

PROACT

G-Cloud 15

Proact Cyber Recovery as a
Service Service Definition

Document control

Document type	Public - Freely Distributable		
Company	Proact IT UK		
Address	Proact IT UK Grayson House, Venture Way, Chesterfield, Derbyshire, S41 8NE		
Telephone	01246 266 300		
Primary contact	bids@proact.oc.uk	Role	N/A

Revision history

Issue date	Author	Version	Revision description
04/12/2025	Colin Abram	V1	Document Upload



Proact Cyber Recovery as a Service Service Definition

Proact's Cyber Recovery as a Service provides a fully managed to service to failover IT services from a customer's production data centre to Proact's DR data centre. The service includes the provision of compute, storage and network resources to provide capacity to failover systems. The Cyber Recovery service includes management of the failover process and one DR test per year with the option to specify additional DR tests.

The deliverables of the Cyber Recovery service are as follows:

- Compute, storage and networking resources required to provide cyber recovery failover, hosted in a Proact data centre
- Provision of software including management to replicate data and achieve cyber recovery failover
- Managed DR processes and DR testing
- 24x7x365 Proact Service desk
- 24x7x365 automated monitoring of devices at Proact's data centre
- Self-service support and management portals
- Management, including break-fix activities, on underlying hardware
- Hosting of the hardware
- Incident management and resolution
- Problem management
- Change and configuration management
- A named Service delivery manager to co-ordinate delivery and provide regular customer reports

This document contains the following appendix detailing the service definitions for Proact Cyber Recovery as a Service:

- [Appendix 1 – Disaster Recovery as a Service - Service Definition](#)

Appendix 1 - Disaster Recovery as a Service - Service Definition

1.1 - Service Overview

Disaster Recovery as a Service (DRaaS) provides the ability for a Customer's server estate to be restarted within Proact's DR Shared Environment and made accessible to the Customer in the event of a complete outage at a Customer's site or cloud environment.

DRaaS allows for one or more replication methods to be chosen to better meet the Customer's replication requirements. Four different replication methods are available. These are referred to as:

Virtual Machine Replication with Continuous Data Protection (**VMR-CDP**)

Virtual Machine Replication with Scheduled Snapshot Replication (**VMR-SNAP**)

Storage Volume Recovery (**SVR**)

Where the Customer has an existing VM based VDI deployment, this can also be copied to the DRaaS platform and then brought online as part of each DR test or failover.

See the glossary for the definition of acronyms used.

General Service Deliverables
Proact shall: • Provide a service desk and customer support portal to report and update incidents, change requests and escalations. • Provide a Service Platform. • Provide service delivery management. • Maintain documentation of the service configuration. • Maintain a CMDB listing for all CIs. • Respond to Service Platform alerts and events and notify the Customer of relevant incidents. • Coordinate any product vendor involvement necessary. • Take appropriate action to restore operation of the Service Platform in case of outage. • Provide a major incident report, where required. • Provide a change advisory board to review normal, standard, and emergency change requests. • Subject to agreement, join the Customer's change advisory board, for relevant changes. • Implement agreed changes to CIs. • Respond to reasonable service requests for relevant information and advice. • Provide reasonable problem management. • Provide incident trend analysis.
The Customer shall: • Maintain compatibility with Proact-managed systems/applications at the hardware, OS, and application level. • Log incidents via the portal, telephone, or email. Priority one incidents must be logged by telephone. • Assist with any systems or applications not under Proact's management. • Respond to requests for information/actions within five working days. Inactive incidents may be closed. • Resolve health issues on customer-managed systems. • Nominate named individuals to engage with Proact on the approval and timing of changes. • Work with Proact to agree predefined actions for common types of incidents.
The following elements are out of scope of the service: • Upgrade or enabling of new features on the Service Platform or DRaaS platform. Proact may upgrade either platform at its sole discretion.

Standing Charge
Proact shall: • Provide the DRaaS platform within Proact's datacentres. • Take appropriate action to restore operation of the DRaaS platform in case of outage. • Provide a dedicated and isolated DR tenancy within the platform, holding the replica copies of CIs.



- Work with the Customer to agree a DR plan, for use during DR testing and failover.
- Update the DR plan with modifications to the environment provided by the Customer.
- Exclude changes to the DR plan, that are not yet tested, from the subsequent DR test success criteria.
- Schedule reports regarding replication task status.
- Provide a service review report.
- Organise a quarterly service review meeting.

The Customer shall:

- Be billed directly by the cloud provider for any public cloud resources consumed.
- Provide anti-virus protection for all systems running within the Customer's site(s)/cloud environment(s).
- Remove or reconfigure existing backup or DR tools that impact the service.
- Work with Proact to agree a DR plan, for use during DR testing and failover.
- Inform Proact, via change control, of modifications to CIs and allow for updates to the DR plan.
- Adhere to the agreed DR plan, during testing and failover.
- Provide 'Service Accounts' and password with privileges required to replicate all CIs.
- Provide 'Local Server' accounts and passwords to allow server login during DR testing and failover.

The following elements are out of scope of the service:

- Replication of flat file dumps of application data.
- Replication of any OS/Application that the vendor classes as 'end of life' or 'end of support'.
- DR testing performed outside of local business hours.
- Failback to the Customer's site(s)/cloud environment(s) once a DR failover has been invoked.

Recovery Server Resource Pool

Proact shall:

- Install and manage replication software at the Customer's site(s), where required.
- Provide vRAM/vCPU resources for the Customer's VMs, during DR testing and failover.
- Schedule a DR test and adhere to the DR plan, once every 12-months, within local business hours.
- Work with the Customer to agree the recovery points used within a DR test or failover.
- During DR testing, isolate recovered CIs, to avoid polluting the Customer's site(s)/cloud environment(s).
- During DR testing, make CIs live within the DR tenancy.
- Deem a test successful, where unmodified CIs are recovered successfully by following the DR plan.
- Update the DR plan and repeat the modified DR test process within one calendar month.
- Disconnect CIs and discard changes made, following each DR test.
- Issue a DR test report and update the DR plan following each DR test.
- Invoke DR failover and follow the DR plan, upon receipt of a validated P1 DR failover request.
- During DR failover, make CIs online within the DR tenancy.
- During DR failover, make Public IPs and CIs accessible to the internet, where required.
- During DR testing or failover, make CIs accessible to assigned Customer end-users, via the DoD firewall.
- Assume test/failover recovery successful where CIs are recovered, but associated applications fail to start.
- Connect PHC VMs/hosted equipment, to the DR tenancy, during DR testing or failover, where required.
- Upon request, provide licenses for Microsoft and Linux OSs and Microsoft applications.

The Customer shall:

- Provide and manage servers/cloud instances required by Proact to host replication software.
- Provide sufficient compute/network/storage resource to allow for management and replication of CIs.
- Work with Proact to agree the recovery points used within a DR test or failover.
- Validate their live environment is working prior to the scheduled DR test.
- Refrain from writing business data to CIs during DR testing. All changes will be discarded.
- Request DR failover with a P1 Incident request, logged by phone (not email).
- Refrain from writing business data to live systems once failover is invoked. All changes will be discarded.
- Make required DNS changes for redirecting users or services.
- Validate the content and functionality of all CIs recovered during a DR test or DR failover.
- Hold a valid vendor subscription/license or DR failover rights, for any OS/Application in the DR tenancy.
- Have an active software assurance contract for any Microsoft applications replicated.
- Inform Microsoft of failover to the DR tenancy, where required by their subscription/license agreement.
- Be responsible for any penalties for application or OS license breaches detected in their DR tenancy.

Recovery VDI Resource Pool

Proact shall:

- Provide vRAM/vCPU resources for the Customer's VDI worker servers, during DR testing and failover.
- Provide vRAM/vCPU resources for the Customer's NetScaler gateway appliances, where required.
- Replicate VDI worker server template images for use during DR testing/failover, with VMR-SNAP only.
- Replicate VDI control/access/management layer servers with VMR-SNAP or VMR-CDP.
- During DR testing, power on worker servers up to 10% of the Recovery VDI resource Pool vRAM.
- During DR failover, power on worker servers up to the Recovery VDI resource Pool vRAM assignment.
- During DR failover, provide internet access to Citrix Cloud Gateway Services, where required.

The Customer shall:

- Manage end-user access to the VDI worker and gateway servers, during DR testing and failover.
- Secure end-user devices accessing the VDI worker and gateway servers.
- Provide valid VDI subscription/licenses for DR testing and failover.

Ultra, Performance & Capacity Storage

Proact shall:

- Offer multiple tiers of storage, offering both capacity and performance.
- Assign DR CIs to the storage tier requested by the Customer.
- Provide parity RAID to ensure component failure redundancy on all storage tiers.
- Create a virtual ONTAP instance in the DR tenancy, to receive a copy of Customer's ONTAP source CIs.
- Provide ONTAP target volumes, in the virtual ONTAP instance, in the requested storage tier.
- Work with the Customer to connect ONTAP replication between the source CIs and target volumes.
- Monitor ONTAP storage replication tasks and respond to failures, where required.
- Present ONTAP LUNs to VMs in the DR tenancy, during DR testing and failover, where required.

The Customer shall:

- Inform Proact of the storage tier required for CIs.
- Request additional storage in a timely fashion, where required.
- Hold valid ONTAP replication subscriptions/licenses to replicate the any required volumes.
- Inform Proact of any ONTAP volumes that require replication and the required storage tier.
- Work with Proact to connect ONTAP replication between the source CIs and target volumes.
- Manage replication of ONTAP volumes from the Customer's site(s)/cloud environment(s) to the DR tenancy.
- Manage ONTAP snapshots and the replication schedule to provide one or more recovery points per day.
- Retain replicated snapshot recovery points for a minimum of three days (72 hours).
- Work with application vendor to achieve volume application consistency, where required.

VMR SNAP Protected Servers

Proact shall:

- Manage replication of VMs from the Customer's site(s) to the DR tenancy.
- Provide all replication software and licenses required to replicate the Customer's data.
- Monitor replication tasks and respond to failures.
- Utilise scheduled replication, providing one or more recovery points per day.
- Retain replicated recovery points for three days (72 hours).
- Compress replication traffic to reduce bandwidth usage.
- Provide application consistency via VSS for compatible applications, where required.
- Assign VMs into consistency groups, to provide consistency across multiple VMs, where required.

The Customer shall:

- Inform Proact of VMs that require replication.
- Inform Proact of VMs that require application consistency or consistency groups.
- Work with their application vendor to achieve consistency, where VSS is not supported.
- Where their existing Veeam server is used: Manage, restart, and troubleshoot replication tasks.
- Request changes to recovery point retention, where required.



VMR CDP Protected Servers

Proact shall:

- Manage replication of VMs from the Customer's site(s)/cloud environment(s) to the DR tenancy.
- Provide all replication software and licenses required to replicate the Customer's data.
- Monitor replication tasks and respond to failures.
- Utilise journaled replication, providing multiple recovery points per hour.
- Retain replicated recovery points for three days (72 hours).
- Compress replication traffic to reduce bandwidth usage.
- Provide application consistency via VSS for compatible applications, where required.
- Assign VMs into consistency groups, to provide consistency across multiple VMs, where required.

The Customer shall:

- Inform Proact of VMs that require replication.
- Inform Proact of VMs that require application consistency or consistency groups.
- Work with their application vendor to achieve consistency, where VSS is not supported.
- Request changes to recovery point retention, where required.

The following elements are out of scope of the service:

- Protection of cloud instances stored on Azure Managed Premium SDD Disks.

Standard Firewall

Proact shall:

- Provide a Dial on Demand (DoD) firewall within the DR tenancy, for use during DR testing and failover.
- Provide DoD VPN client software, compatible with the firewall.
- Provide DoD access to the DR tenancy network for 100 concurrent users during DR testing and failover.

The Customer shall:

- Deploy DoD VPN client software on end-user hardware that requires access.
- Take any steps required to make the DR tenancy accessible to end-users, during a DR test or DR failover.

Biannual Disaster Recovery Test

Proact shall:

- Perform a second scheduled DR test within each 12-month period.
- The second DR test will be conducted within local business hours.
- Issue a second DR Test report and update the DR plan following each DR test.

Direct Internet Access

Proact shall:

- Provide access to the service via the internet, through a secure firewall.
- Provide an encrypted tunnel over the internet to secure management and replication traffic.
- Provide internet bandwidth for the transfer of service traffic.

The Customer shall:

- Provide sufficient internet bandwidth for the transfer of service traffic.
- Provide an external IPv4 public IP address for the creation of the encrypted tunnel.
- Provide sufficient bandwidth ensure DR replicas are up to date enough to meet recovery requirements.
- Provide a network administrator to configure and troubleshoot service traffic.
- Request bandwidth throttling of replication traffic, where required.

Public Facing IP Address

Proact shall:

- Provide a public internet facing IP address bound to a secure firewall.



- Route the IP address to the Customer's systems.
- Manage IP routing and certificate changes on devices within Proact's datacentres.

The Customer shall:

- Make required DNS changes for redirecting users or services to the assigned public IP.

1.2 - Service Level Agreement

1.2.1 - Availability Service Levels

Uptime Commitment – DRaaS platform	Proact will use its reasonable endeavours to achieve an Uptime for the DRaaS platform of at least 99.99% of each month. The DRaaS platform will be available if the hypervisors and storage respond to their monitoring software probes within any single node of the DRaaS platform's hypervisor cluster and any single node of the DRaaS platform's storage cluster.
Uptime Commitment – Comms Internet	Proact will use its reasonable endeavours to achieve an Uptime for the internet connectivity for the service provided to the Customer of at least 99.95% of each month. The internet connectivity will be available if Proact's monitoring software can access commonly available web pages using the communications link.
Uptime	The percentage of total possible minutes the service was available during the month: $[(\text{total minutes in month} - \text{Downtime}) / \text{total minutes in measurement period}] * 100 = \text{Uptime}$
Downtime	The overall number of minutes the service was unavailable during the measurement period. Proact calculates downtime using its standard monitoring tools, the output of which shall be conclusive except in case of manifest error. Downtime excludes any times the service is not available for planned maintenance or reasons beyond Proact's control, as set out in the Standard Terms and Conditions.
Service Credit	If the actual Uptime for this service falls below the Uptime commitment the Customer will be eligible for a Service Credit equal to a percentage of the monthly minimum charges for this service. The relevant percentage is equal to the difference between the actual Uptime achieved and the Uptime commitment, with a minimum of 5% of the relevant monthly charges and a maximum of 50%. A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service.

1.2.2 - Response Time Service Levels

Response	Proact is deemed to have 'responded' when a case is created in Proact's customer support portal, and a case number is allocated.
Initiation	A change is initiated at the point at which (as recorded in the support system) Proact commences implementation of the change.
Response Time SLA - P1 Incident	Proact will use its reasonable endeavours to respond to priority 1 (P1) incidents within 30 minutes . A P1 incident is: (i) a reasonable request by the Customer, which will be logged by phone (not email), for support or information in connection with the services, in

	circumstances in which the service(s) are completely unavailable or are imminently expected to be completely unavailable; or (ii) an alert received by Proact directly from its monitoring platform in connection with the services, that the service(s) are completely unavailable or are imminently expected to be completely unavailable; or have breached defined critical monitoring thresholds; or (iii) an incident logged by Proact in relation to an imminent and serious threat to the service(s). If Proact fails to respond to a P1 incident within 30 minutes the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.
Response Time SLA - P2 Incident	Proact will use its reasonable endeavours to respond to priority 2 (P2) incidents within 1 working hour. A P2 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning such that the service is significantly impacted but remains operational or have breached defined major monitoring thresholds. If Proact fails to respond to a P2 incident within 1 working hour the Customer will be entitled to a Service Credit of 5% of the monthly minimum service Charges.
Response Time SLO - P3 Incident	Proact will use its reasonable endeavours to respond to priority 3 (P3) incidents within 4 working hours. A P3 incident is a reasonable request by the Customer for support or information, or an alert received by Proact directly from its monitoring platform, in connection with the services, in circumstances in which the service(s) are malfunctioning but with no significant impact on service or have breached defined minor monitoring thresholds.
Response Time SLO - P4 Incident	Proact will use its reasonable endeavours to respond to priority 4 (P4) incidents within 8 working hours. A P4 incident is a reasonable request by the Customer for support or information, in connection with the services, in circumstances in which there is no specific malfunction.
Service Credit Limits	A Service Credit is not a refund, cannot be exchanged into a cash amount and is capped at a maximum of 50% of the monthly minimum charges for the relevant service. A Service Credit is the sole and exclusive remedy for any failure by Proact to meet its obligations under the SLA.
Response Time SLO – Standard Change Request	Proact will use its reasonable endeavours to initiate standard changes within 8 working hours from when authorised. A 'Standard' change is any pre-authorised change that is low risk, relatively common and follows a predefined procedure or work instruction. Proact's change advisory board (CAB) is not required to approve 'Standard' changes prior to implementation.
Response Time SLO – Normal Change Request	Proact will use its reasonable endeavours to initiate normal changes within 8 working hours from when authorised. A 'Normal' change is any change that is not a 'Standard' change according to the above definition and is not an emergency. An agreed ad-hoc change to the configuration of the services. The Change Advisory Board (CAB) must authorise 'Normal' changes and approve an implementation plan.
Response Time SLA – Emergency Change Request	Proact will use its reasonable endeavours to initiate required emergency changes within 4 hours from when authorised.



	An 'Emergency' change is any 'Normal' change that requires an expedited timeframe to resolve a P1 incident causing significant impact to the services in scope, and which cannot wait for review and approval from the CAB. Where there is not an active P1 incident, the change shall not be classified as 'Emergency'. Proact's Emergency Change Advisory Board (E-CAB) must authorise 'Emergency' changes and approve an implementation plan. If Proact fails to respond to an Emergency Change Request within 4 hours, then the Customer will be entitled to a Service Credit of 15% of the monthly minimum service Charges.
Response Time SLO – Service Request	Proact will use its reasonable endeavours to initiate service requests within 8 working hours. A 'Service request' is a reasonable request by the Customer for activity or information, in connection with the services, that is neither an incident nor a change and follows a predefined procedure or work instruction. A common example of a Service Request is a password reset.
Working hours for changes	All Standard changes and Normal changes shall be scheduled by Proact and will be carried out during local business hours except where a change is requested by Proact and is expected by Proact (upon evaluation by the Proact CAB) to have a significant impact on availability or performance of the services in scope. The Customer may request that any particular change is implemented at a specific time, including outside local business hours, but, if such request is accepted by Proact, additional charges shall apply as agreed in advance between Proact and the Customer. 'Emergency' changes are implemented 24/7 and are not subject to additional charges.

1.3 - Vendor Terms

In addition to the terms and conditions set out in this Managed Service Agreement the Customer shall be subject to the relevant vendor terms set out at <https://www.proact.eu/en/about-us/terms-and-conditions/vendor-terms/>.

Vendor Name
Veeam
Zerto
NetApp

1.4 - Glossary

Glossary Term	Definition
Configuration Item (CI)	A term used for a component which is within the scope of the Contract and stored within the Configuration Management Database (CMDB). The CIs will be the VMs, physical servers and ONTAP volumes, set out in the Contract.
Service Platform	Depending on the service, Proact will provide monitoring and/or management platforms to enable delivery of the service. These Service Platforms are managed by Proact.