Cloudreach™
an atos company

Infrastructure Reliability

Service Specification

Service Specification

Service Name:	Infrastructure Reliability
Service Level Hours:	Refer to section 1.1
Unit of Charge:	% of AWS, Azure and/or GCP Spend
Prerequisites:	Refer to Deployment Documents Minimum of: - AWS Business Support Plan for AWS; - Azure Standard Support for Azure; and - Role-Based (Production) Support for GCP on all accounts managed by Cloudreach
Supported Cloud Platforms:	AWS, Azure and GCP
Product Codes:	CO-INFRASTRUCTURE-RELIABILITY CO-INFRASTRUCTURE-RELIABILITY-OB
Version Number:	3.1.4
Status:	Live
Published Date:	December 2021

The Small Print

This document has been prepared solely for Cloudreach's customers. It is provided to the Customer on a confidential basis. Any reproduction or distribution of this document, in whole or in part, or the disclosure of its content, without the prior written approval of Cloudreach is not permitted. By accepting, opening or reviewing this document, Customer acknowledges the confidential nature of the information contained in this document and agrees not to reproduce or distribute this document or any information contained in this document.

Definitions

The definitions for all capitalised terms used throughout this Service Specification are set out in the Cloud Operations Service Definitions document which forms a part of this Service Specification and the Cloudreach Order Form to which this Service Specification relates.

Table of Contents

1. Service Overview

Infrastructure Reliability is a managed service for AWS, Azure and GCP. The service will manage the availability and accessibility of the Customer's environment(s) in these public clouds. It will provide operational support services of Customer's environments and support components/ resources/ instances within their cloud platform that is controllable by the Cloud Service Provider's (CSP) console or APIs. It will also support the availability and accessibility of the VMs hosting the Customer's applications.

This service is pursuant to the Customer maintaining a minimum of Business tier AWS Support for AWS, Azure Standard Support for Azure and Role-Based (Production) Support for GCP, on any and all accounts managed by Cloudreach. Depending on the Customer billing arrangement and if necessary, Cloudreach can assist in the procurement of this support.

A summary of the key features of Infrastructure Reliability are listed below:

Onboarding - Cloudreach will assign a Service Transition team member to manage the project of onboarding the Customer environment(s) into Infrastructure Reliability. During the initial phase of onboarding, Cloudreach will assess the time needed to onboard the environment based on the complexity and intricacies involved with onboarding. Please note that Cloudreach will only perform onboarding of Customers environments during Business Hours.

Availability and Performance Management - The service will monitor the availability and accessibility of the Customer's environments up to the Operating Systems. Cloudreach will monitor IAAS and PAAS services at Cloud Provider Platform level by ingesting metrics which are available by default in the corresponding CSP's monitoring service (i.e. AWS Cloudwatch, Azure Monitor, Google Cloud Operations Suite). Cloudreach shall define alerting for these metrics based on the best practices for the corresponding CSP service and customer requirements. The performance metrics will also be collected to detect trends with defined thresholds for alerting and performance analysis.

Patching - Security patches will be applied on a monthly basis, with the ability to audit and report on the patches applied while maintaining compliance standards.

Backups and Restore - Block Level backups will be taken for Operating Systems and Database Engines with restore of backups performed via Service Catalog Requests.

Managed Security Services - As an extension to Infrastructure Reliability, Cloudreach is able to offer managed security services focused on threat and vulnerability management. These offerings are purchased at an additional cost and details can be found in the relevant service specification.

Endpoint Detection and Response (EDR) - as part of managing any Virtual Machine (VM)s in the Customer's environment(s), Cloudreach includes Endpoint Detection and Response software to provide Anti-Virus and Anti-Malware protection. The supply, configuration, tuning, ongoing maintenance and reporting are part of the service.

Services Management Support - the Customer's public cloud environment(s) will be maintained as part of the service including configuration management and any trouble-shooting that may be required to address issues with availability and accessibility of the environment(s). Incidents and Changes will be managed using the corresponding ticketing tools and procedures in accordance with runbooks and/or process(es) documented.

Continuous Improvement (*available if (i) the Customer's Monthly Spend ≥ $25,000 unless otherwise specified in applicable order form and (ii) the number of hours of Continuous Improvement available is set out in the order form*) - This service aims to continuously improve a Customers environment by providing remote access to Improvement Engineers on an adhoc basis to deliver value focused on the following areas; operational improvement, financial optimisation, and security.

Cost Management - designed to address and overcome many of the challenges that enterprises face with public cloud billing, usage insight, financial governance and cost optimisation.

Service Delivery Manager (SDM) - Appointed Service Delivery Manager responsible for owning the Customer experience and delivering the service management outcomes associated with Managed Services provided by Cloudreach. The SDM provides strategic business alignment, business critical IT service management, chaired proactive service reviews and continuous service improvement. The SDM delivered remotely is included as part of Infrastructure Reliability. If the Customer is requesting that the SDM is on-site, and/or has a specific dedicated number of hours or days a month, additional charges, including travel and expenses shall be applied. Customer's specific requirements will be captured during pre-sales and associated additional charges will be priced on application and reflected accordingly in the order form.

1.1 Service Levels

Services	Service Level Hours
Onboarding Continuous Improvement	Business Hours (9x5) (*PDT time zone if the Customer is based in NA and UTC time zone if the Customer is based in EEA & UK*)
Service Delivery Manager	Business Hours (9x5) (*applicable time zone where the SDM is located*)
Availability and Performance Management Backup and Restore Endpoint Detection and Response Service Management Support (P1 and P2 Incidents) Service Management Support (Changes)	24x7
Patching Service Management Support (P3 and P4 Incidents)	24x5 (*PDT time zone if the Customer is based in NA and UTC time zone if the Customer is based in EEA & UK*)

2. Operating Systems Supported

Cloudreach supports the following Operating System versions:

Operating System Version	Comment
Windows Server 2012 R2 (currently under extended	On January 14, 2020, Microsoft officially ended its support for Windows Server 2008 R2 editions. Cloudreach has stopped

support) Windows Server 2016(currently under extended support) Windows Server 2019	support of this version on January 14, 2020. Windows Nano Server is not supported at this time. Please note that once a Microsoft operating system (OS) has reached End of Support, Cloudreach will be unable to provide security updates or patches. The OS may still work after the support of the operating system has been discontinued. However, the possibility increases that new programs will not be performant on an older OS and there is an increase in security threat. Monitoring is not available on End of Support OS's and any incident experienced is not applicable to Cloudreach's SLA. Any support Cloudreach can provide will be considered 'best endeavours' and may be limited to referring the incident to Microsoft if a customer has an existing Microsoft extended support contract in place.
Ubuntu	Only the LTS editions are supported at this time. Cloudreach will support any LTS (Long Term Support) versions which are currently within vendor support. For a list of supported LTS versions and their end-of-life date please visit https://wiki.ubuntu.com/Releases Please note that within an LTS version of Ubuntu, Canonical releases multiple "patch versions" of the LTS distribution. Different patch versions may contain different kernel revisions, with varying support (and security patching availability), which may end before the end of life of the LTS distribution. Cloudreach recommends that customers always opt in for the patch version that uses a kernel version which is supported throughout the lifecycle of the LTS distribution, as otherwise customer may miss out on some security patches until the kernel is upgraded. Kernel upgrades are not part of the monthly patching schedule performed by Cloudreach. For further information please see https://wiki.ubuntu.com/Kernel/Support
Debian	Cloudreach will support any LTS versions which are currently within vendor support. For a list of supported LTS versions and their end-of-life date please visit https://wiki.debian.org/LTS/
Amazon Linux	Cloudreach will support any LTS versions which are currently within vendor support. For a list of supported versions and their end-of-life date please visit https://aws.amazon.com/amazon-linux-ami/faqs/
CentOS	Cloudreach will support any major version which are currently within vendor support. For a list of the currently supported versions and their end-of-life date please visit https://wiki.centos.org/About/Product
RedHat Enterprise	Cloudreach will support any RHEL version which is currently within the vendor's Full Support.

	For a list of the currently supported versions and their end-of-life date please visit https://access.redhat.com/support/policy/updates/errata

2.1 LTS version support

Cloudreach may require to update and test the set of tooling to ensure that it works as expected with new versions of Operating Systems. For that reason, at times, Cloudreach may not be able to support new LTS versions of Operating Systems as soon as they are released.

In the case of OS vendors making changes that require Cloudreach to adjust the tooling, Cloudreach reserves the right to take up to 6 months to make all necessary changes to support new LTS releases.

With regards to Operating Systems end of support, Cloudreach will provide support until such date or extension thereof, from the OS vendors.

3. Onboarding

3.1 Onboarding Terms

Once the service is ready for onboarding, Cloudreach will assign a Service Transition team member to manage the project of onboarding the Customer environment into Infrastructure Reliability. Cloudreach will also allocate a Service Delivery Manager, who will be the main point of contact between the Customer and Cloudreach during the onboarding phase.

During the initial phase of onboarding, Cloudreach will assess the time needed to onboard the environment based on the complexity and intricacies involved with onboarding.

Please note that Cloudreach will only perform onboarding of Customer environments during Business Hours.

Cloudreach will also conduct a security onboarding assessment to analyse the security posture of a Customer's environment, highlight any vulnerabilities and provide a security recommendation report. The Service Delivery Manager will work with the Customer to determine which items from the security recommendation report can be remediated as a part of Continuous Improvement (where applicable) and for which Customer needs to look at our managed security services, or address vulnerabilities with their internal security teams.

3.2 Deployment Strategy

In order to deliver the Infrastructure Reliability service, Cloudreach needs to have access to the Customer’s environment(s) in the form of network, API and system level access. This enables Cloudreach’s operational teams to provide the various management services within the Customer’s environment where configuration, maintenance, troubleshooting and service management are required. For example, in the case of configuration and service management, Cloudreach needs to deploy its monitoring and management tools.

The Deployment Strategy Document also details the policies that the Customer needs to comply with for the duration of the contract.

A separate Deployment Document details the access information required for the customer's chosen public cloud platform such as network address(es), accounts/subscriptions and logins, authentication and permissions. This is a prerequisite for Cloudreach to deliver Infrastructure Reliability to the Customer. The necessary documentation will be made available before and at the time of onboarding the environments to be taken under Cloudreach management.

Here's an example:

If AWS ASG or Azure Scale Sets exist within Customer's Cloud Platform, then the Customer shall provide Cloudreach with relevant access to implement the required integration and deployment tools as made available per the AWS ASG or Azure Resource Groups services. (i.e. User data for an AMI that is used with an ASG launch configuration). Customer shall be responsible for limiting Cloudreach's access to only the specific data, information or other Customer material which is required for the purposes of carrying out the implementation.

The Customer shall inform Cloudreach of any changes to the Golden AMI in use of said resources outlined above to ensure that all Cloudreach monitoring and management tools continue to function effectively upon service redeployment.

3.3 List of VM Agents installed on Compute Resources

Cloudreach, as part of delivery of Infrastructure Reliability service, may install following agents onto the compute resources:

Vendor	Agent	Notes
CINC	CINC Client	For Configuration Management of Cloudreach tooling, where applicable.
Splunk	Splunk Observability Cloud Smart Agent	Monitoring agent which collects telemetry data from OS level instances.
Crowdstrike	Crowdstrike Falcon	Endpoint Detection and Response agent.
AWS	Simple Systems Manager (SSM) Agent	Management agent, used for the purpose of patching and running shell commands externally for customers with environments in AWS.
Azure	Log Analytics Agent	Management agent used for Patching & Backups of Azure VM's. Only for customers with environments in Azure.
Azure	Azure VM Agent	Pre-installed with marketplace images, this agent is required for various management purposes of Azure VMs.
Azure	Hybrid Worker Agent	For execution of Azure Automation runbooks on VMs (used for patching automation).
Azure	OMS Agent	Management agent, used for the purpose of patching
GCP	OS Config Agent	Management agent, used for the purpose of pathing
Cloudhealth	Cloudhealth Agent	Required for Cost Management activities.

Splunk	Splunk Agent	Log collection agent

Cloudreach reserves the right to change or add agents to Customer VM's. Customers will be notified of any changes made to the list above with advance notice.

3.3.1 Agent Maintenance

It is the responsibility of Cloudreach to install and maintain the version and configuration of agents installed on Customer's Virtual Machines.

Unless otherwise agreed by Cloudreach, the Customer shall not alter the agents installed and configured by Cloudreach, as any changes made may result in impact on the service that Cloudreach can provide.

4. Availability & Performance Management

Cloudreach will monitor the health of cloud resources for each mutually agreed AWS, Azure and/or GCP Account and can raise an alert based on the event conditions denoted during Onboarding Process. Cloudreach defined AWS, Azure and GCP health check metrics are based on a subset of available AWS CloudWatch, Azure Monitor Diagnostics and Google Cloud Operations Suite metrics.

In the event that an alert is raised, Cloudreach shall:

- Manage the response to the alert pursuant to the Incident Management Process.
- Send the alert based on the event conditions as an email to the Primary Contact as denoted during the Onboarding process.

4.1 Monitoring Methodology

4.1.1 Data Residency

All monitoring data collected by Cloudreach will be stored on servers hosted in the EU region.

4.1.2 Data Collection

For CSP native monitoring services (i.e. AWS CloudWatch), data will be collected from an external 3rd party tooling provider via API requests to the appropriate CSP service. As part of the onboarding process, a service account role and relevant permissions will need to be created in Customer environments to allow this collection.

For OS-level collection of data, an agent will be installed on the operating system. The agent will report metrics to an external endpoint, either directly or via proxy.

Frequency of collection is configurable, with default being every 5 minutes. Over time, older data might be aggregated for performance reasons.

4.2 Scope of Support

This section provides an explanation of what Cloudreach means in relation to support of CSP services.

Cloudreach is aiming to support all services provided by our CSP partners (AWS, Azure & GCP). If you have a list of services required to be supported we can confirm which of these we support with best practice recommendations.

4.2.1. Best Practice Guidance

Cloudreach holds expert level knowledge of CSP services and leverages this to provide guidance and advice to Customers. Engineers will be able to advise the Customer on changes to the relevant service(s) that are inline with the best practice guidelines provided by the vendor and discuss details and intricacies of the service with customers.

4.2.2 Configuration Management

Cloudreach will perform changes to the service(s) at CSP Level, using either CSP's provided GUI or API to execute the change. The focus of any changes to be carried out will be to either maintain or improve health, availability or accessibility of the resource/service.

4.2.2.1 Out of Scope: Configuration Management

Please note that within the Infrastructure Reliability service, Cloudreach will only perform environment-level support and will not provide application-level administration. An example of this is an RDS service, where Cloudreach will ensure that the database is configured correctly (i.e. Network level access, monitoring CloudWatch metrics, backups).

However, within Infrastructure Reliability, Cloudreach will not provide any service that interacts with the data inside the database (i.e. altering tables, modifying data, creating SQL users). For this level of support, Cloudreach can discuss prior to onboarding what the requirements are and recommend additional bolt on services i.e. in the case of Database Administration, Cloudreach would recommend the Customer "Database Support" as an additional service.

4.2.3 Service Troubleshooting

Cloudreach will assist Customers with troubleshooting issues with the service or resource at CSP level, with the focus of providing availability and accessibility of the resource and service within customer environments.

An example of an issue, where Cloudreach can assist, could be a problem with an application connecting to the database. In such an instance, Cloudreach would be able to review the network connectivity & health of the database to establish the cause of the connectivity issue. With this in mind, within the Infrastructure Reliability service, Cloudreach would not look to investigate any issues with the data once inside the database (i.e. query performing slowly) unless there was the additional service of "Database Support" purchased separately.

4.2.4 Service Monitoring

Cloudreach shall integrate with Cloud Service Provider native monitoring tooling to provide monitoring service to Customers. In most cases, Cloudreach will perform API calls (either directly or via 3rd party tooling) to collect various metrics from CSP Monitoring service (i.e. AWS CloudWatch) and will ingest those metrics into a monitoring platform, where further analysis will be performed to identify problems and patterns within Customer environments.

Cloudreach is utilising the following API services to collect Metrics Data:

- AWS Cloudwatch
- Azure Monitor
- Google Cloud Operations Suite

During onboarding, Cloudreach will discuss and agree on monitoring methodology with the Customer. Cloudreach will configure the monitoring alerts to the needs of the Customer environment(s), focusing on monitoring key components which indicate that

the platform is available and accessible. Cloudreach will only perform monitoring of the services which are critical for the health & availability of the Environment, in line with the Environment usage patterns.

Once onboarding is completed, Cloudreach monitoring software will monitor the Customer environment(s). Cloudreach will receive notifications and investigate events in accordance with the defined monitoring alerting. If appropriate, Cloudreach will raise a support case and contact the Customer primary contact(s) to inform them of the details of the support case.

Cloudreach reserves the right to disable or modify a specific monitoring or alerting configuration on notice to the Customer, if deemed necessary by Cloudreach in order to preserve an accurate and effective alerting signal.

4.2.4.1 Compute Resources

For an additional level of monitoring for compute resources, Cloudreach will require to perform an installation of agent software on every Compute Resource which is to be supported. Further details about the agent installation will be provided within the "Deployment Strategy" document supplied during onboarding.

4.2.5 Out of Scope

- Virtual Machine Hosted Applications. Customer hosted applications such as databases, network and web servers will only be monitored for health and performance of underlying VM infrastructure that they are running on.

- For avoidance of doubt, Infrastructure Reliability will support existing resources, rather than provision net new resources unless necessary in support of existing infrastructure.

5. Patching

Cloudreach shall perform the following Operating System patching where patches are made available by the Operating System provider.

Type	Frequency
Critical and Security Patching	Monthly, within mutually agreed maintenance window with customer during onboarding.
Responsible Disclosures and Zero-day events.	Where the risk profile is severe, responsible disclosures and zero-day events will trigger a patching or remediation effort from Cloudreach.

If Customer makes use of Golden Amazon Machine Imagines (AMIs) or Azure Gold Image as a source for infrastructure deployment Cloudreach will hold temporary Snapshots as a roll-back mechanism if required during critical/security patching periods.

5.1 Scope of Security Patching

For Windows VMs, Cloudreach will configure Windows VM's with Cloudreach-managed WSUS server. Cloudreach will then only whitelist patches classified as "Critical Updates" and "Security updates". No other patches will be applied to those virtual machines by Cloudreach.

For Linux VM's, with example of Amazon Linux or RHEL distributions, Cloudreach will only install patches marked as "security" patches, for example by using the "yum security" plugin (https://linux.die.net/man/8/yum-security).

Cloudreach will install minor kernel security patches during patching activity, however, within the scope of regular patching, Cloudreach will not upgrade kernel version of the underlying OS.

For avoidance of doubt, Infrastructure Reliability will not perform any application-level patching on Customer workloads.

Exception:

- Due to the nature of security and non-security related updates in CentOS, patching will always include non-security related updates for this distribution.

5.2 OS Upgrades

Operating System upgrades are considered to be a complex change, with higher risk to application stability. As such, Cloudreach does not perform this type of upgrade by default within the Infrastructure Reliability service.

Type	Notes
Windows Full version upgrade (e.g. Windows 2008 to Windows 2012)	Cloudreach can perform and assist the customer with this type of upgrade. These upgrades are not performed on in-place systems and require a 'build new' approach where a new VM is built and migrated onto. This type of upgrade is considered a complex change and will be performed as a project outside of the Infrastructure Reliability service
Windows Service Packs (e.g. Windows 2008 to Windows 2008 SP1)	Cloudreach can perform and assist the customer with service pack updates as a complex change when requested. A Windows service pack update is less complex than a full version upgrade and can potentially be performed on an in-place VM. However, it is still considered a complex change and will be performed outside of the Infrastructure Reliability service. These may be performed as a component of continuous improvement.
Linux Distribution Upgrades	Cloudreach can perform Linux Distribution upgrades as a complex change when requested by the Customer. A Linux upgrade (distribution upgrade) will upgrade all existing software as well and install and remove packages to meet dependencies of the new version. This type of upgrade can be very disruptive and considered a complex project outside of the Infrastructure Reliability service
Linux Distribution Updates	Cloudreach can perform Linux Distribution updates as a complex change when requested by the Customer. A Linux update will update the currently installed packages but does not install or upgrade any packages. This type of update is less disruptive than a version upgrade and can typically be performed in-place. However, these updates are considered a complex change and will be performed outside of the Infrastructure Reliability service. These may be performed as a component of continuous improvement.

5.3 Automation of Patching

As part of efficient delivery of service to Customer, Cloudreach will deploy tooling which allows for automated patching of Customer virtual machines, including deployment of CSP native tools on the OS level (SSM agent for AWS, OMS agent for Azure, OS Config agent for GCP). Further details and requirements will be provided to the Customer within "Deployment Strategy" document, supplied during onboarding.

Due to complexities and intricacies of patching activity, Cloudreach will assess the ability to automate the patching activity for each environment and will implement the right level of automation to ensure the stability of the customer environment.

6. Backup and Restore

6.1 AWS and Azure & GCP Virtual Machine Backup / Restore

6.1.1 Schedule and Retention (AWS & Azure)

Cloudreach shall perform daily, weekly and monthly backups of the AWS EC2 and Azure Virtual Machine operating system Instances based on the default schedule and retention periods defined in the table below:

Backup	Schedule	Retention Period
Daily	02:00 UTC Monday to Sunday	7 days
Weekly	03:00 UTC every Sunday	4 weeks
Monthly	04:00 UTC on the first of every month	2 months

Customers may request alternative backup schedules and/or retention periods during Onboarding of the Customer's services which shall be subject to approval by Cloudreach.

Instances are backed up based on the approach defined in the table below:

- All Incidents raised by the Cloudreach backup monitoring and configuration platform pertaining to 'backup failure' will automatically be assigned as an Incident request and actioned by the Cloudreach CSD.

6.1.2 Schedule and Retention (GCP)

Cloudreach shall perform daily backups of the GCP Virtual Machines based on the default schedule and retention periods defined in the table below:

Backup	Schedule	Retention Period
Daily	02:00 UTC Monday to Sunday	30 days

OR

Backup	Schedule	Retention Period
Weekly	02:00 UTC Sunday	52 weeks

Currently Cloudreach is only able to offer Daily OR Weekly backup policy for GCP VM's.

6.1.2 Backup Approach

Cloud Platform	Backup Approach
AWS	Backups are performed using the AWS Backup service or by taking a Snapshot of AWS EC2 EBS volumes on a regular schedule as specified in the preceding table.
Azure	Backups are performed by taking full backups of each Azure Virtual Machine against a regular schedule defined by the Customer. By default the preceding table sets out the backup and retention periods.
GCP	Backups are performed by utilising the “Scheduled Snapshots” functionality in GCP

Instances of Operating Systems can be restored upon request by the Customer based on the approach defined in the table below:

- If required by the Customer, Cloudreach shall invoke an Operating System recovery approach against the Azure VMs, AWS EC2 instances or GCP VMs within the supported account. The restore will be treated with P2 priority if it is service impacting.
- All requests raised by the Customer that are not identified as service impacting will be treated as P4 Service Catalog Requests.

6.1.3 Recovery Approach

Cloud Platform	Type	Recovery Approach
AWS	Instance or Full Volume	Root Volumes: Cloudreach shall create a new volume from a previous Snapshot depending on the date requested by Customer. Cloudreach shall remove the current volume and replace with the newly created volume. Additional Drives: Cloudreach shall create a volume from a previous Snapshot depending on the date requested by Customer. Cloudreach shall remove the volume and replace with the newly created volume or if requested attach the new volume at a different mount point. Time: Time scales depend on the size of the volume and any other file system factors such as encrypted file system implementations (e.g. BitLocker and ProtectV).
Azure	Instance or Full Volume	Virtual Machine: Cloudreach shall recover a chosen Azure Virtual Machine against an existing or retained application consistent backup from a previous recovery point as chosen by Customer. Upon system restore this will also restore all previous system dependent Azure services, installed applications, pre existing files and/or folders. Cloudreach shall re-assign any pre existing Azure endpoints to the newly created Azure Virtual Machines to ensure continued connectivity upon successful restore. Time The time to execute a restore action is variable and

		dependent on the volume of data to be recovered from a backup.
GCP	Instance or Full Volume	Root Volumes: Cloudreach shall create a new volume from a previous Snapshot depending on the date requested by Customer. Cloudreach shall remove the current volume and replace with the newly created volume. Additional Drives: Cloudreach shall create a volume from a previous Snapshot depending on the date requested by Customer. Cloudreach shall remove the volume and replace with the newly created volume or if requested attach the new volume at a different mount point. Time: Time scales depend on the size of the volume and any other file system factors such as encrypted file system implementations (e.g. BitLocker and ProtectV).

6.2 Database Backup

Cloudreach can provide the following backup strategy for specified cloud-native database technologies. There are two types of database backups supported:

1. A differential backup is based on the most recent, previous full data backup. A differential backup captures only the data that has changed since that full backup. The full backup upon which a differential backup is based is known as the base of the differential.
2. The transaction log is a serial record of all the transactions that have been performed against the database since the transaction log was last backed up. With transaction log backups, you can recover the database to a specific point in time (for example, prior to entering unwanted data), or to the point of failure.

Database Technology	Differential	Transactional	RPO	Default Retention
AWS				
RDS (MySQL)	✔	✔	5 minutes	1 week
RDS (Aurora)	✔	✔	5 minutes	1 week
RDS (PostgreSQL)	✔	✔	5 minutes	1 week
RDS (Oracle)	✔	✔	5 minutes	1 week
RDS (MS SQL)	✔	✔	5 minutes	1 week
RDS (Maria)	✔	✔	5 minutes	1 week
Azure				
Azure SQL (Basic Service)	✔	✔	10 minutes	1 week
Azure SQL (Standard Service)	✔	✔	10 minutes	5 weeks
Azure SQL (Premium Service)	✔	✔	10 minutes	5 weeks

GCP				
Cloud SQL (MySQL)	✔	✔	5 minutes	1 week*
Cloud SQL (PostgreSQL)	✔	✔	5 minutes	1 week*
Cloud SQL (SQL Server)	✔	✔	5 minutes	1 week

**Last 7 automated backups and transaction logs are retained as standard. Data shown assumes a daily automated backup.*

Cloudreach utilises cloud-native backup features of database hosting platforms (i.e. AWS RDS, Azure SQL, GCP Cloud SQL). Cloudreach does not actually perform or maintain backups, however, within the service, Cloudreach, upon customer request, will perform configuration changes to backup configuration, and will perform a restore operation, when requested by Customer (see section 6.3 for further details). Cloudreach is limited by the technology limitations of the respective CSP services and may not be able to fulfil requests for changes that are not possible.

With regards to Recovery Time Objective (RTO), Cloudreach is unable to provide generic assertion of how long it will take to restore a database. This is due to a number of factors which are unique to each application and environment (i.e. database size, application intricacies).

6.2.1 Out of scope Database support

Where there is a requirement for non-cloud native database backups Cloudreach has a database support service which can be purchased at an additional cost.

6.3 Database Restore

As part of the service, Cloudreach is able to perform a restore of the database (supported restore databases needs to be defined in table in section 6.2).

Cloudreach will only perform the restore of the database using the CSP generated backups. Cloudreach will only perform the restore as an emergency action, upon agreement with the customer, when the application has become unavailable due to an issue with the database. Cloudreach reserves the right to first investigate and decide if restore is an appropriate action to take. Cloudreach will always take the quickest path to restoring the database.

During this operation, additional maintenance tasks (for example, update of Customer's "Infrastructure-as-code" template) may be required. If requested by the Customer, such tasks may be performed by Cloudreach under Infrastructure Reliability Continuous Improvement.

7. Managed Security Services

Cloudreach's managed security offerings are conditional upon the Customer subscribing to one of our defined offerings.

The security offerings available can be found in the applicable service specification.

Cloudreach Managed Security Services provide a proactive approach for organisations to reduce operational risk and cost in AWS, Azure, and GCP cloud environments.

Cloudreach Managed Security Services:

- Cloudreach Security Fundamentals

- Cloudreach Security Essentials
- Cloudreach Security Enterprise

Features	Cloudreach Security Fundamentals	Cloudreach Security Essentials	Cloudreach Security Enterprise
Install, Configure, Maintain Security Software	✔	✔	✔
Automated Vulnerability Reports	✔	✔	✔
Review & Recommendations	Quarterly	Monthly	Monthly
Active Vulnerability Remediation	x	✔	✔
24*7 Critical Threat Management & Remediation	x	x	✔

8. Endpoint Detection and Response

Cloudreach instals, configures and manages Endpoint Detection and Response software to provide anti-virus and anti-malware protection on virtual machines that it manages on behalf of Customers' environments. The Endpoint Detection and Response software to deliver this service is provided as-is and is subject to compatibility with the OS (Operating System) type and/or version.

Cloudreach has selected a next-generation anti-virus software capable of performing detection of intrusion at kernel level of Operating Systems. Delivering comprehensive and proven protection to defend your organization against both malware and malware-free attacks. Incorporating identification of known malware, machine learning for unknown malware, exploit blocking and advanced Indicator of Attack (IOA) behavioural techniques,

8.1 Event Monitoring

Cloudreach shall proactively monitor the anti malware software for alerts and respond to such alerts based on the severity of the alert.

8.1.1 Quarantined Infections

If the infection has been quarantined, Cloudreach will inform the Customer of the event, and as the incident has been contained, no further action will be taken.

8.1.2 Non-quarantined infections

If the infection has not been quarantined, Cloudreach will investigate and manually contain the infection. Cloudreach will communicate all the details of the security incident to the Customer.

9 Services Management Support

Cloudreach will provide maintenance, troubleshooting, support and service management to ensure the availability and accessibility of the Customer's environment(s) in the Public Cloud. This section covers the service management Cloudreach will provide to the Customers as part of Infrastructure Reliability.

9.1 Incident Management Process

9.1.1 Incident Management Guidelines

Cloudreach and Customer shall adhere to the following guidelines as part of the Incident Management Process:

- All Incidents raised by Customer will be logged with Cloudreach and will be categorised as per the Priority table (see "Incident Prioritisation" table below) in the manner described below:

Priority	CSD Access Level	Log incident by email support@cloudreach.com	Log incident through webportal**	Log incident by telephone*
P1	24X7	X	X	✔
P2	24X7	✔	✔	✔
P3	24x5	✔	✔	✔
P4	24x5	✔	✔	✔
P5	24x5	✔	✔	X

*[UK] 0800 612 2966, [Overseas] +44 207 183 3991 or [US/Canada] (212) 335-0700

**webportal can be found at support.cloudreach.com using login details provided by Cloudreach during the onboarding process

  - The CSD can be accessed on a 24/7 basis to assist with P1 and P2 Incidents in the manner set out below. An Incident can be logged by the Customer or Cloudreach either through:
    - (i) emailing Cloudreach at support@cloudreach.com;
    - (ii) calling [UK] 0800 612 2966, [Overseas] +44 207 183 3991 or [US/Canada] (212) 335-0700;
    - (iii) the web by logging in to support.cloudreach.com using login details provided by Cloudreach during the onboarding process; or
    - (iv) mutually agreed automated event process.

  - For P1 Incidents specifically, the CSD can be accessed on a 24/7 basis only by telephone through the numbers as set out above. For the avoidance of doubt, P1 Incidents cannot be raised by email or through the CSD web portal.

- Customer can access CSD only by a designated Customer employee ("Support

Engineer") raising an Incident.

- Cloudreach is under no obligation to respond to Incidents made in a manner which does not comply with this section. CSD will use reasonable endeavours to find a work-around or solution to the Incident.
- When logging an Incident, Customer will provide to Cloudreach the following diagnostic information:
    - Detailed description of the issue
    - Customer Incident number
    - If available and reproducible, step by step instructions to reproduce the reported Incident
    - If available, date and time (and timezone) when Incident occurred
- Following the logging of an Incident, Customer shall be available via email or telephone to answer questions and assist the CSD as appropriate.
- Customer shall provide telephone or email access to the End User to facilitate troubleshooting Incidents.
- Customer shall provide access to End User support tools or permit Cloudreach to use their support tools to facilitate troubleshooting Incidents.

9.1.2 Incident Prioritisation

The following tables outline the prioritisation of Incidents and the description of each Priority Level.

Priority Level	Type of issue
P1 - Critical Impact	Total loss of service, no workaround available.
P2 - High Impact	Functional but degraded critical service or total loss for a service which supports a critical service. No work around available.
P3 - Medium Impact	Non critical service which is partially impacted and not functioning as intended.
P4 - Low Impact	Minor issue contained to a small group. A work around or alternative service is available.
P5 - Very Low	Impact and urgency are negligible and do not need to be resolved to improve or restore service, or general technical guidance.

9.1.3 Incident Response and Resolution Times

The table below shows the response and resolution times for each Incident Priority. For the purpose of this clause:

- “Response” is defined as Cloudreach acknowledging the Incident by (i) providing a Cloudreach reference number either electronically or verbally to the Customer and (ii) assigning a priority to the Incident.
- “Resolution” is defined as Cloudreach providing a reasonable workaround or solution to the Incident.
- The time for Resolution starts at the same time as the Response time.
- SLA for Response and Resolution times start ticking when an Incident is logged by a Customer (either by phone, email or through the CSD web portal) or when Cloudreach is alerted of a service impact via its monitoring system.

Priority	Target Response Time	Target Resolution Time
P1	15 mins (24x7)	4 hours (24x7)
P2	30 mins (24x7)	8 hours (24x7)
P3	1 hour (24x5)	24 hours (24x5)
P4	4 hours (24x5)	3 Business Days (24x5)
P5	1 Business Day	Reasonable endeavours

9.2 IT Change Management

9.2.1 Change Definition

A Change is defined as the addition, modification or removal of anything that may have an effect on service. The scope includes changes to all architectures, processes, tools, and metrics.

Cloudreach has defined three change types:

Change Type	Description
Normal	A Normal change is a pre-planned change that has been properly coordinated between the customer and Cloudreach. Normal Change requests follow a prescriptive process which requires two levels of approval before being implemented, reviewed, and closed. These changes are most often scheduled outside of defined change blackout windows or during defined maintenance windows.
Standard	A Standard Change is a routine, low-risk, often-done change to the production environment that has been pre-approved by the customer and/or authorised Cloudreach team(s)
Emergency	Emergency changes are defined as changes that need to be evaluated, assessed, rejected or approved, and implemented in a short span of time. Emergency Changes are ONLY performed as a result of an existing or imminent Incident or Problem. Occasionally, emergency changes are also requested to apply urgent vulnerability patches to systems in response to virus or attack activities.

9.2.2 Cloudreach responsibilities

- Cloudreach shall use reasonable endeavours to agree the IT Change Management process with the Customer;

- Cloudreach will only implement Change Requests to the Customer Cloud Platform which are in accordance with the IT Change Management process;

9.2.3 Customer responsibilities

- Customer shall log all required changes made to the Customer Cloud Platform with Cloudreach using the mutually agreed IT Change Management Process;
- Customer shall provide Cloudreach with all necessary Public Cloud Environment and Private Cloud Environment services requested by Cloudreach in order to effect the Change Requests in accordance with the IT Change Management Process
- Customer shall only provide Cloudreach with the credentials required to access the Customer Cloud Platform to complete work authorised through the IT Change Management process

9.2.4 Change Catalogue

Cloudreach will provide a change catalogue upon request from the Customer. This will be a separate document that will contain details and specifics of the available changes for the Customer.

10. Continuous Improvement

10.1 Service Overview

Continuous Improvement provides the customer with remote access to Improvement Engineers. Continuous Improvement is included in the Infrastructure Reliability Monthly Charges when (i) the Customer's Monthly Spend equals or exceeds $25,000 unless otherwise specified in the order form and (ii) the number of hours of Continuous Improvement available is set out in the order form.

Continuous Improvement is available during Business Hours only (9x5). Hours used are inclusive of scoping and implementation and single tasks >5 hours will be out of scope.

Continuous improvement is based on the operational running of the customer estate and is specific to the following areas.

- Cost Improvement
- Security Improvement
- Operational Improvements

10.1.1 Cost Improvements:

Cost improvement's activities are focused on improving the running costs of the customer estate.

Cloudreach will present the Customer with multiple showback reports based on their cloud spend:

- The Customer will define the required cost allocation groups. These groups can represent breakdowns for sub-organisations, business units or services the Customer offers;

- The Customer shall notify Cloudreach in writing of the cost allocation group stakeholders, business units or sub-entities (and appropriate contact, address and tax information) who will receive showback reports for each Group;

- The Customer will agree to the format of each report in either PDF or CSV.

Changes to the defined cost allocation groups, stakeholders or other details will be submitted by the Customer to the Cloudreach Service Desk, as a Billing and Optimisation Support Request, following the Incident raising process described in the Support section further below.

Examples of cost improvement activities include the following:
- Solution rightsizing
- Instance scheduling
- Remove orphan resources
- Action to be taken in the event of an alert (Instance shutdown / Instance termination / S3 resource removal / alert only).

10.1.2 Security Improvements:

Cloudreach will work to identify security risks across customer's supported instances and infrastructure in order to provide greater security posture with customer environments and ensure the reduction of attacks and risk.

Cloudreach will scan the customer's environment once per year and provide threat and vulnerability analysis, with recommendations.

Example security improvements we will remeditate:
- Reviewing & removing orphan security groups
- Orphan load balancers

10.1.3 Operational Improvements:

Identification & execution of operational improvements across the Cloudreach supported customers' estate. These improvements can vary from improvements that can be executed through our operations team.

Example operational improvements:
- OS upgrades identification and remediation
- Patching and backup scheduling - Not applicable to hours, we will just report on this.
- Instance rightsizing
- Optimizing Services Utilization (eg EC2 with a database on it to rds)
- Identifying Single Point Of Failure (Load balancing, or ASG Implementation)
- Noise Reduction
- Automation - Infrastructure-as-Code template, where Cloudreach could undertake the task of moving management of resources into source code.
- Applying effective backup lifecycle policies following a life and shift migration.
- Baking a new image for a containerised application.
- Exposing metrics and logs to an external performance aggregation tool.
- Updating a pre-existing pipeline to include IaC testing.
- Adding new or removing resources e.g. VMs during the life of the service;
- Create & Update AWS CloudFormation templates;

- Create or update Configuration Management resources;
- Create & Update Azure Resource Manager templates;
- Implementation of financial optimisation recommendations / actions;
- Deployment cycle auditing and;
- Operational task automation.

10.2 Improvement Request Fulfillment

The SDM shall request a technical, security and cost investigation to take place, a report shall be produced on continuous improvement items that can be actioned. Based on these reports, the SDM shall collate a plan, to deliver continuous improvement to the customer's infrastructure, based on their priorities.

The SDM shall also take input from the Customer who may suggest improvement on their infrastructure.

The high level steps and activities will be as follows:

- The Service Delivery Manager raises a Service Now request for initial investigation into potential continuous improvement items
- These reports are reviewed with the customer, a continuous improvement register is created with a list of priority items
- The Service Delivery Manager shall create a request(s) for Infrastructure Reliability continuous improvement items to be actioned by opening a service request(s) on behalf of the customer, and informing the customer via email, phone, or self-service;
- Cloudreach will prepare a Continuous Improvement Service Request (CI) and present that to the customer to agree the improvement activity;
- If the customer decides to proceed with the CI, the Service Delivery Manager will provide a proposed date to deliver the CI. There is no associated SLA Resolution Target for continuous improvement;
- The Service Delivery Manager will communicate via email or telephone before the actual day of implementing the CI;
- Should the RCI not be successful, the Service Desk in conjunction with the Service Delivery Manager, will revert back to previous state prior the CI and keep the customer informed at all times;
- If the customer decides not to proceed with the CI, the Service Delivery Manager will not schedule the CI and will keep it in a backlog and will be reviewed again.

Improvements can also be raised by any member of the operations team if and when identified and work can be executed through Operations engineers where improvement hours are available. This should follow our standard change management process.

10.3 Reporting

The Service Delivery Manager will include a summary of continuous improvement items completed and the effort spent during the previous month in the monthly service report.

These improvements will be captured through requests within service now and executed alongside agreed change windows and process with the customer.

10.4 Out of Scope: Continuous Improvement Exceptions

Customer acknowledges and understands that continuous improvement may not be used to perform tasks which are explicitly listed in the Standard Change list which will be provided upon request.

For the avoidance of doubt, Cloudreach may not be able to perform certain tasks under the following circumstances:

- Requests that are not covered within section 10.1 but will be considered on a case by case basis;
- Requests that negatively impact the security of the Customer environment;
- Changes that are unrelated to the support of components/ resources/ instances within the Customer's cloud platform;
- Large projects such as application refactoring and infrastructure modernisation. (Large projects are defined as pieces of work that are >5 hrs inclusive of scoping and implementation)

Examples of improvements that may require further scoping and professional services include:

- Technology changes (CSP to CSP) (Serverless)
- Creation of new landing zones
- Migration of services

11. Cost Management

A summary of the key components of Cost Management are listed below:

- **Financial Governance and Accountability** - Established governance, ownership, tagging policies and budget tracking, aided with monitoring and automation;
- **Reporting and Data Visualisation** - Reports pertaining to Customer's relevant cloud spend;
- **Cost Optimisation** - Continuously identifying cost optimisation opportunities

11.1 Management of the Customer CloudHealth Tenant

Upon request from Customer, the FinOps Delivery team will:

- Configure and setup a CloudHealth tenant on behalf of the Customer, reviewing all requirements as captured within a billing workshop, including:
    - Standard reports;
    - Custom reports;
    - Budget alerts.

- This setup will comply with any limits of the Service as outlined in Appendix A to this Service Specification.

The FinOps team will manage the CloudHealth tenant by:

- Configuring, maintaining and updating any email alerts and distributing reports to key Customer stakeholders as agreed in writing with the Customer;
- Updating the permissions to the Cloud Provider Accounts to ensure the necessary cost, performance and usage data is being ingested into the CloudHealth platform;
- Reviewing cloud consumption and usage with the Customer on request. Meetings are limited to one per quarter. If a Customer requires a higher frequency, this should be outlined at the billing workshop.
- Utilising the CloudHealth platform to obtain resource performance and financial optimisation data to feed into Cloudreach processes to develop optimisation roadmaps.

11.1.1 Financial Governance and Accountability

In order to assist with effective and accurate billing and optimisation reports, accountability tagging policies are established and monitored. Notifications pertaining to the compliance of these policies will be delivered automatically on a scheduled cadence as jointly defined by Cloudreach and the Customer.

11.1.2 Governance and Accountability Policies

Cloudreach can report the tagging status of AWS EC2, EBS, RDS and S3 resources plus Azure Resource Groups, Virtual Machines, Storage Accounts, SQL Servers and SQL Databases and upon request will:

- Review up to five custom tag alerting schedules as agreed with Customer during Onboarding. Additional tag alerting schedules may be reviewed by the Cloudreach FinOps Delivery team subject to the limits agreed in advance.
- Each alert schedule is customisable in the following manner:
    - Combination of tags to be monitored;
    - Exception criteria (presence/absence, format of tag value);
    - Audience to receive alert, which may be one or more Customer-supplied email addresses;
    - Frequency of re-alerting in event of continued non-compliance (in hours, days or weeks, with a maximum frequency of 4 hours); and

11.2 Reporting and Data Visualisation

- Cloudreach provides detailed showback capabilities by breaking down cloud spend data as per defined cost allocation policies;

- Cloudreach offers detailed reports based on a number of facets of billing data and common breakdowns. Customers can also customise reports via Cloudreach upon request;
- Budget Tracking and Alerting monitors expenditure and provides monthly reporting of budget allocation performance and alerting when actual and predicted spend exceeds defined thresholds.

11.2.1 Reporting

Cloudreach will provide automated detailed reporting based on a number of facets of billing data. Cloudreach shall provide the predefined reports listed below in "Standard Reports" using common report criteria. Billing data for the reports is updated daily. Report data can be presented in a number of different formats, including as graphs and as CSV for ingestion into the Customer's business systems.

11.2.2 Standard Reports

The following standards reports can be generated daily, weekly or monthly (as applicable and upon request) and available to view by the Customer:

For AWS:

Report Name	Description
Per Cost Allocation Group	Report showing spend in each Cost Allocation Group
Per AWS Service (e.g. EC2, S3)	Report showing spend for each AWS Service
Per AWS tag (e.g. where tag=value)	Report showing spend for each tag value.
Product-per-time-period (e.g. EC2 spend per day/week/month)	Reports by day/week/month showing spend for each AWS product.
Product-per-usage-type (e.g. spend per m3.large EC2 instance)	Report showing spend for each instance type in EC2
Product-per-resource-placement (e.g. spend in eu-west-1a)	Report showing spend for each AWS product in each region or availability zone
Spend-per-purchase-option (e.g. spend by Reserved Instance)	Report showing spend for on-demand instances vs spend for reserved instances

For Azure:

Report Name	Description
Per Cost Allocation Group	Report showing spend in each Cost Allocation Group
Per Azure Service (e.g. VMs, Blob storage)	Report showing spend for each Azure Service

Per Azure tag (e.g. where tag=value)	Report showing spend for each tag value
Product-per-time-period (e.g. VM spend per day/week/month)	Reports by week and month showing spend for each Azure product
Product-per-usage-type (e.g. spend per Basic_D6 VM)	Report showing spend for each VM sub-category
Product-per-resource-placement (e.g. spend in West Europe)	Report showing spend for each product in each region

For GCP:

Report Name	Description
Per Cost Allocation Group	Report showing spend in each Cost Allocation Group
Per GCP Project	Report showing spend for each GCP Project
Per GCP Service (e.g. GCE)	Report showing spend for each GCP Service
Product-per-time-period (e.g. VM spend per day/week/month)	Reports by week and month showing spend for each GCP product

During Onboarding, the Customer can choose to receive these reports by email.

Reports can be delivered in a number of different formats:

Format	Details
PNG	Graphs and summaries only
CSV	Tabulated data only, without graphs

11.2.3 Custom Reporting

The Customer may request the configuration and generation of up to five custom reports based on a wider range of dimensions including:

- **Billing period** (e.g. 1st October - 30th November)
- **Aggregation period** (e.g. Daily)
- **Cost Allocation Group** (e.g. development accounts)
- **Provider Account** (i.e A single cloud provider Account)
- **Service** (e.g. EC2, Azure Virtual Machines, etc)
- **Usage type** (e.g. AWS m4.large, Azure Standard_F1, etc)
- **Tag** (e.g. BU="IT Services")
- **Resource placement** (e.g. AWS eu-west-1, Azure North Europe, etc)

Once configured, these reports shall be delivered to the Customer in accordance with a delivery plan (e.g. daily, weekly, etc) of their choosing.

11.2.4 Budget Tracking and Alarms

Cloudreach shall help allocate annual budgets and monitor expenditure for the Customer's Provider Accounts by providing a monthly summary to each invoice stakeholder illustrating the spend to date compared with the budget provided by the Customer. The summary will show:

- Cost Allocation Group name;
- List of Provider Accounts;
- Annual budget;
- Budget starting month;
- Actual spend this month;
- Actual spend since start of budget period;
- Budget rate of spend graph.

During Onboarding, the Customer can choose to have a notification sent by email in the event that the costs reach either one of two thresholds defined by the Customer.

The notification email will show:

- Budget Group name;
- Alarm name;
- Current percentage of budget.

Example thresholds:

Alarm name	Threshold
Warning	80% of pro-rated annual budget
Critical	95% of pro-rated annual budget

11.3 Cost Optimisation

Cloudreach can generate a monthly financial optimisation report consisting of Rightsizing and Reservation recommendations, identifying orphaned and underutilised AWS EC2 and/or Azure Virtual Machine resources and performing AWS cloud resource scheduling.

With the aim of reducing monthly spend, Financial Optimisation provides actionable and validated optimisation measures specific to customer requirements. This includes:

- AWS EC2, Azure Virtual Machine and GCP GCE rightsizing-reservation recommendations;
- AWS RDS, ElastiCache and DynamoDB reservation recommendations;
- AWS and Azure orphaned resource removal;
- AWS and Azure underutilised resource removal;
- AWS EC2, ASG, RDS, Aurora, Redshift, Azure VM or GCP GCE scheduling to customer defined schedules.

11.3.1 Rightsizing and Reservation Recommendations

As part of the monthly financial optimisation report, Cloudreach will produce cost and performance-based rightsizing and reservation recommendations detailing:

- AWS EC2 Instances, Azure Virtual Machines or GCP GCE Instances currently receiving benefit from existing reservations;
- Where performance-based utilisation criteria are available, AWS EC2 Instances, Azure Virtual Machines or GCP GCE Instances that are potential targets for rightsizing and subsequent reservation, and approximate savings to be made by by rightsizing and reservation;
- Where performance-based utilisation criteria are available, AWS EC2 Instances, Azure Virtual Machines or GCP GCE Instances that are potential targets for rightsizing only, and approximate savings to be made by rightsizing;
- (AWS-only) Elasticache Instances which are potential targets for reservation, and approximate savings to be made by reserving;
- (AWS-only) DynamoDB tables which are potential targets for capacity reservation, and approximate savings to be made by reserving; and
- (AWS-only) RDS Instances which are potential targets for capacity reservation, and approximate savings to be made by reserving.

11.3.2 Orphaned and Underutilised Resource Termination

As part of the monthly financial optimisation report, Cloudreach will include details of:

- (AWS and Azure) Orphaned storage volumes that can be decommissioned and the approximate savings to be made by decommissioning;
- (AWS-only) Orphaned, aged or excessive number of EBS snapshots in relation to customer defined snapshot limits or backup policies that can be deleted and the approximate savings to be made by deletion;
- (AWS and Azure) Unused IP addresses which can be deleted and the approximate savings to be made by deletion;
- Underutilised EC2 instances or Azure Virtual Machines that are candidates for stopping/terminating and approximate savings to be made by stopping/terminating.

Within the monthly optimisation report, Cloudreach will attempt to include identification of resource owners by tag (where applicable), if the Customer has applied a tag containing an email address (or other similar identifiers) pertaining to the resource owner. In such cases, Cloudreach will liaise with the primary Customer cost management contact to validate the recommendations listed in the optimisation plan.

Upon validation of the recommendations identified in the monthly report, Cloudreach can liaise with Customer resource owners to help them review recommendations of the monthly optimisation plan.

11.3.3 Cloud Resource Scheduling

Cloudreach will deploy tag-based autonomous start/stop scheduling tooling within the Customer's AWS, Azure or GCP environment and will assist in configuring custom scheduling rules as agreed with the Customer during Onboarding. Cloud Resource Scheduling is subject to tooling dependencies described in section 11.4.

11.3.4 Optimisation and Insight Reporting

As part of the monthly optimisation reports, Cloudreach will include a high-level headline report, identifying spend hot-spots, including:

- Identifying the delta in overall spend in terms of percentage, dollar or billed equivalent increase or decrease in spend since the previous month;
- Identifying the primary cloud services that contributed to the increase or decrease in spend since the previous month;
- Identifying any subsets of total spend (for up to two Customer-nominated tag keys) where the delta in spend for the subset varies by more than or equal to a customer-nominated minimum variance value;
- Providing a breakdown of usage corresponding to their respective budgets.

Additional Customer custom reports may be added by the Cost Management Delivery Team.

11.3.5 Financial Optimisation Workshop

Cloudreach, upon request, can provide the Customer with one "Financial Optimisation Workshop" every quarter. This Financial Optimisation Session will:

- Provide basic information on the key concepts of public cloud billing and financial optimisation to key Customer stakeholders;
- Discuss customer progress in financial optimisation;
- Review and identify new opportunities for ongoing financial optimisation activities;
- Provide a strategy/roadmap for financial optimisation efforts moving forward.

The workshop should be coordinated with the Customer's nominated SDM and will be delivered remotely/virtually.

11.4 Dependencies

11.4.1 Dependencies

The services provided are dependent on the existence of an existing CloudHealth license either as procured by Cloudreach on behalf of the Customer or by the Customer granting access to a pre-existing Customer CloudHealth tenant (if applicable).

Section 11.3.3 (Cloud Resource Scheduling) is dependent on the existence of an existing ParkMyCloud license either as procured by Cloudreach on behalf of the customer (and subject to relevant pricing) or by the Customer granting access to a pre-existing Customer ParkMyCloud tenant (if applicable).

11.4.2 Limits

Cloudreach imposes the soft limits identified per section as listed [in Appendix A (the "Limits")] in respect to this section 11. If Customer exceeds the Limits, Cloudreach shall notify Customer and work with Customer to understand the reason for exceeding the limits and attempt to find a solution or workaround. If Customer consistently and regularly exceeds the Limits, as determined by Cloudreach, Cloudreach shall be entitled to charge the customer an additional fee for the exceeding of Limits.

12. Service Delivery Management

The Service Delivery Manager (SDM) is responsible for owning Customer experience and delivering the service management outcomes associated with Managed Services provided by Cloudreach. The SDM provides the following services:

- Strategic business alignment - The SDM shall work with the Customer to ensure the operational services are delivered in line with the business objectives of the Customer. They shall also manage the business relations the Customer has with Cloudreach to enable delivery of services.

- Business critical IT service management – The SDM shall provide dedicated management of business-critical IT service management. They shall be the point of escalation and ensure the appropriate priority, resource, and associated governance is in place to progress to resolution.

- Proactive service reviews - Owned by your dedicated service delivery manager focusing on business as usual reporting and identifying and driving improvements recommendations.

- Continuous service improvement - The SDM shall implement a continuous service improvement plan. The plan shall cover recommendations, for example, on processes, procedures and run book improvements with action plan(s) mutually agreed with the Customer.

12.1 Service Review Meetings

The SDM will conduct and chair a monthly service review meeting with the Customer at a time and place to be mutually agreed in advance by the parties. The agenda for the service review shall include:

- Review service report management summary and discuss any points including but not limited to Cloudreach or Customer actions;
- Review Incidents, Problem(s), and Change Request(s) records, review performance and capacity issues identified (if applicable);
- Review status of existing, and any new mutually agreed, service improvement(s);
- Make recommendations for improvements of the service which have been identified by Operations team

12.1.1 Service Reports

Cloudreach shall provide Customer with a monthly service report in Google Docs format or PDF . The monthly service report shall include:

12.1.1.1 Management Summary

- Amazon Web Services (AWS) and Microsoft Azure performance summary: overall status plus availability and performance concerns, if any, on the following components: Cloud service availability, Instance CPU, memory, and network load;
- AWS and Azure security: overall status plus any security concerns, if any, for the following components: Instances in VPC, Security Groups, 2 factor authentication;
- Instance patching: overall status plus any security and compliance concerns ;
- Instance backups: overall status plus any business continuity concerns

12.1.1.2 Service Management

- Incident record summary including:
    - Current open Incident records and/or Service Catalog Requests
    - Recently closed Incident records and/or Service Catalog Requests
    - Summary of Incidents by priority and/or Service Catalog Requests
    - Summary of Incidents by component and/or Service Catalog Requests
- Problem record summary:
    - Current open problem records
    - Recently closed problem records
- Change Request record summary:
    - Pending Change Requests
    - Recently closed Change Requests
- SLA compliance summary
- Escalation Matrix
    - This lists the people and teams within Cloudreach and the customer organisation to contact and escalate an incident or an issue for example that remains unresolved at a support level

12.1.1.3 Performance Management

- Description of notable performance and/or capacity issues
- Performance charts from Cloudreach, AWS and/or Azure monitoring tools to support issues
- Information on cause of issue, if known
- Recommendations to remove or prevent future issues, if known

12.1.1.4 Cloud Environment Management

- Cloudreach will capture a view of customer cloud environment and provide the snapshot of it to customer via monthly service reviews;

- Cloudreach will provide a monthly report of the cloud environment compliance based on specified policies and criteria, for example:
    - Configuration management compliance (backups, patching)

12.2 Service Improvement Initiatives

- Cloudreach and / or Customer actions and risks aimed at improving the quality and performance of the managed service;
- The SDM shall implement a continuous service improvement plan that covers recommendations for example, on processes, procedures and run book improvements with action plan(s) to be mutually agreed with the Customer;
- Maintain and update Customer contact information;
- Cloudreach will provide Customer with trending analysis in the quarterly and bi-annual service review meetings

12.3 Custom

Any service reporting that requires additional work to customise to Customer's requirements i.e. requires additional data to be collected and/or produced will be assessed and may be subject to additional charges

12.4 Service Review Timetable

Deliverable	Frequency
Introductions and Review of the Cloudreach Escalation Matrix Guideline	Kick Off
Conduct Monthly Service Review (Onsite or Remote)	Monthly
Provide Monthly Service Reports	Monthly
Provide Quarterly Service Report (trend reports for the quarter, analysis and recommendations)	Quarterly
Provide Annual Service Report (trend reports for the year, analysis and recommendations)	Annual

13. Offboarding and retention of customer data

The table below details the type of customer information that Cloudreach requires for the provision of the services and how such information is handled upon termination of a customer service contract.

Customer Data	Type of data	Retention (From Offboarding Date)	Retention During Contract	Format / method of transfer or deletion (if applicable)

Personnel Email Address	Identity contact	Up to 45 days	Duration of contract	Deletion from internal systems (ServiceNow, Cloudreach Confluence)
Personnel Phone Number	Identity contact	Up to 45 days	Duration of contract	Deletion from internal systems (ServiceNow, Cloudreach Confluence)
Personnel Name	Identity contact	Up to 45 days	Duration of contract	Deletion from internal systems (ServiceNow, Cloudreach Confluence)
Personnel Title	Identity contact	Up to 45 days	Duration of contract	Deletion from internal systems (ServiceNow, Cloudreach Confluence)
Ticket Data	Ticket	13 Months	Duration of contract	Deletion from internal systems (ServiceNow)
CINC data	Configuration Attributes	Up to 45 days	12 Months	Deletion from internal systems (Cloudreach CINC Server)
Performance data	Monitoring	Up to 45 days	13 Months	Deletion from internal systems (Cloudreach Splunk Observability Cloud (was SignalFX))
Log data	Monitoring	Up to 45 days	90 days	Deletion from internal systems (Splunk Cloud)
Trace data	Monitoring	Up to 45 days	13 Months	Deletion from internal systems (Splunk Cloud)
Incident Data	Monitoring	Up to 45 days	Duration of contract	Deletion from internal systems (PagerDuty)
Instance Metadata	Monitoring	Up to 3 months	Duration of contract	Deletion from internal systems (Conductor)
Access credentials to CSP	Access	Up to 45 days	Duration of contract	Deletion of Cloudreach roles from CSP
Switch role	Access	Up to 45 days	Duration of contract	Cloudreach or customer will remove switch role access and this includes any individual IAM accounts in the customer account
PEM keys	Access	Up to 45 days	Duration of contract	Deletion from internal systems (Jungle Disk)
AMI snapshots	Backup	Up to 45 days, unless otherwise agreed	As agreed with the customer	Deletion from AWS console, unless customer wishes to retain these
WSUS data	Monitoring	Up to 45 days	Duration of contract	Deletion from Cloudreach WSUS Server and reset of registry keys

Alert Logic data	Monitoring	Up to 45 days	13 months	Deletion of customer tenant from Cloudreach Alert Logic
Crowdstrike data	Monitoring	Up to 45 days	Duration of Contract	Deletion of customer tenant from Crowdstrike Portal
Source Code	Customer IP	Up to 45 days	Duration of contract	Deletion of any customer source code from Customer source code repositories or transfer ownership of repositories if applicable

14. Document Management

14.1 Revision History

Version	Description of Changes	Revision Date
3.1.3	Addition of Change Definition CrowdStrike as new EDR	December 2021
3.1.4	Removed references to Chef Updated section 5.2 OS Upgrades	April 2022

14.2 Approvals

This document requires the following approvals:

Name	Title	Approval Type	Approval Date	Version
Stephanie Leopold	Head of Compliance	Global Sign off	29/04/2022	13.3.4
Andy McBride	Director of Cloud Operations	Global Sign off	29/04/2022	13.3.4
Caroline Griffiths	Senior Product Manager	Global Sign off	29/04/2022	13.3.4

Appendix A - Cost Management Soft Limits

Service	Limit
Onboarding Workshops	1 three hour session delivered remotely/virtually.
Training sessions on the Billing Dashboard. Additional training sessions can be delivered upon mutual agreement between the Customer and Cloudreach and may be subject to additional charges.	5 one hour sessions.
Monthly Reviews	1 to be delivered remotely/virtually - this will be scheduled subject to the finalisation of usage and billing data provided by the Cloud Provider.
Budget Alarms. Additional Budget Alarms shall be mutually agreed between the parties subject to the charges in an order form.	15
Additional custom **Billing and Financial Optimisation Reports (per 11.2.3)** prepared by the Cost Control Delivery team. Additional reports shall be mutually agreed between the parties subject to the charges in an order form.	5 reports per month via the Billing Dashboard
Cloud Resource Scheduling rules. Additional Cloud Resource Scheduling rules shall be mutually agreed between the parties subject to the charges in an order form.	5
Tag Alerting Schedules. Additional Tag Alerting Schedules shall be mutually agreed between the parties subject to the charges in an order form.	5