

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	4
Overview of the G-Cloud Service	6
Associated Services	16
2. Data Protection	17
Information Assurance	17
Data Back-Up and Restoration	17
Business continuity statement/plan	18
Privacy by Design	19
3. Using the service	20
Ordering and Invoicing	20
Availability of Trial Service	20
On-Boarding, Off-Boarding, Service Migration, Scope etc.	20
Training	21
Service Management	22
Service Constraints	22
Service Levels	23
Outage and Maintenance Management	24
Financial Recompense Model for not Meeting Service Levels	24
4. Provision of the service	25
Customer Responsibilities	25
Technical Requirements and Client-Side Requirements	25
After-sales Account Management	26
Termination Process	26
5. Our experience	28
Case Study	28
Clients	30
Contact Details	30

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 11:11 as our key partner for Managed

Cloud, Backup, Disaster Recover, Connectivity and Security. 11:11 Systems is a managed infrastructure solutions provider that empowers customers to modernise, protect, and manage mission-critical applications and data, leveraging 11:11's resilient cloud platform, making them the ideal partner for our customers to engage and trust as the service provider for this proposed platform.

NG-IT are 11:11's only UK Platinum partner, which further highlights the strong success we have had as a partnership. The following proposal outlines how NG-IT will deliver the 11:11 service. NG-IT's Infrastructure as a Service is powered by 11:11, the leaders in platform and managed cloud. Backed by a 100% SLA guarantee and delivered in a simple, predictable consumption-based cost model.

11:11's award-winning suite of solutions and services ensures that customer applications and data are always running, accessible, and protected.

Backup as a Service, Disaster Recovery (DR) as a Service is essentially Backup and DR as a service that provides a zero-trust data protection platform across data and applications on premises or in the cloud. Ransomware detection and remediation, eliminating backup software integrating data orchestration, catalogue management, and 'deduplicated' storage into a single fabric.

11:11 delivers increased performance and savings to organisations while freeing up IT resources to focus on their core business. They count with strategic partnerships with industry leaders such as Veeam, VMware, HPE, Zerto, and Cohesity provide customers with best-in-class solutions to further power and fortify their applications, data, and environments.



Single point of management for all services using the award winning easy to use web console. The console provides management, monitoring, control, and visibility across all 11:11 services including public and private clouds, data protection, and disaster recovery. With the console, you can:

- Monitor cloud storage usage
- Receive utilisation alerts
- Proactively add and resize resources on demand
- Gain insight into billing information



The 11:11 Systems management team brings together years of leadership delivering an integrated and unified cloud, connectivity, and security experience.

Backup as a Service

11:11 Cloud Backup gives you a secure, offsite backup and the added reassurance of flexible, all-inclusive cloud storage for your growing business. Utilising Veeam or Cohesity technology, our integrated options give you cloud backup with less complexity, cost, and administration requirements.

Backing up data to traditional equipment can be difficult. Tape backup is challenging and labour intensive. Adding storage nodes to disk backup servers can likewise prove problematic, whether you're worrying about the possibility of disk failure, or the costs of continually adding storage. 11:11 Cloud Backup resolves these challenges with high performance, flexibility, and scalability.

As a fully managed service, we will monitor and ensure any backup failures are resolved. We will even perform data recovery for you should you choose not to do it yourself using our easy-to-use management console.



**3-2-1
Strategy**

3



**Copies of
your data**

2



**Media
types**

1



**Copy
Offsite**

Key Benefits

Cloud backup is offsite - Critically, cloud backup is completely physically removed from the organization's location. This protects the data from any events tied to campus, including hardware failures, natural disasters, theft, or human error.

It supports the 3-2-1 strategy - Backup best practices dictate that businesses keep three copies of their data, on at least two different types of media, with one instance in the cloud

It can fill holes in your infrastructure - Cloud backup can extend beyond standard data storage to meet additional needs.

It outperforms tape - Tape, one of the most common backup storage media, is notoriously weak. Tape suffers from tape rot (not to mention the manual effort and uncertainty involved with third-party storage facilities), while cloud backup enables you to trust that your data will be available if and when you need it.

It's always accessible. Cloud backups can be accessed any time, anywhere, for dramatically 6 increased flexibility over when, where, and how data can be extracted.

It requires zero maintenance. With cloud backup, you are no longer in the business of feeding and caring for hard drives, storage media, servers and more. That means your team has more time and energy to dedicate to value-add activities.

It improves compliance. Leading cloud backup providers offer fully compliant backup services 8 that ensure that your data follows all applicable rules and regulations.

It's cost effective. Cloud backup allows companies to scale their backup storage elastically, so you only pay for what you use instead of maintaining physical storage solutions that may not always be required.

It's more secure. Unlike internal IT teams, cloud service providers specialize in keeping data secure. Organizations can reap the benefits of best-in-class security protocols without having to provide it in-house

Disaster Recovery as a Service

All 11:11 DRaaS solutions include:



Dedicated compliance team

To help make the transition to cloud easier from a compliance standpoint, and to help tackle your geographic and/or industry-specific concerns, 11:11 maintains an in-house [compliance](#) team that is ready to support you.



Multi-layered security

11:11 DRaaS includes managed, purpose-selected [security](#) across your recovery environment. 11:11 security is directly integrated into the 11:11 Cloud Console to provide for ease of use, transparency, and control.



Network support services

11:11 offers Network Support services and multi-cloud connectivity to give you the flexibility to maintain and preserve your existing network policies and investments to ensure your workloads can communicate.



Strategy and design.

11:11 provides cloud planning and design services leveraging [11:11 Catalyst](#), our environment assessment tool, used to model and ensure application performance requirements are met prior to DRaaS deployment.



Industry-leading technology and experience

We are consistently recognized as an industry leader in disaster recovery, including in Gartner's Magic Quadrant for Disaster Recovery as a Service (DRaaS).



Flexible and individual design

11:11 DRaaS enables you to replicate all your IT workloads and applications from public or private clouds, and for both virtual and physical environments, to our proven, VMware-based cloud platform.



Unified cloud management

The [11:11 Cloud Console](#) is our award-winning, unified management platform. The console provides management, control, and visibility across all 11:11 services including public and private clouds, data protection, and disaster recovery.



VMware-based technology

11:11 DRaaS, like all 11:11 services, is built on [proven technology](#) from VMware. With VMware, 11:11 enables you to quickly failover and failback during and after the disaster event without having to convert your applications to a new operating format.



Seamless onboarding and deployment

To help you simplify your move to the cloud, 11:11 takes a comprehensive approach to migrating data by including a dedicated project manager and cloud services engineers to ensure that data is migrated safely and securely to the 11:11 Cloud Platform.



Included customer support

Our 24x7x365 [support team](#) is available by phone, email and ticketing system to address your questions. That begins with our seamless onboarding process through to your ongoing operations – for questions large and small.

All organisation's disaster recovery plans are different. 11:11 experienced disaster recovery engineers will help guide you through designing and implementing your DR strategy, from first click to failover. With 11:11 DRaaS, you can replicate all your IT workloads and applications to our proven, VMware-based cloud platform. 11:11 DRaaS provides:

- **“Many to many” data replication** - Flexible recovery options include the ability to failover to 11:11 Public or Private Cloud and to/from virtual or physical environments.
- **Custom performance options** - We'll work with you to tailor solutions to your business and application needs — including RTOs and RPOs that can be set to minutes or even seconds.
- **Built-in security and data protection** - Options can be customised based on industry and geographic requirements.
- **Support for legacy systems** - Whether it's a specific hardware asset that's critical to your infrastructure, or one that's simply not worth re-factoring for the cloud, 11:11 colocation options can help support your cloud expansion.
- **Global data centre footprints** - Available in all geographies where 11:11 Systems operates.

When disaster strikes, you need the ability and confidence to recover as fast and as easily as possible. 11:11 DRaaS will get you fully integrated disaster recovery management within the 11:11 Cloud Console. 11:11 Cloud Console provides management, control, and visibility across 11:11 services, including public and private clouds, data protection, and disaster recovery:

- Unified management across all applications, services, and resources such as compute, storage and networking.
- Integration with leading solutions from VMware, Veeam, and Zerto, enabling a seamless experience between software providers

- Ability to easily deploy disaster recovery, production applications, and hybrid cloud environments and manage from a single view
- Ability to test your 11:11 DRaaS for both Veeam and Zerto environments directly from the Console, without disruption
- Comprehensive security and compliance integrated directly into the console
- Detailed performance, security, compliance, and billing information
- Ability to restore from backups, and replicate data to other 11:11 clouds

Easy Recovery Options with DRaaS Runbooks

11:11 DRaaS Runbooks allow your organisation to build individual Recovery Groups for specific applications, workloads, or virtual machines. Combine your recovery strategies into a single, unified entity to simplify management of your DR environment when testing failover or performing a live failover of your environment.

11:11 DRaaS Runbooks allow you to:

- Configure recovery to include systems that need to failover at the same time, even if they are in separate Recovery Groups
- Create DR presets with multiple configurations of Recovery Groups that you can choose as needed, rather than having to manage them individually when time is critical
- Test how your environment will perform during an actual failover
- Provides a central repository to easily troubleshoot an issue, or quickly locate and resolve a point of failure
- Troubleshoot an issue, or quickly locate and resolve a point of failure from a central repository
- Report on the full environment or on a per-Recovery Group basis, and provide a centralized view of the entire failover process from start to finish
- 11:11 provides Runbook assistance every step of the way, including failover.

Fully Managed Disaster Recovery

11:11 Managed Recovery is a fully managed program that frees up your team to focus on what matters most to your business.

With Managed Recovery, you will count with a team of experts:

- Work with your team to develop recovery procedures
- Assess your environment and prioritize critical applications
- Manage recovery during testing and following a disaster
- Provide comprehensive reports and reviews

Defense in Depth

11:11 DRaaS includes managed, purpose-selected security across your recovery environment. The 11:11 Cloud Console provides visibility into your security so you can ensure your data is safe. 11:11 security includes:

- RBAC (Role Based Access Control)
- Two-factor authentication
- Available VM encryption
- Vulnerability scanning
- SSL-VPN
- Antivirus/anti-malware
- Integrity monitoring
- Deep-packet inspection for intrusion detection and prevention
- Detailed firewall and log events
- Storage-based encryption enabling encryption at-rest

Through the management console, you also have access to on-demand reporting and alerting for security and compliance, making it easier to complete audits.

Compliance Requirements

All of 11:11 solutions and services are supported by our certified in-house compliance team. The 11:11 compliance team is dedicated to ensuring our services meet regulatory requirements around the world, and we strive to meet industry best-practice standards. Our compliance team is available to:

- Answer your due diligence questions
- Provide compliance & security documentation
- Assist with audit information and guidance

Another way we meet your compliance needs and demonstrate strong security controls is through detailed reports provided directly in the 11:11 Cloud Console. With reports on malware detection, event histories and more presented in an easily consumable graphical layout, you can be confident you'll have the information to support your audit.

Network and Flexibility

One of the challenges of moving to the cloud, or adopting a multi-cloud strategy, is the need for end user access during a failover event. The ability to communicate with other networks or applications can be critical for success. To keep communication consistent between workloads, 11:11 allows you to preserve your existing network policies and investments.

This provides network flexibility and allows you to proceed with your existing corporate network strategy without disruption.

11:11's network flexibility gives you control of your existing and future application environments:

- Familiar and integrated VMware-based network services via VMware NSX for security segmentation and access (IPsec/SSL VPN), managed through the 11:11 Cloud Console
- “Bring your own” options including physical/virtual network appliances, as well as flexible carrier and circuit options (MPLS/VPLS, direct circuit) for global connectivity
- Megaport/SD-WAN and our high throughput circuits for performance and integration purposes
- Unlimited, unthrottled, and highly resilient bandwidth to maximize uptime following a disaster

End-to-end Protection for Critical Workloads

In the event of a disaster, your DRaaS solution effectively becomes your production platform. For this reason, it needs the same performance, security, and data protection as your primary environment. So that your DRaaS solution is ready for production, when necessary, 11:11 Systems includes built-in data protection services managed by the 11:11 Cloud Console. This adds another layer of confidence that data is protected, and secure in the event of hardware failure or other internal or external events.

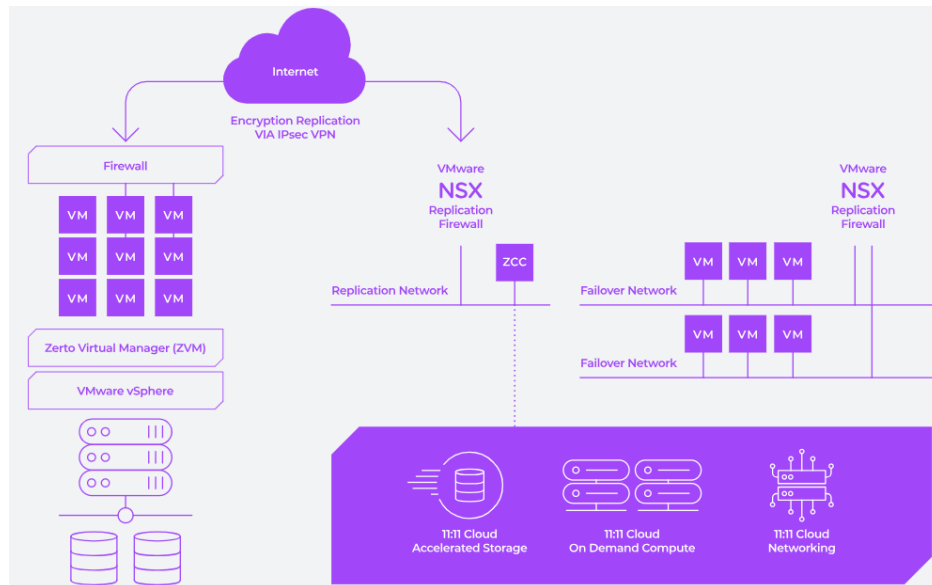
Zerto for DR

11:11 DRaaS for Zerto provides you with the ability to reduce downtime and customise your IT recovery. Easily replicate your mission-critical virtual machines (VMs) to the secure 11:11 Cloud through our seamless integration with your on-premises, VMware-based environment and Zerto's industry-leading technology.

With customised runbooks, 11:11 DRaaS for Zerto helps you orchestrate failover and failback. Enjoy optimised recovery time objectives (RTOs) and near instantaneous recovery point objectives (RPOs), along with network flexibility, straightforward pricing, and unified management of your DR environment.

Traditionally, disaster recovery means recovering data before accessing systems whereas with 11:11 DRaaS for Zerto, a journal keeps a historical record of changes made to VMs over the past 30 days. This capability gives users the ability to “rewind” time to before disaster strikes — including data loss, ransomware, and human error. During failover, every end user request is analysed to determine if the response should be returned directly from the virtual machine or from the journal, whichever is more current. This process continues until the failover is complete.

Ultimately, customers benefit from sub 10 second RPOs and aggressive RTO for speedy recovery (orchestrated recovery). In addition, failover network and integration capabilities allow end users to seamlessly access data during and after a failover event.



Key Benefits

- Centralised management and reporting via the award-winning 11:11 Cloud Console
- Orchestrated failover and failback
- Integrated Zerto replication
- Simplified DR management with Runbook Recovery Groups
- Available planning, design, and management services to address organisational requirements
- Dedicated compliance support to address geographic and industry regulations
- Included 24x7x365 customer support

11:11 DRaaS for Zerto provides optimised replication and rapid recovery. Zerto's continuous replication technology cuts RPOs to seconds and RTOs are nearly instantaneous. The integrated Failover Wizard also delivers alerts and reports from the 11:11 Cloud Console to help you through the failover process.

Veeam for DR

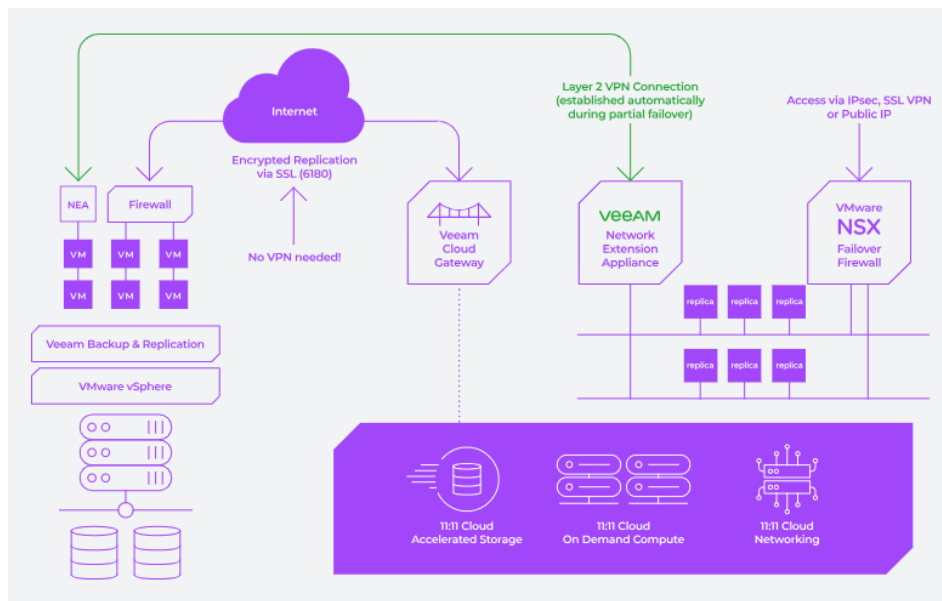
11:11 DRaaS for Veeam integrates the leading solution for backup, disaster recovery, and hyper-availability with the 11:11 Cloud. This deep integration with your on-premises Veeam solution provides you with quick recovery following unexpected events and with central, unified management of your DR environment — onsite and in the cloud.

With years of experience and industry-recognised leadership in disaster recovery as a service (DRaaS), 11:11 Systems makes deployment, testing, and failover in the cloud simple and straightforward.

11:11 DRaaS utilizes efficient technologies to ensure failover and failback meet your business and application-specific requirements. 11:11 DRaaS for Veeam comes with:

- Fast replication. Integrated network compression enables both closer Recovery Points and reduced WAN bandwidth requirements.
- Existing network compatibility. 11:11 DRaaS can be configured with recovery networks that match your internal private network range(s), yielding a more aggressive RTO with no reconfiguration of VMs.

- DNS failover. Disaster recovery management is simplified with the integration of DNS management into the cloud console. DNS management can be performed from the same location in which you manage cloud resources and disaster recovery. Easily manage your public IP blocks, DNS zones, records, and make updates to all your DNS records in the event of a failover through an easy-to-use search and edit tool within the console.
- Storage options. 11:11 supports replication of VMware virtual machines and is storage-agnostic with two tiers of encrypted storage to ensure all key workloads are protected.
- SSAE 16/ISO 27001 certified Tier III data centres around the globe. In addition to global data centres, 11:11 also maintains connections to more than 500 IP providers to ensure your data is secure, fixed within your chosen country, and fails over rapidly.



Key Benefits

- Centralised management and reporting via the award-winning 11:11 Cloud Console
- Integrated Veeam replication and failover plan orchestration for recovery in the cloud
- Available planning and design services to address organisational requirements
- Dedicated compliance support to address geographic and industry regulations
- Included 24x7x365 customer support
- On-demand, fully managed failover option available for added support

As a fully managed service, experts will be there, from design to implementation, from deployment to testing. The 11:11 Cloud Console also allows you to test your DR plan at any time, without disrupting normal operations. You can also expect recovery time in minutes during failover or failback following a disaster.

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

30-day free trial Service is available at no risk and upon request. This can give you first-hand look on how the BaaS and DRaaS looks like, and you will get access to the same core features as a regular IaaS subscription. Please contact gcloud@ng-it.co.uk for more details about the 30-day free Trial.

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

Once the design and planning are agreed 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 the IT Reseller, NG-IT will assign a dedicated Service Delivery Coordinator, that will look after your contract and liaise periodically with the Service Provider during the whole lifetime of your service. At this point, your dedicated Service Delivery Coordinator will make sure that the Service Provider will follow the steps outlined in their onboarding process.

The dedicated Project Manager assigned by the Service Provider and its team of cloud services engineers will help you with the migration and deployment process. They will support you on the workload deployment (VMs, storage, networking) and help you configure the cloud environment.

The onboarding usually involves the following steps:

- Infrastructure design, that will define sizing, storage profiles and networks
- Security Settings
- Compliance
- Backup

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

Week 0-1 – Engagement, Scoping and Requirements definition

- Formal engagement between your organisation, 11:11 Project Manager and Cloud Engineering Teams, and NG-IT Service Delivery Team
- Requirements validation
 - ✓ Capacity planning
 - ✓ Compliance obligation
 - ✓ Backup and disaster recovery expectations (when applicable)
 - ✓ Connectivity, security baselines and support models
 - ✓ Review of existing workloads, dependencies and integration points

Week 2 – Environment Build and Access Provision

- Service Provider will provision the tenant environment within their Cloud Platform by establishing:
 - ✓ Identity and access controls
 - ✓ Networks
 - ✓ Segmentation
 - ✓ Storage tiers
 - ✓ Resource pools

As an output from this phase, it is expected that you get access to the 11:11 Cloud Console and that the test connectivity is established and validated.

Week 3-4 – Pilot Migration and Functionality testing

- Controlled Migration to confirm that the environment supports workload and security expectations. This stage involves:
 - ✓ Migration of non-critical VM
 - ✓ Backup Validation
 - ✓ Process restoration
 - ✓ Testing monitoring and alerting

Week 5-6 – Full Migration and Optimisation

- Workloads are prioritised by risk, criticality and technical complexity and moved into full migration

Week 7-8 – Go Live, Knowledge Transfer and Service Handover

- Transition into Business-as-Usual operation
- 11:11 provide formal Knowledge transfer, documentation, escalation pathways and guidance on cost optimisation and capacity planning
- Disaster Recovery and backup policies are reviewed when applicable

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. Service Provider will be responsible for the deployment and migration of your virtual servers and contracts are typically a minimum 3 years, ideally 5 years.

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 11:11 Cloud Console 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, 11:11 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 11:11 Cloud Console, either via training materials or walk-throughs, to ensure that you have all necessary information to navigate through 11:11 with confidence. You will also have access to Webinars and Education Sessions, and an extensive learning content library available on the customer portal.

A 24x7 support team will be available and can be contact via email, phone or ticket not only to assist you with incidents and technical related issues, but by 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

Even though Provider's Self-Service Infrastructure guarantees 100% availability of the service, we also take into consideration the fact that 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.

For all services, the Provider's Infrastructure will be deemed unavailable if (a) the Customer can neither transmit nor receive data to or from the Provider's Infrastructure (whereby inability is confirmed by way of Customer documentation that verifies said inability is due to an issue with the Provider's equipment) and (b) such inability has been communicated to the Provider in sufficient detail to enable the Provider to open a case in respect thereof. The Provider's Infrastructure shall not be deemed unavailable (without limitation) in the event of any of the following:

Any circumstances whatsoever which are not within the reasonable control of Provider or its subcontractor(s);

Breach of the Agreement, the Services Schedule, the Order or SLA and SLO by Customer.

Force Majeure events.

Virus activity and hacking attempts.

In accordance with a court order or any requirements of any authority or other competent local authority.

Periods of scheduled or emergency maintenance on Provider's Infrastructure of which the Customer has been notified.

Failure or malfunction of the Customer's or End-User's connection to the Provider Network (e.g. via the public Internet or the Customer's own network) or related problem beyond the Provider's Network Demarcation Point.

Failure or malfunction of equipment, software, or other technology not owned or controlled by Provider.

Failure to comply with any terms of Provider's current Acceptable Use Policy.

Failure or malfunction caused by Customer over-provisioning Reserved Resources in excess of the specifications set out on the Order.

A malfunction that results from inconsistencies in the environment or unavailability that result from changes in the Customer's source environment, including, but not limited to, either intentional or accidental connection or disconnections to the environment.

A malfunction that results from the negligence, or intentional acts or omissions of Customer or its employees, agents or any third party.

A malfunction that results from anyone gaining access to the Cloud Resources by means of Customer's passwords or equipment.

Any failure to restore an environment from a Cloud Backup file chain in the Provider's cloud services (Secure Cloud Backup only); or

Unavailability of any management console or APIs.

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

Provider's Self-Service Infrastructure guarantees 100% availability of Service.

Response times are as follow:

Severity 1 - Production System Down - < 15 mins

Severity 2 - System Impaired - < 2 business hours

Severity 3- General Guidance - < 24 business hours

Severity 4 - Change request - < 8 business hours

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.

11:11 Systems publishes our most up-to-the-minute information on service availability on the 11:11 Status page. You will be able to check the page any time to get information about current Service Provider state or subscribe to an RSS feed to be notified of interruptions to each individual service.

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

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. The SLAs is an important way of measuring service quality rather than to trigger financial compensation, therefore, there is no financial credit available or refund.

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 11:11 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

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 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 Agreement commences upon its signing by the Parties (the "Effective Date") and, unless terminated earlier as provided in the Agreement, continues until no Orders have been in effect for at least one (1) year.

Each Order will commence on the Order Effective Date and continue for the initial period specified in such Order (such Order's "Initial Order Term"). Unless otherwise specified in an Order, such Order will renew automatically for successive one-year terms (each, a "Renewal Order Term") (the Initial Order Term and any Renewal Order Term, collectively the "Order Term"), unless (a) either Party to such Order provides the other Party with written notice of non-renewal at least sixty (60) days prior to any such renewal, in which event the Order will terminate on the final date of such Order's then-current Initial Order Term or Renewal Order Term, as applicable; or (b) such Order is otherwise terminated in accordance with the Service Agreement or the relevant Service Schedule.

Any Party may terminate the Service Agreement and any or all Orders if the other Party materially breaches the Service Agreement or an Order, and such breach is not cured within thirty (30) days after the non-breaching Party has provided the breaching Party written notice thereof. A Provider may immediately terminate the Service Agreement and any or all Orders if Customer fails to pay any Fees when due to such Provider and Customer does not cure such non-payment within ten (10) business days after Provider has provided Customer with notice of such failure to pay.

An Order may also be terminated under the Service Agreement:

By the applicable Providers by notice to Customer if such Provider's rights to use the data centre specified in such Order for the purposes contemplated by such Order terminate or expire for any reason;

By any Provider immediately if a Customer or any of its Affiliates or their agents, invitees, or employees enter any Provider's data centre with any firearms, illegal drugs, or alcohol or are engaging in any criminal activity, eavesdropping or foreign intelligence activities;

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

5. Our experience

Case Study

Managed Platform Services for a Large UK Public Sector Organisation

Overview

A UK Public Sector institution with over 2,000 users faced growing challenges around production, backup and disaster recovery platforms. Legacy technology, reduced internal resources, mounting pressures on local and hosted data centre facilities meant the organisation required managed platforms for some digital assets.

Challenges

- High hosting and IT costs
- Slow customer support response
- Inability to easily modernise and scale
- Lack of visibility and control
- Unsatisfactory performance
- Insufficient internal IT resources

Solution

The organisation partnered with NG-IT and 11:11 to provide next generation managed cloud platforms for critical digital services to provide:

- Significant savings on IT operations costs
- Increased ability to scale and modernise
- Faster and better customer service response
- Simplified management, configuration and setup
- Flexibility to easily change or upgrade environment as needed
- Commitment to meeting data sovereignty and compliance requirements
- Significant improvement in performance

A construction and infrastructure company are a leading UK construction and civil engineering company est. 1869, who designs, develops, builds, and preserves some of Britain's most iconic buildings, found themselves in a tricky situation where their storage support agreement was reaching expiry, and a solution needed to be found quickly. Working us, NG-IT, as their trust Provider, they identified IaaS as the next step in their IT journey, removing the pain points experienced with DC ownership, day-to-day management and staff time usage as the key drivers. As a Nimble and VMware user already, the client found 11:11 to be their preferred IaaS provider following our suggestion, for its VMware/ Nimble stack, overall service package, pricing model and single interface console, and finally, the impressive migration processes and timeframes for completion possible.

As a business who had suffered several outages, including fires and floods, it was also imperative for the business that their provider has a DR site available. As 11:11 are global leaders for DR, with 2 UK data centres to enable this requirement, 11:11 were quick again to meet the business's needs.

Solution Differentiators

- VMware, Cisco & Nimble 11:11 infrastructure aligned perfectly with client's current infrastructure
- 11:11 DRaaS capabilities proved advantageous for migration methods, Solution Provider were able to meet the very tight deadlines required to successfully move the customer into IaaS
- 11:11 cloud console provides one interface for all services, including IaaS, DRaaS, BaaS & 365
- Resource Pool & Right Sized pricing structure enabled 11:11 Infrastructure as a Service and VM as a Service to be cost effective and competitive over alternative options
- Reservation + Burst model created a scalable service for the client

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.