SERVICE CATALOG

EDITION 2026.1

Service Catalog

CONTENTS

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

Spotlight

Agentic AI The Concierge AI agent	Automates knowledge work on your secure infrastructure, ensuring IP protection, departmental privacy, human-in-the-loop control, and know-how that accrues to your firm rather than a vendor. All agent execution is confined to an isolated runtime sandbox that blocks unauthorized network egress.
Desktop as a Service (DaaS) Virtual Desktop Add-on	A **"Digital Clean Room"** for secure Windows access from any device. This maintains your firm's sovereignty while offering a reliable failover solution should a physical device become unavailable. Beyond security, **DaaS** can function as an on-demand high-performance workstation; it allows users to access specialized, resource-heavy applications like **CAD** at lightning speed. See our Azure Virtual Desktop and Gartner on AVD brochures for technical details.
Virtual App Delivery (VAD) Virtual App Delivery Add-on	Secure **streaming of critical Windows applications** delivered natively through the browser on any hardware without the operational overhead of a full virtual desktop. Our **VAD** implementation integrates directly with your host operating system and cloud storage to ensure these applications feel local and respond intuitively to your existing workflow. Alternatively, strict Data Loss Prevention (DLP) policies can isolate corporate data by forcing all file saves to managed cloud environments.
Concierge Cloud Atelier The Concierge Cloud Atelier	A private Collaborative Suite for board papers, R&D and anything you would rather was not scanned to train someone else's AI. Google-level real-time collaboration, including Docs, Sheets, Kanban and Whiteboards, with every document encrypted in your browser before it reaches the server.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

Pricing and alignment

Unit-Based Model

Modern organizations no longer fit into a single “IT seat,” and your pricing should reflect that reality. Our **Unit-Based Model** lets you combine exactly what your workforce needs across personas, identities, and assets. Each unit is aligned to a specific **Operational Mandate**, ensuring you invest only in the value delivered rather than a one-size-fits-all rate. Units are ordered through this catalog, and their full lifecycle is managed within our payment portal.

Fiduciary Mandate

Our pricing is grounded in a strict **Fiduciary Mandate. We renounce the markups, margins, and hidden kickbacks that define traditional IT services**. Hardware, cloud services, and VoIP usage are delivered as pure MSRP pass-throughs. When an efficiency rebate exists, half is returned to you, and half donated to a charity of your choice.

1.20 Readiness Standard

Every unit includes our **1.20 Readiness Standard**, maintaining both a 20 percent hardware buffer and a virtual desktop for a 15-minute return to billability. We have eliminated **“project bleed”** by including the natural evolution of your estate in our flat fee. Read our terms to determine what constitute managed and project services. **Scaled Stewardship Credits** are automatically applied as your organization grows, aligning your investment with your operational maturity.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

Deployment terms and cost optimization

Ordering Logic

To scale existing mandates with tiered credits and avoid redundant setup fees, please utilize our **Payment Portal**. Use this catalog for new service enrollments and distinct structural orders only. To ensure full fiscal transparency, all hardware, cloud services, and VoIP usage are delivered as pure MSRP pass-throughs.

The Stewardship Model

Provision for a specific number of Personas that evolve with your organization, irrespective of the individuals assigned to them. For your permanent infrastructure, **Annual Mandates** provide one month of stewardship at no additional cost. Two-Year Mandates extend this advantage to 1.5 months. **Monthly Mandates** provide on-demand elasticity, serving as a flexible operational buffer for short-term contractors and transitional staff.

Architectural Governance

To enforce consistent security and governance without sacrificing flexibility, your architecture is anchored by a single Identity Provider (Microsoft or Google). From this baseline, you dictate your footprint: drive deep integration within a single-cloud Primary Foundation or provision Multi-Cloud Enclaves for specialized teams.

Where organizational scale and go-to-market strategy demand it, you may also embrace a company-wide Dual-Ecosystem to unlock best-of-breed capabilities, support highly specialized workflows, and effectively integrate with external clients' and partners' ecosystems.

Marginal Scaling

We apply **Scaled Stewardship Credits** to every progressive tier of your estate: 5% (units 10 to 25), 10% (units 26 to 100), and 15% (units 101 to 400). This ensures your average cost per unit decreases as your operational maturity increases, reflecting the architectural efficiencies gained as you scale.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

The Genesis Mandate	To give you complete visibility into your infrastructure before beginning a possible long-term residency, we invite you to undergo a comprehensive Discovery Audit. This initial project maps your digital estate to identify vulnerabilities, strategic opportunities, and pre-existing technical debt. While our ongoing mandates focus strictly on the buildup and proactive evolution of your environment, the audit provides a clear diagnostic of your starting point. You can explore this engagement in **Projects**.
Foundation Fees	These one-time, organization-level engineering fees cover the architectural hardening of your primary tenants and virtual environments. A separate **Foundation Fee** applies to each ecosystem you introduce (e.g., a Multi-Cloud enclave deployment may require both Microsoft and Google Foundation Fees).
Asset Setup Fees	These charges apply per-device to ensure provisioning, persona alignment, and architectural security. When subscribing to our persona mandates, **set the quantity to match your hardware count** at the time of order. Additional setups for subsequent adjustments or replacements are available in **Add-ons**.
Licensing	Wherever applicable, our persona mandates include a premium productivity suite, such as Microsoft 365 Business Premium or Google Workspace Business Plus. Where a persona does not need a full suite, that becomes a Frontline license or Teams. ChromeOS personas include Chrome Enterprise. For a plan-by-plan breakdown of what each Microsoft license actually contains, see M365 Maps.
Maintenance Absorption	Assets vetted by a Principal Steward qualify for our **"One-In, One-Out" policy**. This ensures that any standardized device replaced during a Persona mandate is hardened and integrated at **no additional cost** for the remainder of that term.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

ACH Stewardship Discount

Partners who remit via ACH bank transfer receive a 1.5% recurring discount applied automatically to their mandate. This reflects the elimination of card network interchange fees, a cost we pass directly back to you rather than absorbing into our pricing. To get the discount, pay from a verified bank account and apply the matching code: **ACH** for recurring mandates, **ACH-ONETIME** for single charges.

If you are currently paying by card and would like to switch, contact your Principal Steward or update your method through the Payment Portal.

Enrollment

Once you have deployed your order, please register and log in at conciergecio.com to manage your onboarding. **Your Principal Steward will guide you through your first deployments, onboardings, and offboardings.**

Group 01

PERSONAS

Core Stewardship Mandates, Cloud Personas

Full Concierge Single-Cloud

MICROSOFT 365

The Full Concierge Single-Cloud Mandate is our **Executive Standard:** a comprehensive stewardship residency that pairs the strategic depth of a dedicated CIO with senior-level engineering. We manage your firm's entire technical lifecycle, including long-term technology roadmapping, cybersecurity hardening, daily employee support, and cloud service management. By acting as your single point of accountability for all technology vendors, we eliminate the "productivity tax" of unmanaged IT and ensure uninterrupted billability. This establishes the architectural baseline for teams requiring durable performance, verifiable data integrity, and a permanent, high-trust partner to lead their digital strategy.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

Full Concierge Single-Cloud, continued	Azure Virtual Desktop and Virtual App Delivery available as add-ons, see Add-ons.
Full Concierge Enterprise, Cross Platform / Multi-Cloud Microsoft 365 + Google Workspace (or Zoho Workplace)	**The Multi-Cloud Standard**. Advanced governance for teams operating across fragmented cloud ecosystems and diverse hardware platforms. This mandate eliminates administrative islands, keeps systems aligned, and supports a frictionless experience while mitigating orphaned data and identity risks. When you need a secondary collaborative environment strictly to isolate management or sensitive R&D workflows, we also offer The Concierge Cloud Atelier. The Atelier completely air-gaps your data from Big Tech ecosystems and makes your intellectual property immune to AI training scans by encrypting it before it ever reaches a server.
Full Concierge Single-Cloud GOOGLE WORKSPACE	**The Hardened Baseline**. This mandate is designed for firms seeking to harden their perimeter and reduce capital hardware costs for task-oriented and cloud-native teams. It combines the near-impenetrable, "ransomware-proof" security of Google Enterprise devices with seamless, browser-based access to essential Windows applications via an optional **Virtual App Delivery (VAD)** layer. If your firm runs Google Workspace on Windows PCs without an existing Microsoft 365 mandate, a 365 Foundation is required for device management and endpoint threat protection. Apply code GooglePC at the time of order for 25% off. Windows Virtual App Delivery and Virtual Desktop available as add-ons, see Add-ons.
Concierge Cloud Workspace Microsoft 365 via Virtual Desktop	**The Digital Clean Room**. Secure virtual workspaces for contractors and BYOD users. A controlled, on-your-soil digital environment delivered through Windows 365, Azure Virtual Desktop, or your VDI infrastructure that enables external talent to work within your firm's ecosystem and security standards, on a full desktop they do not have to own.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

Concierge Cloud Workspace, continued

For a deeper look at the architecture behind virtual desktops and how isolation boundaries enforce compliance, see Why Virtualization?

Stewardship does not include physical hardware coverage or the 1.20 Readiness Standard for personal computer management.

Full Concierge Federated Enterprise

Multi-Cloud + Cross Platform + Virtual Desktop

This is the **apex of stewardship**, unifying multi-cloud governance with full-stack virtualized resilience. Built for high-compliance sectors like FinTech and Defense, it combines federated identity across all SaaS platforms with the isolation of a Digital Clean Room. This integrated mesh enables zero-day productivity on any platform or device while maintaining a Zero-Trust posture that meets SOC 2 standards.

Concierge Frontline

Microsoft 365

Frontline Mobility Governance. Many field-based roles operate entirely on mobile phones, tablets, and web apps. This mandate equips your mobile team for secure, efficient work without the licensing or management overhead of a primary desk workstation. It protects the communication silos where institutional intelligence resides and applies identity-driven governance to maintain firm-wide standards.

This mandate is restricted to mobile and web-only use. Stewardship does not include physical hardware coverage or the 1.20 Readiness Standard for personal computer management. Desktop as a Service and Virtual App Delivery available as add-ons on any monitor size, see Add-ons.

Concierge Cloud Workroom

Virtual Windows App Delivery

The Surgical Clean Room. Secure virtual application delivery for contractors and BYOD users. A tightly scoped, on-your-soil digital environment delivered natively through the Chrome browser that enables external talent to access critical Line-of-Business apps within your firm's high-governance ecosystem on any device, company-owned or not, without the complexity of a full virtual desktop.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

Concierge Cloud Workroom, continued

To understand how app streaming achieves Zero Trust isolation on unmanaged devices, see Why Virtualization?

Includes one primary application.

FURTHER READING

Check our Service Blueprints and our detailed Mandates feature list for more information.

Group 02

ADD-ONS

Persona Mandate Add-ons

Virtual Desktop Add-on (DaaS)

High-Governance Performance & Continuity

Each virtual desktop is a governed, isolated environment with controlled data egress, centralized logging, and a consistent security baseline across every session regardless of the device or location from which the user connects. For organizations with compliance obligations, it enables the auditability and access controls that a physical workstation estate alone cannot guarantee uniformly. For users with demanding workloads, the compute tier scales independently of local hardware, accommodating resource-intensive applications without capital expenditure at the desk.

Beyond the stewardship of a regular managed endpoint, this mandate covers the platform-side discipline specific to virtual desktops: image configuration and lifecycle, policy correctness, controlled patching, profile reliability at scale, and response to platform-wide issues that may affect many users at once.

For a deeper look at the architecture behind virtual desktops and how isolation boundaries enforce compliance, see Why Virtualization?

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

Virtual Desktop Add-on (DaaS), continued

A Virtual Desktop functions as a distinct, enterprise-grade endpoint within your environment. To maintain platform integrity, each instance requires the same security and management posture as a physical workstation. This fee is commensurate with the essential licensing and tooling required to secure and manage this secondary environment. This mandate is delivered using Azure Virtual Desktop (AVD), Windows 365, or a private VDI environment to meet your firm's governance, security, and data residency requirements. See Virtualization Costs in Context for a comparative breakdown of the underlying infrastructure economics.

Virtual App Delivery Add-on

Windows App Streaming on any Device

For environments requiring secure access to business-critical Windows applications on any device, Virtual App Delivery (VAD) streams a Digital Clean Room natively to the browser or a local client. This allows for high-performance streaming of individual apps while maintaining absolute data sovereignty and global access from any hardware without the operational overhead of a full virtual desktop. Our VAD implementation integrates directly with your host operating system and cloud storage to ensure these applications feel local and respond intuitively to your existing workflow.

To understand how app streaming achieves data sovereignty and Zero Trust isolation on unmanaged devices, see Why Virtualization?

Includes one primary application.

The Outlier Mandate

Standalone macOS Hardening & Governance

For Microsoft or Google environments with a limited macOS footprint (1 to 2 units), the Outlier Hardening Fee is a right-sized management path that avoids the cost of a Full Concierge Enterprise mandate. In Microsoft environments, we utilize Platform SSO to sync Mac logins with firm credentials and enforce Compliance Hardening that enables Remote Wipe and cloud-based FileVault escrow. For Google estates, we deploy a specialized bridge to achieve the secure SSO and remote administrative control that Google Workspace lacks natively. This one-time engineering investment is a lifecycle commitment to your "Digital Persona"; any hardware replacements for that seat are hardened and enrolled under your existing stewardship at no additional cost.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

Unit Provisioning & Hardening

Technical Preparation for High-Governance Asset Enrollment

Hardening is required for all personal computing hardware, including primary workstations, 1.20 standard buffer units, secondary computers, and silent infrastructure like lobby or conference room terminals. This mandate establishes **Shields Up stewardship** through a protocol of hardware verification, security enrollment, and application configuration. This thorough preparation ensures that every asset is delivered fully patched, tested, and documented for a frictionless handoff the moment it is activated. This mandate also applies to hardware acquisitions that fall outside the initial order of a Full Concierge mandate or our **One-In, One-Out** maintenance absorption policy for the replacement of vetted assets. Common examples include a transition from a virtual environment to physical hardware or the replacement of a legacy device that was never vetted by a Principal Steward.

Group 03

FOUNDATIONS

One-time Per-org Tenant Hardening Fees

Microsoft 365 Foundation

Required for all Personas except Google Single-Cloud

Microsoft 365 Tenant Architecture and Security Hardening establishes the governance and security foundation required before a single persona can be managed with integrity. This one-time engineering engagement hardens the Entra ID identity layer, designs the Conditional Access architecture, deploys the Intune device compliance framework, activates your threat detection posture, and locks down your collaboration perimeter across Exchange, Teams, and SharePoint. The baseline that remains is documented, audit-ready, and aligned to the CIS Microsoft 365 Foundations Benchmark.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

macOS Foundation

Required for macOS Fleets

Apple Fleet MDM Architecture and Identity Integration establishes a native standard of governance that works directly with the platform. This one-time engineering engagement builds the device management and identity foundation for your Mac fleet. We bind your organization to Apple Business Manager, design your MDM policy framework for zero-touch enrollment, and integrate Platform SSO with your primary identity provider. Encryption, privacy, and application control policies are enforced to enterprise security standards. The fleet then provisions itself, stays aligned, and behaves like a first-class citizen on your network.

Google Workspace Foundation

Required for Single-Cloud Google and Enterprise Mandates

Google Workspace Tenant Architecture and Security Hardening closes the gap between convenience-focused factory defaults and a properly governed enterprise environment. This one-time engineering engagement secures your email domains against spoofing and structures your administrative console so that security policies and access levels apply accurately to specific user roles. It enforces context-aware authentication that binds every session to explicit identity and device posture. We lock down data boundaries across email and cloud storage, regulate third-party application permissions, and establish court-ready retention protocols in Google Vault. The finished tenant is documented and aligned to the CIS Google Workspace Benchmark.

ChromeOS Foundation

Required for Enterprise ChromeOS Fleets

The Zero-Surface Baseline. The build starts with the Admin Console architecture for your ChromeOS fleet. It is structured around a deliberate Organizational Unit hierarchy, so policies apply precisely to the right devices and users. Your Chrome Enterprise baseline is deployed and hardened. Chrome Enterprise Premium security controls are activated, covering data loss prevention, context-aware access, and real-time threat intelligence. Device authentication is federated with your primary identity provider, ensuring every Chrome session is governed by your firm's identity and access policy. Where Windows application delivery through the browser is required, the integration groundwork is laid as part of this engagement. The result is a fleet that requires almost no endpoint intervention while maintaining an uncompromising security posture.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

Microsoft Virtual Desktop Foundation

Required for Enterprise Mandates, Workspace, and DaaS Add-on · AVD or Windows 365

The architecture underneath a **Digital Clean Room** decides what it can promise. We design and deploy your Azure Virtual Desktop environment from the ground up. It establishes your Azure resource architecture and configures optimized host pools. The process also builds a documented golden image maintenance pipeline and deploys FSLogix profile containers for persistent, portable user identities. It thoroughly engineers your network topology for strict performance and security. Conditional Access policies are systematically wired through every session. Finally, autoscaling, monitoring, alerting, and full disaster recovery procedures are validated before handoff. The ongoing stewardship of this environment, covering golden image lifecycle, policy correctness, patching, profile reliability, and platform-wide incident response, is functionally distinct from end-user support and is covered by the monthly Virtual Desktop add-on cost.

This mandate is delivered using either Azure Virtual Desktop (AVD) or Windows 365. See Virtualization Costs in Context for a comparative breakdown of the underlying infrastructure economics.

Self-hosted Virtual Desktop (VDI) Foundation

Required for Enterprise Mandates and DaaS Add-on · Proxmox or Nutanix

This mandate establishes the orchestration layer that runs a platform of dedicated Windows 11 virtual machines on an existing hyperconverged cluster and sustains its performance at scale. It covers the connection broker, through which each user authenticates via Entra ID (SSO and MFA) and is routed to their own machine. On-demand power management starts and stops each virtual machine as users connect and disconnect. At its core is the building of a full golden image from which individual desktops are provisioned. Around this sits the ongoing stewardship that keeps the estate healthy: golden image lifecycle, platform policy correctness, controlled patching, profile reliability at scale, and response to platform-wide issues that may affect many users at once. This ongoing stewardship is functionally distinct from end-user support and is covered by the monthly Virtual Desktop add-on cost.

This mandate is delivered using either Proxmox or Nutanix. See Virtualization Costs in Context for a comparative breakdown of the underlying infrastructure economics.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

Virtual App Delivery Foundation

Required for Workroom and VAD Add-on · App Session-level Orchestration

We deploy a session-level delivery layer that streams critical legacy or server-resident systems directly through any web browser, so the hardware in front of the user stops mattering. By containerizing individual applications, this architecture guarantees complete session isolation and local user experience parity while preventing corporate files from ever being stored on unmanaged local drives. Your people work in a flexible, highly compliant environment that preserves firm-wide data sovereignty and authenticates every interaction against your primary governance baseline.

Zoho Workplace Foundation

Required for Enterprise Mandates with Zoho

Zoho Workplace Tenant Setup and Security Hardening supplies the governance a freshly provisioned nine-app suite does not ship with. We configure your email domains against spoofing in Zoho Mail's Admin Console and structure Zoho Directory so that security policies and access levels reflect actual organizational roles. Conditional access then evaluates every login against identity, device, location, and time-of-day signals. WorkDrive data boundaries are locked down with automated DLP classification. Third-party OAuth permissions are governed from the Zoho One admin panel, and court-ready retention policies and legal holds are stood up in the built-in eDiscovery portal. Every layer of the Workplace stack ends up hardened, and documented.

Group 04

ASSETS

Infrastructure Asset Mandates, Managed Assets

The Managed Asset

Add-on device stewardship beyond your 20% buffer

"Shields Up" Stewardship for the "silent infrastructure" that anchors your office: hot spares, secondary workstations, lobby terminals, conference room hardware, and home office. This mandate ensures every unmanned device remains patched, hardened, monitored, documented, and ready for work the moment it is activated.

Managed assets carry the identical remote telemetry, patching, and MDR/SOC licensing burden as a primary endpoint. Because secondary and shared devices often introduce unique vulnerabilities, they demand equal, continuous oversight and hardening.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

The Managed Server

Server stewardship for on-site or cloud-hosted systems

Comprehensive oversight for your firm's server infrastructure. This mandate covers the setup, cyber-protection, and administration of physical or virtual Windows and Linux systems, on-site or in the cloud. Stewardship applies to systems such as Line of Business applications, databases, and backup infrastructure. Expert management of the technical layer ensures data remains accessible and under your total control.

Software licensing and third-party hosting fees not included. They are delivered as pure MSRP pass-throughs.

Cloud Workload Protection

Optional Add-on to The Managed Server mandate

Active compliance and hardening for Linux and Windows server workloads exposed to the public internet. This mandate installs and tunes the specialized tools and OSSEC rules required to satisfy stringent data security and privacy standards. Stewardship ensures infrastructure remains audit-ready through continuous monitoring and defensive hardening. Supported frameworks include NIST 800-171, JSIG, PCI DSS, GLBA, GDPR, HIPAA, and others.

This protection is available for new servers and as a standalone service for self-managed or Legacy Sustainment assets. This add-on mandate covers the management and tuning of your security architecture. Because application and compliance requirements demand a highly tailored solution, the underlying software licenses and infrastructure for the protection itself are procured separately.

The Managed Network

Stewardship for sites beyond your primary office

Office Connectivity Stewardship. Comprehensive oversight for your office connectivity infrastructure. This mandate covers the setup and administration of the stateful gateway, firewalls, and switching fabric. Stewardship applies to services such as Multi-WAN routing, VLAN segmentation, VPN access, and IDS/IPS for one physical /24 subnet. Expert management of the gateway ensures the network remains secure, optimized, and under your total sovereignty.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

The Managed Network, continued

The Foundation fee is waived for preexisting, remotely manageable networks running Ubiquiti UniFi or Netgate infrastructure, provided the hardware has not reached End-of-Life (EOL) and administrative control is fully transferable.

The Sovereign Network Enclave

Zero-Trust Access and Sovereign Network Fabric · Zero Trust

Today's workforce and applications operate beyond physical perimeters. Zero Trust Network Access eliminates implicit trust entirely: every connection requires continuous, identity-first verification. We enforce this mandate across two planes:

The North-South Perimeter (People-to-Systems): We project your applications securely onto the internet through a centralized, high-speed identity gateway that replaces vulnerable traditional access methods. This sovereign perimeter enforces identity-first validation for personnel, it retrofits modern Single Sign-On (SSO) and MFA protection onto legacy or non-compliant applications, and it grants clientless, scoped access for third-party vendors.

The East-West Overlay Mesh (System-to-System): Across your servers, cloud environments, databases, and endpoints, we weave an encrypted virtual backplane. Traffic routing and micro-segmentation run on infrastructure you own and control, keeping the data plane sovereign. This software-defined mesh darkens communication paths between disparate locations, eliminating the risk of lateral threat movement.

The Hyperconverged Cluster (HCI)

Scalable Private Cloud for your Core Applications and Remote Workspaces (VDI) · Datacenter

We architect and oversee a resilient, software-defined platform for workloads where the public cloud is not cost-effective, not suitable, or not yet viable. This mandate builds robust **on-premises data center infrastructure** on a redundant three-server cluster that unifies compute, storage, and networking into a single scalable high-availability system.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

The Hyperconverged Cluster (HCI), continued

This platform is purpose-built to host stateful line-of-business applications and persistent virtual desktops with predictable performance. This sovereign architecture replaces volatile, consumption-based cloud billing with a durable, fixed-cost asset. It reduces long-term spend and gives you a resilient foundation for projecting these workloads across the local network and the global edge.

For robust disaster recovery, we strongly advise provisioning a fourth, storage-optimized server to act as a dedicated local backup repository. Because backup workloads require disk capacity rather than high compute power, this node can be provisioned with reduced specifications, providing an isolated, cost-effective vault for your virtual desktops, servers, and container snapshots.

This mandate is delivered using either Proxmox or Nutanix. See Virtualization Costs in Context for a comparative breakdown of the underlying infrastructure economics. For VDI environments, a Virtual Desktop Foundation is required to establish the orchestration layer that runs dedicated Windows virtual machines and sustains their performance at scale. Management of the backup node incurs no additional labor fees; it is covered under this Cluster Stewardship mandate.

The Concierge Cloud Vault

Provisioned within any of our Full Concierge mandates · Credential Governance

Collaborative enterprise vault. Self-hosted and single-tenant, this multi-user system handles shared credential management for your entire team. It extends beyond standard web passwords to act as an encrypted repository for API keys, database connection strings, software license keys, PINs, and secure notes. The zero-knowledge OpenPGP architecture ensures passwords remain private even from your Steward, while allowing for instant user revocation. GDPR compliant, tracker-free, and accessible via any device or browser.

Organizations with advanced regulatory needs should consider the Compliance Edition, which adds a hardened Business-core layer and full activity logging to satisfy SOC 2 and industry-specific audits.

This standard edition of the Concierge Cloud Vault is provisioned and managed within our Full Concierge mandates.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

Group 05

LEGACY

Legacy Asset Mandates, Business Continuity

Active Directory Domain Controller(s) and Member(s)

Stewardship of your legacy AD/DS or hybrid AD Domain Controller(s). On-premises or cloud-hosted. Administration and cyber-protection **while we move your environment to M365** or as a permanent solution when M365 is not suitable. FOSS option available.

Per Microsoft Specification, 3 Domain Controllers are required for high availability. Foundation fee waived for preexisting server. Microsoft Licenses not included.

Legacy File Server

Stewardship of your legacy workgroup on-premises File Server. Administration and cyber-protection **while we move your files to SharePoint or Google Drive** or as a permanent solution when cloud storage is not suitable. Microsoft Licenses not included. FOSS option available.

Per Microsoft Specification, 2-node Failover cluster is required for high availability. Setup fee waived for preexisting server. Microsoft Licenses not included.

Group 06

PROJECTS

Strategic Project Mandates, Prepaid Blocks

The Genesis Mandate

Discovery Audit & Sovereignty Initialization

For prospective clients seeking complete visibility into their digital estate, we offer a comprehensive diagnostic engagement at a discounted package rate. This includes a thorough infrastructure inventory and our **Sovereignty Snapshot** security assessment, as well as the identification of strategic opportunities and pre-existing technical debt.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

The Genesis Mandate, continued

Following the audit, we provide a detailed report and a **Hardening Roadmap** estimating the hours required for our Principal and Technical Fellows to resolve any technical debt. When you transition to an ongoing stewardship mandate, we will proactively manage and evolve your environment based on the scope of that mandate. However, resolving pre-existing technical debt remains a **separate mission, billed outside the mandate** at our standard principal consulting rate.

If significant technical debt is discovered, whether during an initial audit or an active mandate, we reserve the right to limit or suspend certain performance and security guarantees until a foundational **Baseline of Sovereignty** is properly established.

To maximize your investment, clients who initiate an ongoing Stewardship Mandate concurrently with their audit immediately unlock our 15% Preferred Partner Discount (Code: INNET). This preferred rate applies directly to the Discovery Audit itself, as well as any subsequent engineering labor required to resolve legacy technical debt. By running both engagements in parallel, we secure your daily operations immediately while systematically hardening your underlying architecture.

Cloud Migrations

Provisioned within Full Concierge Mandates

Moving your firm's digital foundation, whether shifting to the cloud, transitioning between platforms, or repatriating data to your private HCI cluster, is a high-stakes engineering event that requires patience and precision. We manage the entire technical lifecycle, from mapping complex identity permissions and executing DNS cutovers to navigating vendor throttling and platform constraints, all while ensuring bit-perfect data integrity. While we handle the underlying complexity, our focus remains on your Business Continuity. We keep the firm working through the cutover, and the hours normally lost stay billable. Whether you are seeking better cost predictability or a hardened security posture, we ensure your migration is a strategic upgrade you can measure on your bottom line.

Initial user migrations are included in our Cloud Productivity Suite mandates with two-year commitments. For the virtualization of legacy servers or specialized applications, please call to discuss your specific architecture.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

IT Consulting: Principal Steward

Offered in discrete hourly blocks, this engagement is fractional CIO leadership for specialized projects, technical due diligence, or complex troubleshooting. The Principal Steward functions as both a fiduciary advisor and a lead engineer, translating high-level business goals into a technical reality. This is a standalone service for high-stakes objectives requiring deep technical skill and architectural oversight. We ensure your technology is secure and performant on a per-project basis, with no long-term stewardship mandate required.

Strategic Mandates of 40 hours or more qualify for a 10% Governance Credit, providing a pre-paid value bonus and priority scheduling for large-scale advisory and engineering projects. Use Code INNET for 15% off project labor, reflecting the management overhead already satisfied by your Full Concierge monthly mandate.

IT Consulting: Technical Fellow

Senior Engineer

Offered in discrete hourly blocks. The Technical Fellow brings specialized engineering depth to advanced infrastructure builds, including server hardening, complex networking, and virtualization. This role executes high-level technical specifications to transform strategy into a functional reality. The Technical Fellow is the master craftsman of our Guild.

Strategic Mandates of 40 hours or more qualify for a 10% Governance Credit. Use Code INNET for 15% off, reflecting that we already own the documentation and access through your monthly mandate.

IT Consulting: Remediation / B-F

Offered in discrete hourly blocks on a best-effort basis. This category covers reactive interventions and the hands-on repair of systems suffering from neglect or a disregard for established security standards. Remediation involves high-intensity labor to stabilize a crisis or restore business continuity after a preventable failure. Because this work is unscheduled and results from infrastructure decay, it carries a premium rate and lacks the priority status or service guarantees provided under our proactive mandates.

Remediation services are strictly excluded from all discounts and volume credits.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

The Sovereignty Snapshot

Security Assessment

Before committing to a long-term mandate, many partners begin with this high-impact diagnostic of their current risk posture. We utilize a non-invasive, read-only handshake to perform a no-credential-storage scan of your Microsoft 365 environment. We identify immediate gaps in MFA coverage, privileged account risks, and Entra ID configuration issues. This deep-dive includes a Shadow IT Discovery and a Domain Spoofing check to ensure your brand isn't being weaponized by external actors. We then supplement this cloud data with a "Principal's Walk-Through" of your physical infrastructure to identify the legacy hardware "ghosts" and connectivity bottlenecks that a remote scan cannot see. The result is a clear Sovereignty Scorecard: a strategic roadmap that separates your stable assets from those requiring urgent remediation.

If you transition to a Persona Mandate within 30 days of your Snapshot, the fee is credited in full toward your first month of service.

Compliance Governance (WISP & HIPAA)

Regulatory compliance is not a "set and forget" project; it is the practice of maintaining a defensible position. We specialize in the development and governance of mandated Written Information Security Plans (WISP) and specialized HIPAA/Regulatory procedural documentation. Rather than providing generic templates, we translate abstract federal requirements into a practical "Operating Manual" for your firm. This engagement satisfies the documentary standards required for Cyber Insurance renewals, HIPAA Security Rule audits, and FTC Safeguards compliance. By aligning your technical controls with formal policy, we ensure that your "Baseline of Sovereignty" is not just implemented, but legally documented and audit-ready.

Strategic Mandates of 40 hours or more qualify for a 10% Governance Credit. Use Code INNET for 15% off, reflecting that we already own the documentation and access through your monthly mandate.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

Structured Cabling Systems

Design and installation of IEEE 802.3 structured cabling systems in Cat6 and high-performance Cat6A standards. This service includes professional termination, comprehensive performance testing, and updated as-built network drawings to ensure a fully documented physical layer. Baseline rates apply to standard commercial environments with accessible drop-ceilings. Adjustments are required for hard-lid ceilings, cable runs exceeding 100 feet, plenum-rated requirements, after-hours labor, and the architectural complexities of historical or industrial facilities.

Use Code INNET for 15% off project labor, reflecting the management overhead already satisfied by your monthly mandate.

Group 07

SOFTWARE

The Stewardship Toolkit

TimeSqueeze

Universal Activity Tracking Endpoint

TimeSqueeze is the "Activity Intelligence Layer" Windows never had. It runs at system level and captures a second-by-second record of digital work. It automatically organizes apps, files, websites, and sessions into a defensible timeline, so nobody reconstructs a week from memory at month end. That matters more as AI compresses the visible effort behind a deliverable. Built for professional service firms, TimeSqueeze powers our internal Settlement Ledger. Peer-to-peer support inside the mesh is logged and settled without anyone filing paperwork. Whether used for precise billing, workflow forensics, or operational analytics, TimeSqueeze keeps a complete, local-first history of work that integrates with your existing enterprise systems.

This mandate includes the software license, deployment, API integration, and continuous system and user stewardship. For self-managed environments, standalone licenses are available via the Microsoft Store or directly through timesqueeze.net.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

GWSL Graphical Linux Bridge

Automated X-Server & Linux Integration

GWSL is an automation layer designed to run graphical Linux applications directly on Windows 10 and 11. Engineered to support local WSL (1 and 2) environments and remote Linux servers or workstations via SSH, it replaces per-application X-server setup with a single launch action. GWSL puts Linux applications in the Windows Start menu and on the taskbar where they open in ordinary windows and behave like any other program. Developers run Linux IDEs and specialized toolsets at native stability. GWSL has become the standard graphical layer between Windows endpoints and Linux infrastructure.

This mandate includes the software license, deployment, and continuous system and user stewardship. For self-managed environments, standalone licenses are available via the Microsoft Store.

OpenInWSL Integration Utility

Native Linux File-Handler for Windows

OpenInWSL registers Linux applications as Windows file handlers. Open a file or folder in Windows File Explorer and it arrives directly in a Linux IDE or utility. No path translation, no shell session in between. It operates alongside GWSL, which supplies the graphical layer, and it removes the context switch that otherwise accompanies every file crossing between the two environments.

This mandate includes the software license, deployment, and continuous system and user stewardship. For self-managed environments, standalone licenses are available via the Microsoft Store.

DISCLOSURE

In keeping with our Code of Ethics, we disclose that TimeSqueeze, GWSL and OpenInWSL are sold by a sister company under common ownership with Concierge CIO Partners LLC.

WHERE OUR TOOLS ARE INSTALLED

Sampling of the organizations where our tools are in daily use, based on download records. Not Concierge CIO Partners clients.

Google NASA AIRBUS Bloomberg NVIDIA SPACEX
MICHELIN ERICSSON CLOUDFLARE LG Electronics THALES DASSAULT SYSTEMES
SOCIETE GENERALE BROADCOM ARM ATLASSIAN amazon web services UBISOFT

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

Group 08

AUXILIARY

Auxiliary mandates and stewardship extensions

The Concierge AI agent

Server and User-Side Agentic AI Stewardship

Sovereign Agentic Infrastructure. We build a dual-node AI architecture that automates challenging or repetitive intellectual work without exposing your data. A high-compute local node runs advanced open-weight reasoning models on private silicon while a cloud coordination server handles connections to your external tools and services. You direct the agent in plain language through a messaging app; it executes multi-step digital workflows in the background and reports back only when a job is done or a decision is needed. All execution is strictly confined within an isolated runtime sandbox powered by NVIDIA to block unauthorized network egress and eliminate data exfiltration risks. Routine operations run free on your local hardware while novel or complex problems autonomously escalate to a frontier model like Anthropic's Opus. Once the problem is solved, the agent saves the procedure as a reusable, plain-text "skill." Your firm stops renting temporary intelligence, slashes overhead, and builds compounding proprietary equity that works 24/7.

User-Side Stewardship. We govern the human and operational boundaries of your automated workforce to keep it controlled and secure. Strict profile isolation lets multiple executives or departments use the system simultaneously without cross-contaminating their workflows or memories. We maintain a centralized, human-readable "Shared Playbook," a secure repository where the agent's generated procedures are reviewed and curated before they become standard practice. And we enforce strict approval protocols: the agent must request explicit human sign-off, via chat or mobile push, before executing any high-risk action. We operationalize the intelligence, ensuring it remains a strictly governed, highly efficient extension of your organization.

Agentic AI remains experimental. While the sandbox secures the host, opening API tunnels to external tools introduces risk. An AI hallucination could execute unintended commands on connected systems, making human-in-the-loop oversight critical.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

The Concierge Cloud Atelier

AI-Shielded Zero-Trust Zero-Knowledge Productivity Suite

Sovereign Collaborative Suite. A dedicated, single-tenant Cryptpad server instance for your most sensitive R&D and management workflows. The atelier hosts Google-level real-time collaboration, including Docs, Sheets, Kanban, and Whiteboards using browser-side OpenPGP encryption to secure data before it ever reaches the server. As your Steward, we manage the infrastructure while your data remains mathematically invisible to us and immune to big-tech AI training scans. This GDPR-compliant "secure enclave" gives you managed Shared Drives and external sharing without the privacy risks or vendor lock-in of the public cloud.

A secure enclave is only as strong as its access protocols. Our user-side stewardship enforces that boundary. We integrate your team into zero-knowledge workflows, architect precise permissions, and anchor your intellectual property within organizationally controlled Team Drives. Should team composition change, we execute immediate server-side access revocation. The departing user is cryptographically locked out of the workspace while your firm's data remains accessible and the zero-knowledge perimeter unbroken.

The Concierge Cloud Vault: Compliance Edition

Add-on to our Full Concierge mandates

Audit-Grade Credential Stewardship. For firms requiring SOC 2 or high-compliance governance, our Compliance Edition adds granular activity logging and enforced security policies. Unlike standard password managers, this mandate builds the "Chain of Custody" auditors require, including automated user provisioning, hardened MFA enforcement, and a managed physical escrow for organizational recovery. As your Steward, we maintain the audit trail and the infrastructure, ensuring your credentials are not just secure, but compliant. We deploy each vault as a private, single-tenant residency, architecturally isolating your credentials from the systemic vulnerabilities inherent in commercial mass-market password managers.

The standard edition of the Concierge Cloud Vault is provisioned and managed within our Full Concierge mandates.

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com

Index

A TO Z

All 42 mandates in alphabetical order, with the group each belongs to

1301 S Bowen Rd, Ste 435, Arlington, TX 76013
+1-408-479-3136
www.conciergecio.com