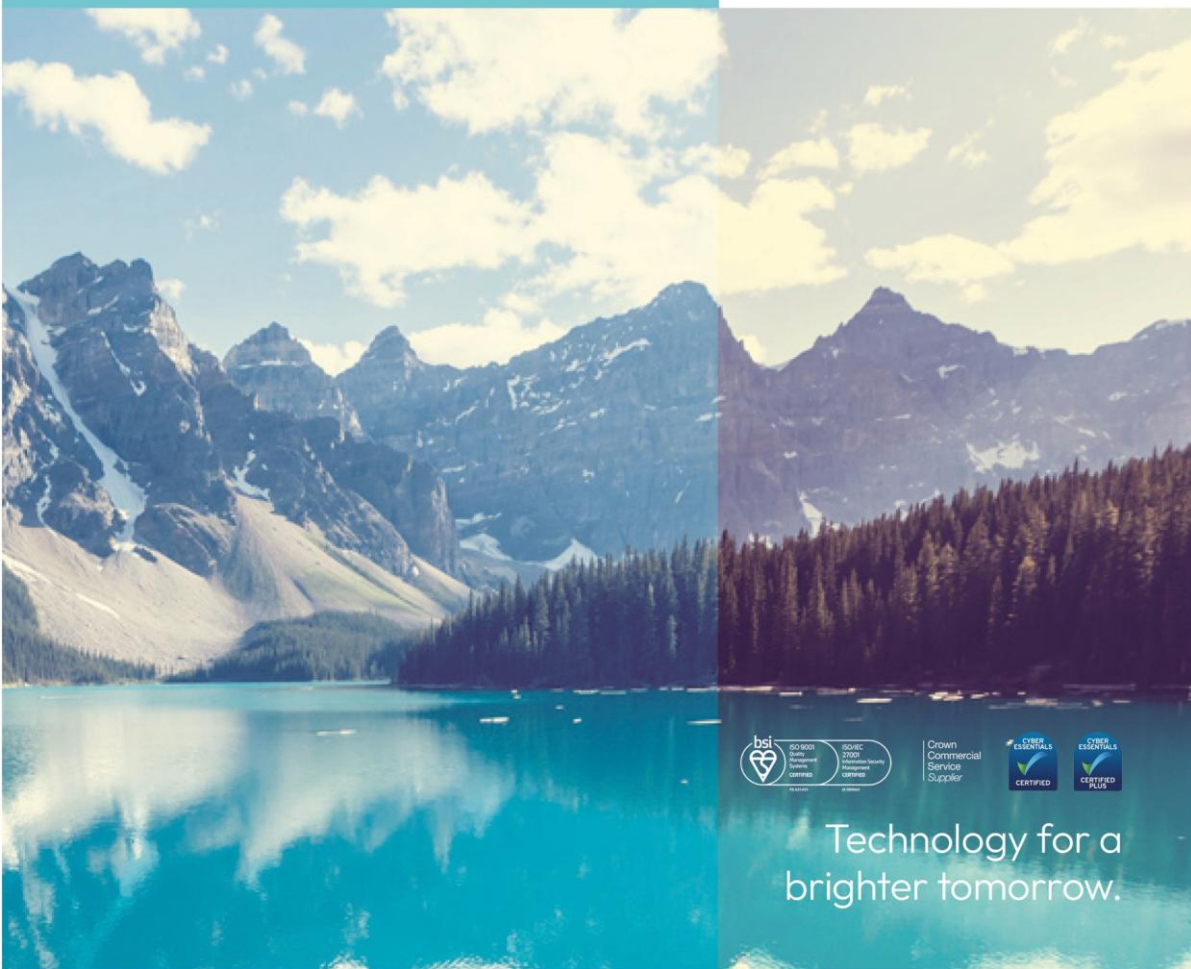




Managed Cloud backup & DraaS – Service Level Description



Crown
Commercial
Service
Supplier



Technology for a
brighter tomorrow.

©Copyright IT Professional Services Ltd. 2026

The Information contained in this document is the property of IT Professional Services Ltd.

The contents of this document must not be reproduced or disclosed wholly or in part or used for purposes other than that for which it is supplied without the prior written permission of IT Professional Services Ltd.

This document, or any information contained within it, must not be provided, or issued to any third party without the prior written consent of IT Professional Services Ltd.

Registered Office:

IT Professional Services Ltd
Angel House
Unit 5
Angel Park
Drum Industrial Estate
Chester-Le-Street
DH2 1AQ

<http://www.itps.co.uk>

Contents

1.0	Reference Number	Error! Bookmark not defined.
2.0	Detailed Description	5
3.0	Billing	6
4.0	Business Benefits.....	7
5.0	Scope of Service	7
6.0	Service Hours.....	7
7.0	Standard Service Components	8
8.0	Service Exclusions	8
9.0	Toolsets	9
10.0	Terms.....	9
11.0	Appendix.....	10

Document Control

DOCUMENT TYPE:	SERVICE LEVEL DEFINITION & DESCRIPTION
DOCUMENT CLASSIFICATION:	RESTRICTED
DOCUMENT VERSION:	V1.2
DOCUMENT OWNER:	LEE NEVIN & STUART GIBB
CREATION DATE:	3rd JANURAY 2026
PRODUCT OFFERING COMPONENT(S)	CLOUD & DATA CENTRE INFRASTRUCTURE [OFFERING] [COMPONENT]

Revision History

DATE	VERSION NUMBER	AUTHOR / AMENDED BY	DESCRIPTION OF AMENDMENTS
03/01/2023	1.0	Lee Nevin & Stuart Gibb	
28/09/2023	1.2	Lee Nevin	Rebranded
03/01/2026	1.3	Stuart Gibb	

Distribution

NAME	ROLE	CONTACT NUMBERS

Document Review

This document will be reviewed and updated, when necessary, as stipulated below:

- ✓ As required to correct or enhance the content.
- ✓ Following changes to the ITIL or ISO quality systems standard as defined by ITPS.
- ✓ Following any organisation changes or restructuring.
- ✓ No longer than 12 months after the previous approval date.

Managed Cloud Backup

1.0 Detailed Description

This service provides a fully managed backup and recovery service (with encryption options) to all platforms for servers located inside and outside of ITPS data centres to a schedule and retention policy agreed with the client.

The services will be delivered by ITPS teams based in Chester Le Street and utilises several toolsets as dictated by the particular client.

Backup data held in Acronis data centres.

Backup data is encrypted in transit using HTTPS and encrypted at REST using AES256.

No tape backups are performed with recovery points being held on disk, performed by Acronis.

Retention must be defined by the client on a per server basis to ensure all data retention requirements are met for the business.

Data will be restored to a destination agreed and provided by the customer.

Onboarding

Ensuring everything required to manage the account is set up and in place. Responsible teams include:

- Accounts
- IT Service Desk Management
- Data Centre Service Team
- Managed Service Team
- Field Engineer Team

Role	Step	Description
Accounts	1	When accounts process purchases and contracts to customers with maintenance elements, the accounts team create an on boarding ticket, they enter on to the system and subsequent automatic weekly reports alert the Service Desk Management by email.
ITPS Service Desk Management	2	The type/item of "On Boarding" creates tasks to steer the service team into specific activities to review the level of support required.
Accounts	3	The accounts team work with the salesman to resolve any issues from 2 and then relay the answers back to the service desk management.
ITPS Service Desk Management	4	This is an iterative process that concludes only when the Service Desk Management are happy that they have all the information they need to understand the service the customer purchased.
ITPS Service Desk Management	5	Once the support contract has been defined, the service team review the technical information to establish whether there is enough detail to deliver a technical service.
ITPS Service Desk Management	6	When the information has been collected, the info is updated on intranet and the relevant settings put in place such as the default contact used for that customer.
ITPS Service Desk Management	7	The customer is sent our standard call logging information, which describes how they raise support issues and also how to escalate a matter if required.
ITPS Service Desk Management	8	Finally, the new customer tasks checklist is completed and the ticket closed.

In addition to the above, to ensure the backup service meets the customers' needs, onboarding will also consist of:

- Defining a list of objects to be protected
- Creation of Cloud resource for recovery
- Configuration of replication toolset
- Perform initial offline tests

2.0 Billing

Price is calculated per TB of consumed backup storage at the start of the contract and reviewed monthly.

Commented [LN1]: Storage reviewed monthly not annually

Per TB is based on raw data.

3.0 Business Benefits

- No need to become experts in backup software and worry if it's been configured correctly. Allow ITPS experts to ensure customer data is backed up.
- Fully managed by ITPS. We'll not only set up the backup solution to customer requirements, but also proactively manage and monitor the success of the backups.
- ITPS will resolve any issues if a backup fails meaning customer has peace of mind.
- We'll provide daily status updates of backups so the customer has the confidence that everything is taken care of and working as expected.
- We have the knowledge and expertise to recover data quickly if required
- UK based experts allowing the customer to speak to a human if they ever need us.
- Data and systems backup and recovery of platforms hosted outside the central ITPS data centres
- Ability to retrieve lost or corrupt data required for client BAU
- Single point of ownership to take responsibility for back up service delivery
- Geographically dispersed server estates can have their backups managed remotely from a single location

4.0 Scope of Service

All virtual server platforms and their supported operating systems that are hosted and managed on client and ITPS sites.

5.0 Service Hours

Priority 1 Incidents	24 x 7 x 365
Priority 2, Priority 3, Priority 4, Change Management and General Enquiries.	08:00 – 18:00, Monday to Friday
Extended Support	Bespoke service priced and defined on an ad-hoc basis

6.0 Standard Service Components

- Backup of all hosted and managed servers within scope of the contract between ITPS its customer(s)
- Administration of centralised backup environments including:-
 - Day to day backup scheduling for all Windows and Unix/Linux servers that are hosted and managed in ITPS or client environments
 - Ensure client retention periods for data are satisfied
 - Test data restore procedures as part of scheduled Disaster Recovery tests
 - Monitor success rates and manage remedial actions as required
- Restore of client data on receipt of a service request via the Service Desk
- Support of client restoration where disaster recovery is invoked
- A data backup copy is held in two separate data centres, each with two copies

Reporting

Example report in Appendix.

Report will include:

- Success or failure of backup jobs.
- An overall average success rate against the number of listed jobs
- Further detail on any backups that have failed.
- Report will be in Microsoft Excel, HTML or any other format currently employed by ITPS
- Report will be delivered via email to the relevant client Service Manager
- The report will assume the backup status at the time of the shared backup window closing (07:00)

Report will not include:

- Detailed data relating to size or volume of data backed up
- Details of Drives or File systems that have been included or excluded within the backup
- Start/End times of each backup

7.0 Service Exclusions

- Operating System versions that are out of supplier support.
- OpenVMS
- Mainframes
- IBM AS400 or other midrange devices
- Oracle servers
- Desktop and laptop devices
- Handheld devices e.g. Blackberries
- Development environment hosted devices

8.0 Toolsets

- Acronis Server products for managing the storage systems
- Connectwise for managing Incidents, Problems and Changes
- Acronis providing a technical support knowledge base
- RDP and Putty providing a Virtual, Telnet and SSH Client for the Windows and Unix platforms

9.0 Terms

Scheduled Maintenance:

Clients are required to agree with a forward schedule of maintenance – within the Forward Schedule of Change (FSC). The service shall not be guaranteed during scheduled maintenance work. All scheduled maintenance work will be notified to you via the FSC. However where, in our reasonable opinion, an emergency situation exists, we also reserve the right to carry out emergency maintenance outside the normal notification period.

Termination:

We shall cease providing the service on termination of the contract.

10.0 Appendix

ITPS Backup Reports

Managed Backup Service Report :

Report for : Friday - 05_02_2023 Including Saturday and Sundays results as an overall combined percentage

Failed / Running Backups

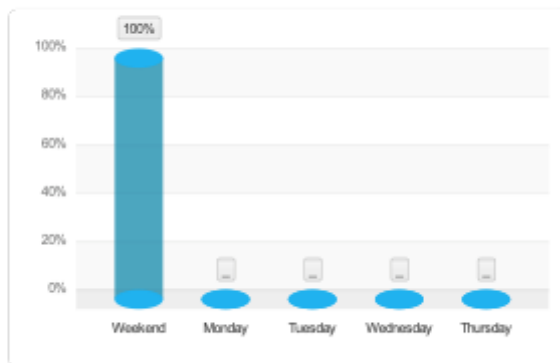
0%

Successful Backups

100%

Number of Servers Protected : 6

Week View



Graph: Daily Success (in percent)
(Weekend column includes last Friday's results as a consolidated view)

Failure Detail

Failed / Running Backups

Server Name	Result	Failure Reason	Resolution	Required Resource	# Concurrent Failures
-------------	--------	----------------	------------	-------------------	-----------------------

Disaster Recovery as a Service

11.0 Detailed Description

ITPS operate, deliver and support a range of Business Continuity services for and on behalf of our clients, this particular document concentrates on Disaster Recovery. ITPS operate the same Business Continuity facilities, products and services for themselves.

If a customer loses a site or data due to an unexpected event, ITPS can invoke a procedure to recover the critical data to enable the customer to continue working.

Recovery would take place into an ITPS provided Cloud location that has been pre-configured and defined.

This would be considered IT continuity that would feed into wider business continuity.

This covers the DRaaS service using Zerto as a solution.

Onboarding

Ensuring everything required to manage the account is set up and in place.

Responsible teams include:

- Accounts
- IT Service Desk Management
- Data Centre Service Team
- Managed Service Team
- Field Engineer Team

Role	Step	Description
Accounts	1	When accounts process purchases and contracts to customers with maintenance elements, the accounts team create an on boarding ticket, they enter on to the system and subsequent automatic weekly reports alert the Service Desk Management by email.
ITPS Service Desk Management	2	The type/item of "On Boarding" creates tasks to steer the service team into specific activities to review the level of support required.
Accounts	3	The accounts team work with the salesman to resolve any issues from 2 and then relay the answers back to the service desk management.
ITPS Service Desk Management	4	This is an iterative process that concludes only when the Service Desk Management are happy that they have all the information they need to understand the service the customer purchased.
ITPS Service Desk Management	5	Once the support contract has been defined, the service team review the technical information to establish whether there is enough detail to deliver a technical service.
ITPS Service Desk Management	6	When the information has been collected, the info is updated on intranet and the relevant settings put in place such as the default contact used for that customer.
ITPS Service Desk Management	7	The customer is sent our standard call logging information, which describes how they raise support issues and also how to escalate a matter if required.
ITPS Service Desk Management	8	Finally, the new customer tasks checklist is completed and the ticket closed.

In addition to the above, to ensure the disaster recovery service meets the customers' needs, onboarding will also consist of:

- Defining a list of objects to be protected
 - Size
 - Memory
 - Number of VMs
 - Failover priority
- Creation of Cloud resource for recovery
- Configuration of replication toolset
- Perform initial offline tests

Ongoing

Monthly activity will consist of:

- Ensuring Cloud environment remains available in the event of a disaster.
- Management of any issues raised that may require invoking disaster recovery solution.

12.0 Business Benefits

- Allow ITPS experts to managed and oversee the set up and testing of the solution
- Know that the business can be back up and running quickly in the event of a disaster
- UK based data centres and support
- Cost effective solution to mitigate risk and reduce any business impact

13.0 Scope

- Identification of what's included for disaster recovery.
- Data Centre application and data hosting services.
- Backup services.
- Disaster Recovery testing.
- Support and Maintenance services.

14.0 Service Hours

Priority 1 Incidents	24 x 7 x 365
Priority 2, Priority 3, Priority 4, Change Management and General Enquiries.	08:00 – 18:00, Monday to Friday
Extended Support	Bespoke service priced and defined on an ad-hoc basis

15.0 Standard Service Components

Support Team

- 1st line helpdesk
- 2nd/3rd line support
- Incident Management
- Problem Management
- Change Management

More detailed information on Support can be found in the Managed Services Support Core SLD.

Escalation

The service desk operates an escalation procedure to monitor the progress of incidents.

This enables us to effectively monitor whether the appropriate resources are being made available and are actively working to resolve a support incident.

Issues logged will be assigned a priority and then SLA timelines will be adhered to based on that priority. Escalation takes place for any issues that fall outside the agreed SLA.

Invocation support and planning

The service team would put together a plan of how the disaster recovery process would work, how it's initiated and invoked.

This would include supporting any decision to invoke disaster recovery, what it meant and how to fail back to normal services.

16.0 Service Exclusions

- Live invocation testing
- Connectivity between sites – This is a prerequisite and can be delivered under an appropriate communications service

17.0 Toolsets

- Zerto – Hypervisor based object replication with journal functionality
- VCloud – Private Cloud environment
- Azure – Public Cloud environment
- AWS – Public Cloud environment
- Connectwise – Managing Incidents, Problems and Changes

18.0 Terms

Scheduled Maintenance:

Clients are required to agree with a forward schedule of maintenance – within the Forward Schedule of Change (FSC). The service shall not be guaranteed during scheduled maintenance work. All scheduled maintenance work will be notified to you via the FSC. However where, in our reasonable opinion, an emergency situation exists, we also reserve the right to carry out emergency maintenance outside the normal notification period.

Termination:

We shall cease providing the service on termination of the contract.