation team on the operational work required to start the service which will include the hardware building, configuration, testing and monitoring of the initial data recovery of your environment. Depending on the scope and complexity of the service, the assigned Service Provider Project Manager may suggest a weekly call to track the progress of the process.

If your contract includes Disaster Recovery as a Service, you will be assigned a team of Solution Engineers that will build and deploy all Disaster Recovery elements required. This will be a collaborative process and that will guarantee that the service will progress from its initial set up into steady-state operation.

We have outlined a timeline of the process to facilitate its comprehension:

Kick off call – Complete Site Survey – Service Provider orders HW – HW build & ship to customer – Configuration – Monitor – Test Recover and Training – Troubleshoot and Replication Success – Validation – Steady State Call – Handover to CS & Support - BAU

Onboarding Timeframes

- Implementations: 10-12 weeks
- Solutions (DR): 5-6 Weeks
- M365: 4 Weeks
- Cloud Native: 10-12 Weeks

Please have in mind that this is not a static process and the steps and timeframes may vary according to the environment sizing and complexity.

A detailed implementation plan can be provided to the buyer on request.

Training

As a reseller, we provide buyers with access to the service provider's comprehensive training and onboarding resources. These include online help documentation, knowledge bases, and guided assistance to support orientation with the new service. Introductory onboarding sessions are available to ensure buyers understand how to configure, monitor, and manage the Assured Data Protection (ADP) systems effectively. Where required, we facilitate access to the provider's customer success team for tailored onboarding support. Our role is to ensure buyers are connected to the appropriate resources and that any queries are escalated promptly to the service provider for resolution.

To guarantee a seamless and smooth environment transition and data migration, Assured Data Protection (ADP) will provide support and guidance as part of the Service onboarding. You will receive all the instructions to help you migrating and setting up your Service. Service Provider will provide training around the ADP Portal, either via training materials or walk-throughs, to ensure that you have all necessary information to navigate through ADP with confidence. You will also have access to Webinars and Education Sessions, and an extensive learning content library available on the customer portal.

You will count with 24x7 support team, that can be contact via email, phone or ticket and will be available not only to assist you with incidents and technical related issues but answering any questions you may have on how to use the Service Provider features.

Service Management

We take an integrated approach when it comes to the management of Services as we understand that an effective service delivery relies on a balanced integration of expert personnel, mature ITIL v4 aligned processes and technology. From a workforce perspective, our team possess both technical and behavioural competencies required. This includes not only the commercial knowledge of our products and solutions, but technical proficiency to build the service architecture, relying on a Team of experienced Solution Architects that holds the accreditations necessary to support the delivery of our Services.

In alignment with the technical team, we have a Service Delivery process in place that maps out the level of Service that is expected and provide operational consistency and governance throughout the delivery of the Service. This includes a Team of dedicated Coordinator that hold ITIL v4 Certification and is assigned to reinforce a customer-centred approach and guarantee that all aspects of your contract are being provided accurately. This process guidelines are outlined based on ITIL Framework, which set the basis for all the procedures followed to guarantee the delivery of IT Services that meet customer's needs.

This process counts with clear escalation paths, service level agreements and communication protocols to safeguard service continuity and accountability. We also count with a well-structured continuous improvement procedure, including post incident review with the customer and the Service Provider, and trend analysis that will help us to identify and tackle any systemic issue and enhance our client experience and satisfaction. These processes help us to set the standards of what we do as the IT Reseller but also direct what we expect from the Service Provider Partner.

Service Constraints

The Service Provider do not count with a published Uptime Guarantee as the solutions include outside factors that are outside their control including use of hosting providers. They also ingest data from 3rd party sources which could be delayed due to items outside of their control and result in an inability to notify/detect threats for a given telemetry source.

While Service Provider does not publicly publish uptime numbers, their typical uptime SLO is 99.5%.

The Provider, to the extent possible, will notify the Customer about scheduled or emergency maintenance through the Provider's Account Management Application. The Provider will constantly update the Account Management Application information to advise the Customer when a maintenance is completed.

Rest assured that, as your IT Reseller, we will make sure that the Service Provider notifies you of any outages with a portion of its solution and provide a recovery time estimate.

Service Levels

Clients will benefit from unlimited access to ADP's global support team, together with a dedicated Service Delivery Manager. All clients will have access to ProtectView, ADP's cloud-based, centralised platform which enables users to proactively view and monitor their entire Rubrik estate from a single pane of glass.

The Service Desk operation is available 24 x 7 x 365 and can be contacted by telephone and email. Your service call is routed directly to the ADP Service Desk who will log your service call, agree the priority and assign a customer service call number which will allow your request to be identified efficiently and tracked at all times.

The following detail examples of the priorities to be used when logging Incidents or Service Requests. The service desk shall respond to all requests for support in accordance with the guidelines in tables below:

Incident Priorities - Priorities of the incident are set upon ticket creation by the Service Desk Analyst based upon the generated alert, support email or customer phone request, and will be agreed with the customer.

Priority 4 (P4 - Low) - Minimal Business Impact – An anomaly, issue or error which has no direct impact on service availability. Typical Event:

- Request version upgrade.

Priority 3 (P3 – Medium) - Isolated Business Impact – Loss of service to a single entity or impact to a small number of entities. Noncritical function or procedure is affected and no direct impact on services availability. No significant business impact is encountered. Typical Events:

- Hardware redundancy failure (HD in RAID group, redundant node, etc.).
- Errors in isolated object backups (single VM, single fileset, etc.)
- Disaster Recovery environment performance of On Demand resources.

Priority 2 (P2 – High) - Significant business Impact- a degradation, failure or outage which has a significant impact to important, time critical or business operations but has an effective workaround or a failure which presents a risk of significant impact to the business operation. Typical Events:

- Replication link down.
- Hardware failure causing intermittent interruption to backups.
- Errors across many object backups.
- Temporary workaround available.

Priority 1 (P1 – Critical) - Critical Business Impact – A failure or outage that severely affects or materially risk's the normal business operation. Typical Events:

- Disaster Recovery environment offline during a live event.
- Hardware failure of on-site appliance where data is unable to be restored.
- Failure to restore an object due to service availability.
- Escalation of P2 incident

Service Request Priorities - Priorities of the service request are set upon ticket creation by the Service Desk Analyst and agreed with the customer.

Priority - Low - Minimal Business Impact – Where the request will not have an impact on their service within 36 hours. Typical Events:

- Change or modify SLA set (this will be under change control).
- Schedule a DR test.
- Advice & Guidance.
- 4. Information requests.

Priority - High - High Business Impact – Where the request will have a material impact on their service within 6 hours. Typical Events:

- Errors in isolated object backups (single VM, single fileset, etc.
- Disaster Recovery environment performance of On Demand resources

NG-IT as your IT Reseller, throughout its Service Delivery Process and according to the ITIL v4 Framework guidelines, will make sure that the Service Levels will be followed by the Service Provider according to what has been agreed on the Service Agreement signed by all parties. As part of this, you will be able to count with a dedicated NG-IT Service Delivery Coordinator that will conduct period checks to all support tickets that you might have opened with the Service Provider and action on whatever is required to guarantee the effective delivery of the service.

Outage and Maintenance Management

Service Provider will monitor and manage the technology components required to deliver 24/7 Service. This includes upgrades, uptime/status monitoring, etc. As well as monitoring their own infrastructure we also monitor the feeds / agents / sensors etc. from our customers environments that are ingested into their environment.

The Provider, to the extent possible, will notify the Customer about scheduled or emergency maintenance through the Provider's Account Management Application. The Provider will constantly update the Account Management Application information to advise the Customer when a maintenance is completed.

NG-IT as your IT Reseller, throughout its Service Delivery Process and according to the ITIL v4 Framework guidelines, will make sure that the Service Levels will be followed by the Service Provider according to what has been agreed on the Service Agreement signed by all parties. As part of this, you will be able to count with a dedicated NG-IT Service Delivery Coordinator that will conduct period checks to the Service Provider state and promptly address any outages and request ad-hoc service if applicable. Root Cause Analysis and Service Improvement Plans will also be requested whenever is appropriate.

Financial Recompense Model for not Meeting Service Levels

The availability of service credits due to Service Level Agreement (SLA) if the Service Level Agreement (SLA) is not achieved, will be determined for each Customer as part of their individual Service Agreement. Where a customer requires credits as part of their commercial terms these will be

discussed during contract formation and may be incorporated into the applicable Service terms and conditions.

While us, as your IT Reseller and the Service Provider, aim to meet all proposed Service Levels, there may be occasions where performance falls short of circumstances outside of our direct control as outlined in the Service Constraints and Outage and Maintenance Management sessions of this document

In case of a failure from Service Provider on achieving the agreed SLAs, as your IT Reseller we will focus on addressing the issue with Assured Data Protection (ADP) and providing you with clear answers and, when applicable, formal root cause analysis. We will also work collaboratively to ensure that a Service Improvement Plan is put in place and, if necessary, apply any change to prevent the failure from happening again in the future.

We are confident that this approach helps us maintain a strong and transparent partnership with our clients and service partner, keeping the service reliable, issues visible and improvement actions transparent.

4. Provision of the service

Customer Responsibilities

To deliver the best service and guarantee efficiency on the Service implementation and consistent service delivery, we operate under a shared-responsibility model, where all parties contribute and work in partnership during the lifetime of your contract. As our client, for service delivery effectiveness, we kindly ask your collaboration on:

- Providing the most accurate information during all phases of the Service Delivery
- Providing complete current infrastructure details
- Promptly notifying us of any significant business and technical changes that may affect the Service performance
- Providing timely responses to the Service Provider queries, incident responses and approval requests
- Adhering to agreed change-management processes, including approvals, lead times and risk assessments
- Submitting requests using approved channels
- Participating in Services Reviews
- Honouring contractual payment terms

It is expected that the client is aware of some responsibilities beforehand which we have outlined here:

The Subscriber shall at its own expense supply ADP with all necessary Documents or other materials, and all necessary data or other information relating to the Services and any access to the Subscribers software and systems needed by ADP to deliver the Services. Such supply/access shall be provided, within sufficient time to enable ADP to provide the Services in accordance with the Contract.

The Subscriber shall ensure the accuracy of all Input Material. The Subscriber has all licenses and consents necessary for ADP to provide the Service.

The Subscriber shall be solely responsible for retaining and maintaining the security of any password supplied by ADP for the use of the Services; and all access and use of the Services made via the Subscribers account.

The Subscriber will always keep the Equipment (unless agreed otherwise) at the Premises detailed in the Equipment Document. The Subscriber will allow ADP (or such alternative third party as it nominates) access to the Premises to deliver, install and where requested (on reasonable notice at reasonable times except in an emergency where no notice will be required) to maintain the Equipment.

The Subscriber will not try to maintain the Equipment and/or allow any third party other than ADP to do so [In the event that the Equipment is damaged in any way (except for fair wear and tear) or stolen the Subscriber will pay ADP the full cost of repair and/or replacement as appropriate.] The Subscriber grants a license to the Premises (or any alternative premises where the Equipment is held)

to allow ADP (or its agent) to enter such Premises at any time in the event that this Contract is terminated, and/or the Subscriber goes into liquidation, makes a voluntary arrangement with its creditors, has a receiver or administrator appointed, cannot pay its debts when they fall due or ADP reasonably believes that any of the above may occur.

Detailed Service Terms and Conditions, including the Contractual Customer Responsibilities, will be addressed in the Service Agreements.

Technical Requirements and Client-Side Requirements

To determine the details about the exact technical and client-side requirements to deliver the service, it is essential that we have a full understanding of your current environment, operational needs and challenges you may be facing. This initial assessment will help us to guarantee the correct application of the Infrastructure as a Service and VM as a Service solution. Therefore, many of the technical requirements and client-side requirements will be discussed prior to an order being placed, but also during the onboarding and implementation stages, where all parties will work together to refine connectivity, security, access and workloads considerations. All requirements discussed prior to the order being placed shall be documented in the Order form and agreed between the parties. We consider that this approach ensures that the technical prerequisites are mapped out accurately and are aligned to the customer needs and expectations.

After-sales Account Management

As the IT Reseller, we are not only committed to offering the best solution but also to build strong relationships with our clients, working with you closely, not only during the initial phase of the project but also after the Service is delivered and implemented. This is pivotal to us, as a Company, to work with you on a full end to end service and make sure your expectations regarding the Service are met during the whole lifetime of your service. Unlike some specialist integrators, we are not just about selling a product, we are more interested in providing the right solution and we are committed to our customer's satisfaction.

As part of your service, you will have a designated Account Manager that will work closely with you on period reviews of our environment and will guarantee that you are being offered the most suitable solution/ service. You will also count with a Service Delivery Team that will liaise with you and the Service Provider on a regular basis, addressing all aspects of your service delivery and serving as your advocate to all your related service matters.

Termination Process

The service will commence on the service start date agreed and shall be for the minimum term also agreed beforehand. Service shall continue under the agreed terms and conditions for further terms of one year each one starting from the relevant anniversary of the commencement date of the Contract (each a "Renewal Term").

Customer shall be entitled to terminate the Contract at any time by giving not less than three months' written notice to ADP such notice only to expire at 12 midnight on the last day of the Minimum Term or relevant Renewal Term as applicable.

Either party may (without limiting any other remedy) at any time terminate the Contract by giving written notice to the other, if the other commits any material breach of the Contract and (if capable of remedy) fails to remedy the breach within 30 days after being required by written notice to do so, or if the other goes into liquidation, makes a voluntary arrangement with its creditors or has a receiver or administrator appointed.

Effect of Termination

Upon termination of the Contract, customer's access to store additional data under the Services shall cease immediately and its access to any data already stored as part of the Services shall be permanently terminated upon 7 days' notice from ADP; if termination is other than in accordance with the standard termination process or as a result of a breach by ADP, then the customer will be liable for ADP's Standard Charges for the remainder of the term of the Contract; and the Subscriber shall pay to ADP all sums due under and related to the Contract.

Detailed Service Terms and Conditions, including the Termination, will be addressed in the Service Agreements.

5. Our experience

Case Study

Managed Backup and DR for a Large UK Education Organisation

A major UK education institution with over 450 servers, 35,000 users—a mix of students, academic staff, and administrative teams—faced escalating security risks across a highly distributed, multi-site environment. With critical teaching, research, and operational services at stake, the organisation required a modern approach to protecting their hybrid cloud and on premise workloads against the risk of data loss or cyber attack that met with their strategic operating model, and operate within tight public-sector budget constraints.

Challenges

- Complex, multi-site estate: The organisation operated multiple campuses and satellite locations, each with differing levels of maturity and legacy infrastructure.
- Highly sensitive data: Research outputs, student records, financial information, and regulated datasets demanded robust protection and rapid incident response.
- Limited visibility: Fragmented tooling and inconsistent logging meant the internal team lacked a unified view of the protected data landscape or if there were issues with data sovereignty and origination.
- Public-sector budget pressures: The institution needed a predictable, fixed-cost model that avoided unexpected overages or consumption-based volatility.
- Varied service needs: The solution needed to provide the same level of protection and SLA regardless of where the University placed the data. Over the lifetime of the contract data will move to and from private and public clouds and the operating model must protect data and provide recovery regardless of location. 24/7 monitoring for critical systems if potential data encryption or movement was observed.

Solution

- The organisation partnered with a specialist Backup and Disaster Recovery provider to deploy a fully managed Backup, Replication and Disaster Recovery Solution built around the following capabilities:
- Unified visibility: Integration with existing services like VMWare and Microsoft Azure created a single, correlated view of activity across the entire environment.
- Technology-agnostic approach: The service was designed to work with the institution's current investments, regardless of hardware, platform or location the solution integrates seamlessly avoiding costly rip-and-replace programmes.
- Predictable pricing: A fixed annual subscription model aligned with public-sector budgeting cycles, ensuring transparency and long-term affordability.
- Noise reduction: Automated and human triage enrichment filtered out false positives, the managed service would ensure backups completed and ensure that only genuine, high-fidelity alerts were escalated to IT teams.

- Customisable service levels: Tailored SLAs allowed the organisation to match response times and operating hours to the criticality of each system or service, optimising service delivery & resources without compromising protection.
- Multi-site coverage: The SOC provided consistent monitoring and response across all campuses, regardless of local infrastructure differences.

Clients

Who we do it for – Public Sector/Charities



Who we do it for - Commercial



Contact Details

For any questions regarding this offer, please send an email to ***gcloud@ng-it.co.uk*** and we will respond as quickly as possible to assist with your request.