CIRRO

Service Description

G-Cloud14

v1.0

Document Overview

This is a Service Overview for Services on G-Cloud, at Cirro we believe in delivering excellence to our customers. And in providing high-quality, complementary services. We build projects using external experts in many cases and create highly functional virtual teams, so you can be sure to get the best people, services and value for money. This combination and focus ensure you can deliver your desired outcomes efficiently and effectively.

Whilst this is a generic document for G-Cloud, we welcome the opportunity to detail our service capabilities, and be flexible with terms, pricing and working methodologies to suit our customers' needs.

Getting started with Cirro

Each project has a Statement of Work, which details the:

- Onboarding process
- Roles & responsibilities
- Prerequisites
- Service Scope, Options & Deliverables
- Your Obligations
- Our Obligations
- Data Protection, Security, Standards
- Data Ownership & Management
- Project-specific terms & conditions

Termination

Termination during the contract period is typically based on the following criteria:

1. Continual or non-remedial Default – where a catastrophic event results in a loss of Service which we cannot recover from, fix or continue to provide the agreed Service
2. Continual missed SLA – where the contracted SLAs are not met, typically multiple times within a period, such as twice in a quarter or four times in any twelve-month period.
3. Achievement of Minimum Spend Commitment – where a payment threshold has been met

At the end of the initial service term, we naturally hope customers will continue with us and renew the services for an extended period. However, as and when a customer terminates or the term ends. We will offer our professional services to ensure a smooth transition to an alternative provider. Cirro can also offer certified data destruction

Pricing Overview

At Cirro we like to keep pricing as simple as possible. We don't like it when suppliers hide charges or look to make money on the much-needed extras, so our pricing promise is to be open and transparent and to make sure our customers know what they are getting and what the service will cost. Importantly, we like to ensure that customers know what they need to do and we highlight any gaps.

This pricing document details how we charge for our services. Which is typically license-based with some professional services and some hardware fees. For each project, we provide a Sales Order a Statement of Work or a detailed proposal. Our services, whilst standardised as much as possible, are generally very configurable. We do this because we want to ensure our customers get the most relevant services for their needs. This is

probably why we have such a long average customer duration with very low customer churn.

All pricing is in UK sterling and excludes tax and should be used as a guide only. All services are quoted against your specific requirements.

Unless stated otherwise the price is a monthly service charge and is per unit measure per month. Pricing is based on a minimum term commitment which is typically 24 months of invoiced service.

Pricing Summary

Lot 1 - Hosted Services

Our pricing for Lot 1 is typically utility-based on a per unit per month basis, with typically some options for professional services, charged per day or per hour. Additionally, SaaS and Support options are also potentially available.

Lot 2 - Software as a Service

Pricing is typically based on the number of users, devices or quantity and based on a per unit per month, with options for support and professional services.

Lot 3 - Support

Here our professional services are available, typically on a Time & Material (T&M) basis, generally at a day rate.

Licensing

Every project will detail the licensing requirements for the deliverables. Usually, Cirro licenses all application and system elements on behalf of the customer, unless agreed or detailed otherwise.

Hardware

Some projects require dedicated hardware, these can range from low-cost IoT sensors to higher-cost Edge Data Centres or OT cybersecurity hardware. Ownership, warranty and

hardware options are detailed in the specific Terms & Conditions for the relevant sales order.

Intellectual Property Rights

By default, Cirro holds and retains all existing IPR, with Cirro-owned IPR being licensed for use to a customer where required to deliver a SoW. Where Cirro has been requested to create IPR or source code for a customer, a license agreement will be created to detail IPR ownership and any licensing or support arrangements, typically the customer will own the IPR.

Escalation Process

Cirro aims to achieve the highest levels of service and customer engagement. We provide a detailed SLA for every project and an escalation path to ensure our customers can get any issues dealt with as quickly and professionally as practically possible,

Level of Priority	Time to Escalate	Escalation Point
Priority 1	30m	Top Tier - Director
Priority 2	1 Hour	Top Tier - Director
Priority 3	2 Hours	Next Tier - Manager
Priority 4	12 Hours	Low Tier - Coordinator

Uptime & Service Credits

Services in Lot 1 and Lot 2 will typically have an SLA which would detail the expected service level availability and uptime. Options typically exist to increase the baseline uptime with ways of increasing service resilience or performance perimeters. Failure to

meet the agreed uptime or SLAs would result in a Service Credit being offered to any affected customer.

Service Credit Exceptions

Outages or incidents caused by a customer or a customer's user will usually mean a service credit is not available for that incident. Some force major events and other exclusions may apply.

Service Overview

Lot 1 Services

Infrastructure and hosted services are designed against requirements and typically over Microsoft Azure, Amazon AWS and Google Cloud, as well as other managed service providers such as Wasabi.

Cirro typically provides add-on services for the design, architecture, build, deployment, continual improvement, security or monitoring of these environments as a monthly managed service. Commercially, we generally charge a percentage of the total monthly spend to runtime service. We are also able to combine Lot 2 and Lot 3 services to deliver additional value and ensure the optimal outcomes are achieved.

Where Cirro acts as the CSP the customer must agree to the relevant terms & conditions of services from the provider regardless of any terms under G-Cloud. Cirro cannot offer alternative terms to those providers.

Cirro will however detail the services being delivered to the customer as a Statement or work, following is an example for Microsoft Azure:

Category	Sevice Description
DevOps	Deliver tested DevOps scripts and publish to Library
DevOps	Deploy updated DevOps scripts into environment
DevOps	Maintain Script Library
DevOps	Monitor Script Library
DevOps	Secure Script Library
Service Desk	Health Check - Daily health checks of all BigHand systems prior to 7am (in Country) to ensure that are no issues prior to the business day starting

Service Desk	Health Check - Microsoft's Service Status across all regions and assess and advise on any disruptions that could impact systems/DevOps services
Service Desk	Realtime monitoring and response for all BigHand Services
Service Desk	Realtime monitoring and response for BigHand workload monitoring
Service Desk	Cloud Configuration Monitoring and management
Service Desk	Routine Patch Management on any remaining Virtual Machines – troubleshooting errors, modifying patch groups, patch compliance reporting – Create custom patching scripts (pre / post)
Service Desk	Monthly maintenance (including Windows Updates)
Service Desk	Monitor Microsoft Updates, assess risks and implications
Service Desk	Realtime monitoring of Database data and log sizes across DAG members
Service Desk	Routine Database health checks
Service Desk	Logging of Incidents with parties – Incident Management
Service Desk	Triage of issues with parties & remedial action
Service Desk	1st Line Azure Infrastructure Support
Service Desk	Monitor & triage platform-based alerts
Service Desk	Azure-certified engineering support for configuration, monitoring, management & escalation
Service Desk	DNS status monitoring
Service Desk	SSL status monitoring
Network Ops	External networking monitoring for in country latency
Network Ops	External application port monitoring for application latency within country. Monitor latency in the BigHand App & in-country hops
Network Ops	BGP hop monitoring per country to assess and respond to stale peering links
Network Ops	24x7 Network Performance Monitor
Network Ops	24x7 networking triage, response, and escalation team
Network Ops	Post incident reporting and analysis carried out to understand and optimise network reliability
Security Ops	24x7 Security Operations Support & Analytics - – Including Design, access control & privilege management
Security Ops	24x7 SIEM Platform, Support & Analytics – monitoring & event management
Security Ops	24x7 managed cyber threat detection & response, including threat monitoring, management and prevention - Monitoring cyber security associations and threat control lists - Monitoring software vendor threat updates - Threat signature updates
Security Ops	Intrusion Detection & Prevention – management access, insider threat, RBAC, access auditing and logging
Security Ops	Realtime risk monitoring for misconfigurations – SOC monitoring & alerting

Security Ops	Realtime risk monitoring for application vulnerabilities – weekly risk scan report & remediation
Security Ops	Anti-virus - Weekly AV scan, report and remediation
Security Ops	Vulnerability and risk assessment and monitoring based on real-world cyber events / threats
Security Ops	Realtime human risk monitoring & analytics – Azure AD - Monitoring of anomalous or unique user behaviour
Security Ops	Monthly vulnerability scan of all environments (internal & external)
Security Ops	Monitoring and auditing of all user account activity throughout all systems - Monitoring of service account usage and file access and interactions
Security Ops	Monitoring and auditing of all user account activity throughout all systems - social engineering or interruption of supply chain/code injection
Security Ops	Monitoring and auditing of share permissions changes
Security Ops	Realtime monitoring for failed user logins – on VM's and instances
Security Ops	Quarterly firewall rule review and assessment - continual review of the NSG's validity
Security Ops	Continual rule development to identify and pick out risks and security issues between networks in each node
Service Availability	Design of business continuity solution – back-up, restore & fail-over policy planning, design, build & management
Service Availability	Traffic monitoring and DDOS mitigation planning, network planning & traffic forecasting
Service Availability	Management of back-up routines & jobs - troubleshooting – VM's, databases, logs, replica's
Service Availability	Failover testing, documenting, risk reduction & service improvement
Service Availability	Subscription management – reserved capacity
Subscription Management	Cost Reporting & management – Pro, Non-Prod
Subscription Management	Billing, billing support
Subscription Management	Spend forecast & trend analysis
Subscription Management	Subscription Management & optimisation – ECIF funding
Service Management	Incident Management & Reporting – (Security, network, infrastructure, systems, risks, spend)
Service Management	SLA Management & Reporting
Service Management	Root Cause Analysis, Investigation & Resolution, Preventative measures & improvements
Service Management	Change Control Process – review & assess change requests
Service Management	Regular service reviews - continual improvement
Service Management	Capacity management & planning
Service Management	Future technologies – Azure updates – new services

Service Management	Compliance & conforming to ISO 27001, documenting & evidencing
Dashboard	Management dashboard with summaries and drill down spend analysis based on data tags
Dashboard	Resource & spending monitoring
Dashboard	Realtime view of user sessions and event states
Dashboard	Traffic flows between services
Dashboard	Monitoring, logging and escalation of all SSL Certificate renewals
Dashboard	Service performance & traffic light reporting
Dashboard	Rule development - identify and report on Event's or State changes – create & manage rules
Dashboard	Compliance & Governance reporting based on rules & policies

Managed Wasabi S3 Storage

Wasabi immutable S3-compatible cloud object storage offers unparalleled security, speed, and savings for your data protection and recovery plan. Data management teams love being able to test and retrieve their backups without being penalized with extra fees, while Infosec appreciates our multi-layered approach to security. With the industry's only multi-user authentication account control, no single person, not a hacker or an account administrator, can delete a Wasabi storage account alone.

Data migration tools

Whether you're pushing petabytes off-prem or want out from expensive hyper scale clouds, Wasabi has the tools to make it seamless. We'll even take care of your egress fees.

Integrating Wasabi

Wasabi is 100% AWS S3 and IAM API compatible, making it an ideal drop-in replacement or secondary storage target for your next hybrid or multi-cloud deployment. Our validated integrations with the industry's most popular S3-compatible applications ensure a simple, seamless and optimised user experience. No heavy lifting. Just fast, efficient, and cost-effective cloud storage.

Getting started with Wasabi

Wasabi is designed for organisations that require a high-performance, reliable, and secure data storage infrastructure at minimal cost.

Wasabi stores data as objects in a bucket. An object consists of a file and, optionally, any permissions and metadata that describe the file. A bucket is a storage container into which you upload your files. You can have one or more buckets and, for each, you can:

- Control access to it (who can create, delete, and list objects in the bucket)
- View access logs for the bucket and the objects it stores

AI, HPC and Big Data - Green Data Centre in Norway

Cirro has an office in Norway and collaborates with several distributed High-Performance Data Centres to deliver HPC, high-end multi-media GPU and AI-designed colocation facilities based on Norwegian hydro-power. Each solution is designed for customer requirements. Technically Norway is outside of the EU however it sits within the EEC and complies with EU regulations. Making it attractive as a security, remote, data centre location.

Multi-Media Edge Compute (MEC) to Cloud to Edge

Cirro has several prominent relationships that support Edge to Cloud. Our service capabilities mean that through our partners, we can deploy edge modules, to act as on-site data centres or as city deployments for next-generation services. We can also combine these edge locations with our cloud capabilities to create hybrid cloud solutions. Edge services can be leased, lease-purchased or purchased outright. Under Lot 3, we can provide managed services and Edge management software to support the entire solution.

Operational Technology (OT) Cyber Security

Working with our specialist partner, Industrial Defender who focuses solely on OT cyber security and has industry-leading solutions which allow customers to:

1 - Have full visibility of OT assets

The ability for organisations to properly and consistently identify and consistently manage data, personnel, devices, systems, and facilities based on their relative importance to provide the foundational capability to support an organisational cybersecurity program

2 - Monitor Configuration and Change Management

Understanding what changes (and why) is critical to both safety and security. Change and configuration management is a crucial process that ensures the secure configuration of systems and evaluates any changes for potential security risks and compliance issues.

3 - Simplified Compliance Reporting for OT Environments

Automate manual compliance tasks with a suite of built-in policy management options and one-click compliance reporting for dozens of international standards.

4 - Reduce risk with OT Vulnerability Management

When assessing vulnerabilities in ICS/OT environments, a different approach is required compared to traditional IT. Industrial Defender recognises the unique design, context, and critical nature of OT assets, offering an operationally safe method for identifying and prioritising vulnerabilities. Our platform provides an accurate, complete, and up-to-date view of vulnerabilities across your OT environment and intelligently prioritises your remediation efforts based on the potential impact on your specific environment.

The Industrial Defender solution also comes with on-premise hardware, as well as various applications which can be on-premise and cloud-based. Additionally, professional services, configuration, training and ongoing support are provided as part of the service.

The Internet of Things (IoT)

This falls under all 3 lots in G-Cloud as it combines IoT sensors, a centralised core IoT application, installations, and integration or development work.

The core application is a lifecycle management application designed specifically for IoT and allows for any devices, and network, anywhere to be managed, secured and standardised. This open approach ensures longevity and removes any vendor lock-in seen in other platforms. In addition, Cirro offers:

- IoT Strategy & business case development

- Pre-installation site surveys - risk & method of install
- Device installations, cabling, electrical and connectivity support
- SDK bespoke application and API integration work

Virtual Desktop Infrastructure (VDI)

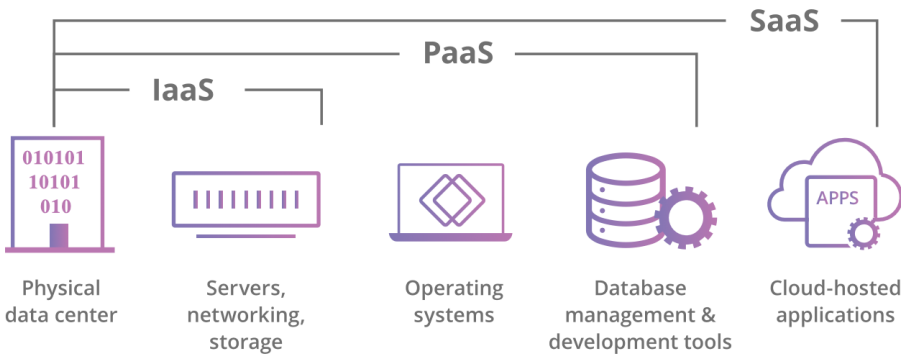
This service can either be a Microsoft Azure VDI or a non-Azure VDI, which can be run from any other location, such as on-prem, private cloud, private data centre, shared cloud or a hybrid set-up. This can include dedicated hardware but is delivered as an on-demand cloud service.

For Azure VDI, we charge a managed service fee based on the level of support required. This can also include professional services, dashboards and alerting, application streaming, security, business continuity and continual improvement.

Similarly, for non-Azure VDI, we will design, build and operate a suitable environment(s) to deliver the required outcome. We typically charge per desktop based on the resources of those desktops (CPU, RAM, HDD etc). We create Golden Images, user profiles and application sets. Every VDI can be firewalled off and effectively sandboxed to improve security.

Platform as a Service

This can be run from a hyperscaler, such as Azure, AWS, GCP or a private data centre or



a shared private cloud from the UK.

PaaS offers a full suite of operating systems, databases, developer tools, networking and security capabilities. These are either run as a managed service, typically where

workloads are more static. Or customers can manage their own deployments and environments, this is typically used for more elastic workloads and environments, or for DevOps where high levels of continual change are occurring.

Our service can offer support only, typically for Azure PaaS, or fully managed platforms and environments.

Infrastructure as a Service

Our on-demand computing resources include networking, storage, and other infrastructure components. Infrastructure as a Service (IaaS) allows users to develop, grow, and scale without the need to buy and maintain physical hardware. The power and flexibility of IaaS make it suitable for a wide variety of businesses, developers, researchers, and individuals who want complete control over their infrastructure the IaaS (Infrastructure as a Service) is a cloud computing service that allows users to have control over their infrastructure while not having to manage physical hardware.

Users can choose the level of control they have over their infrastructure and set it up according to their requirements. Developers can add layers of abstraction to their infrastructure, making it easier to maintain their applications. They can also add load balancers or managed services like Managed Kubernetes or Managed Databases to make it more efficient.

IaaS is broken into three main components: compute, network, and storage. With these offerings, users have the building blocks they need to create their customised systems, as complicated or powerful as they need, and the ability to scale up and down based on current needs.

Compute

Servers are powerful IaaS resources with hundreds of CPUs, storage, and thousands of GBs of RAM. IaaS providers can partition physical servers into VMs, which can run OS and apps independently. Kubernetes can containerise code into smaller namespaces, running only one application, with automatic traffic management. Users choose the operating system when purchasing a VM, which can be scaled vertically or horizontally. Virtual machines can be quick and easy to set up.

Storage

There are three types of storage options available: file storage, object storage, and block storage.

File storage works in a similar way to the storage on our home computers. It stores data as a single entity within a file. The files can exist within each other as other data, creating a hierarchical structure. For example, a path for file storage could be "/home/photos/selfie.jpg".

Object storage, on the other hand, takes saved data as a single entity and appends metadata and an identifier. Object storage deals with whole objects that are stored over the network. These objects could be things like images, files, logs, or HTML files. Object storage is the most popular option because of its simplicity and cost savings.

Block storage is likely to be found underneath the file or object storage. Block storage services provide access to a traditional block storage device over the network and attach it to your virtual machine. It takes data and saves it as blocks of actual bytes or bits. It has advantages over the other two types of storage by being faster to transfer data, but it is not user-friendly unless abstracted by a file system like the one on your computer.

Network

The network function talks to the storage function, other VMs, containers, other servers, the internet, the intranet, and other components. It's how information is transferred through the architecture regardless of endpoints. Users will need different networking bandwidths depending on the amount of data transmitted between computing resources.