General Pharmaceutical Council

Statement of Requirements- Technical

1.1 Background

The GPhC regulate pharmacists, pharmacy technicians and pharmacies in Great Britain. We work to assure and improve standards of care for people using pharmacy services. Our role is to protect the public and give them assurance that they will receive safe and effective care when using pharmacy services. We set standards for pharmacy professionals and pharmacies to enter and remain on our register.

The GPhC seek assurance that pharmacy professionals and pharmacies continue to meet our standards, including by inspecting pharmacies. We act to protect the public and to uphold public confidence in pharmacy if there are concerns about a pharmacy professional or pharmacy on our register.

Through our work we help to promote professionalism, support continuous improvement and assure the quality and safety of pharmacy GPhC is seeking qualified respondents to ideally provide a hybrid Azure managed service in support of its business operations and create sustainable relationships that meet the following strategic sourcing objectives:

- Performance Optimisation – Enable improvements to service delivery and customer experience both for internal and external customers, allowing better management of cost, risk and results.
- Agility / Speed – Implement an agile, responsive and scalable partnership with the organisation addressing their rapidly changing needs, lowering complexity and improving global delivery capabilities.
- Improved Relationship Management – Achieve clear and proactive account management with the flexibility of services to support future business requirements.
- Cost Control & Reduction – Effectively manage services to provide transparency with clear cost control with flexibility in consumption of services to allow funding of future IT requirements.
- Innovation – Partner with an MSP that will bring technology leadership in IT services and assist GPhC with becoming “faster followers;” enabling the adoption of better practices and solutions to improve business outcomes.
- Risk & Accountability – Proactively identify issues and themes that may have an impact on GPhC’s business operations and service.
- Plan of approach detailing the solution, delivery and effort to cover the services requirements to include but not limited to – in no particular order:

    1. Infrastructure & Hosting
    2. Desktop Management

3. Mobile device Management
4. Infrastructure Monitoring
5. Security
6. Disaster Recovery
7. Service Transition.
8. Service Management as per ITIL processes
9. Service Levels & Service Credits
10. Governance
11. Technical Account Management
12. Release & Configuration Management
13. Resource Skillsets & Coverage
14. Project support and resourcing

1.2 Current challenges

- Challenge in flexibility in project resourcing
- Lack of stand-in in key technical areas
- Innovation capabilities
- Service management
- Sub-contractor management

1.3 High level architecture

1.3.1 Overall architecture diagram

GPhC's overall enterprise architecture is as shown below. We are continually upgrading and improving our environment to provide best service to our customers. All systems are updated as and when necessary and we don't have any tech-debt.

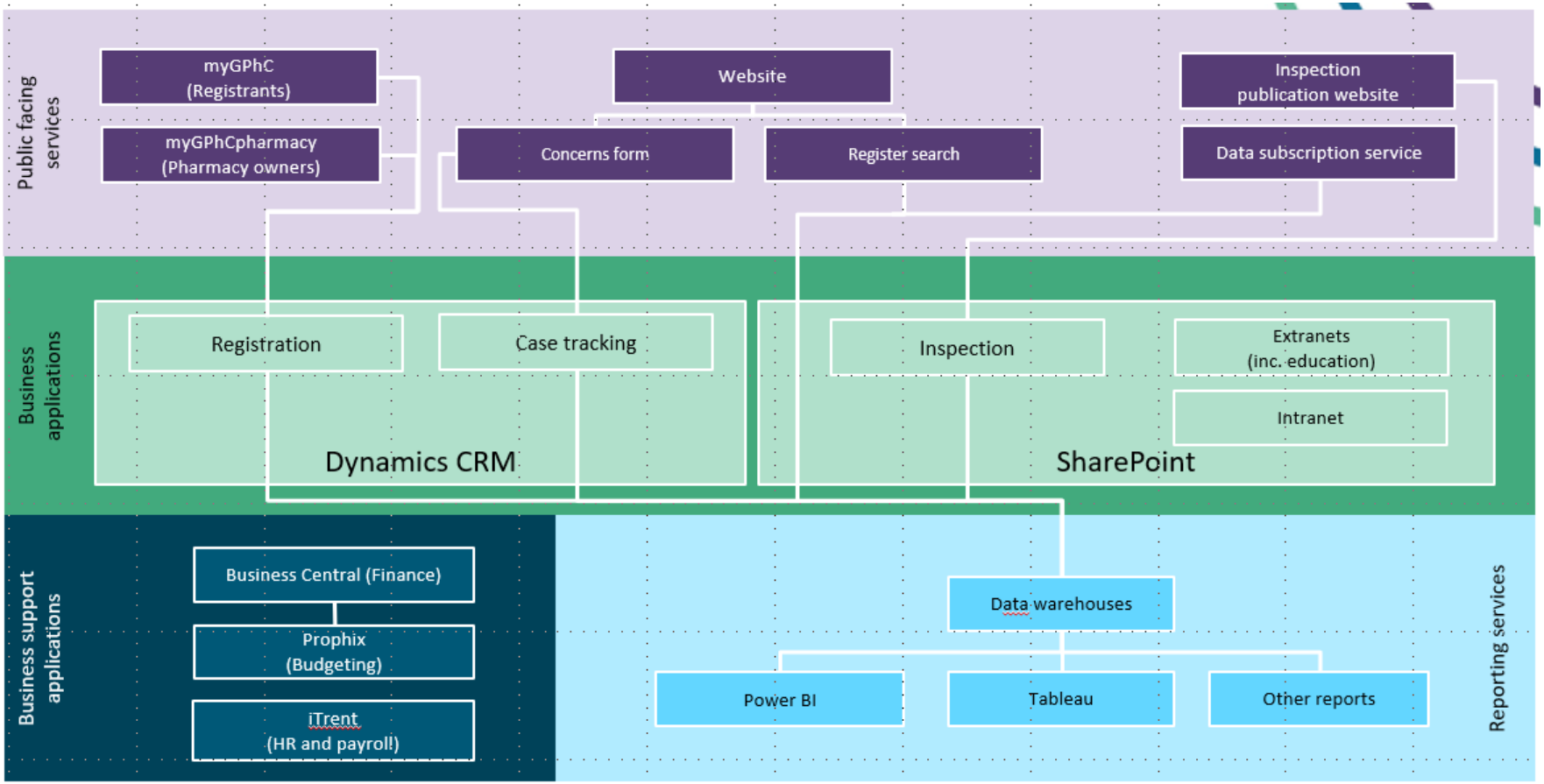


Figure 1 system Overview

As part of continuous improvements, GPhC is planning to upgrade some of its key systems to improve the service we are providing, and we expect that the incoming managed service providers will support us in upgrading the infrastructures for some of the

roadmap projects. Overall roadmap is as shown below (Please note that some of the projects are likely to be completed by the time the new provider is in place next year.

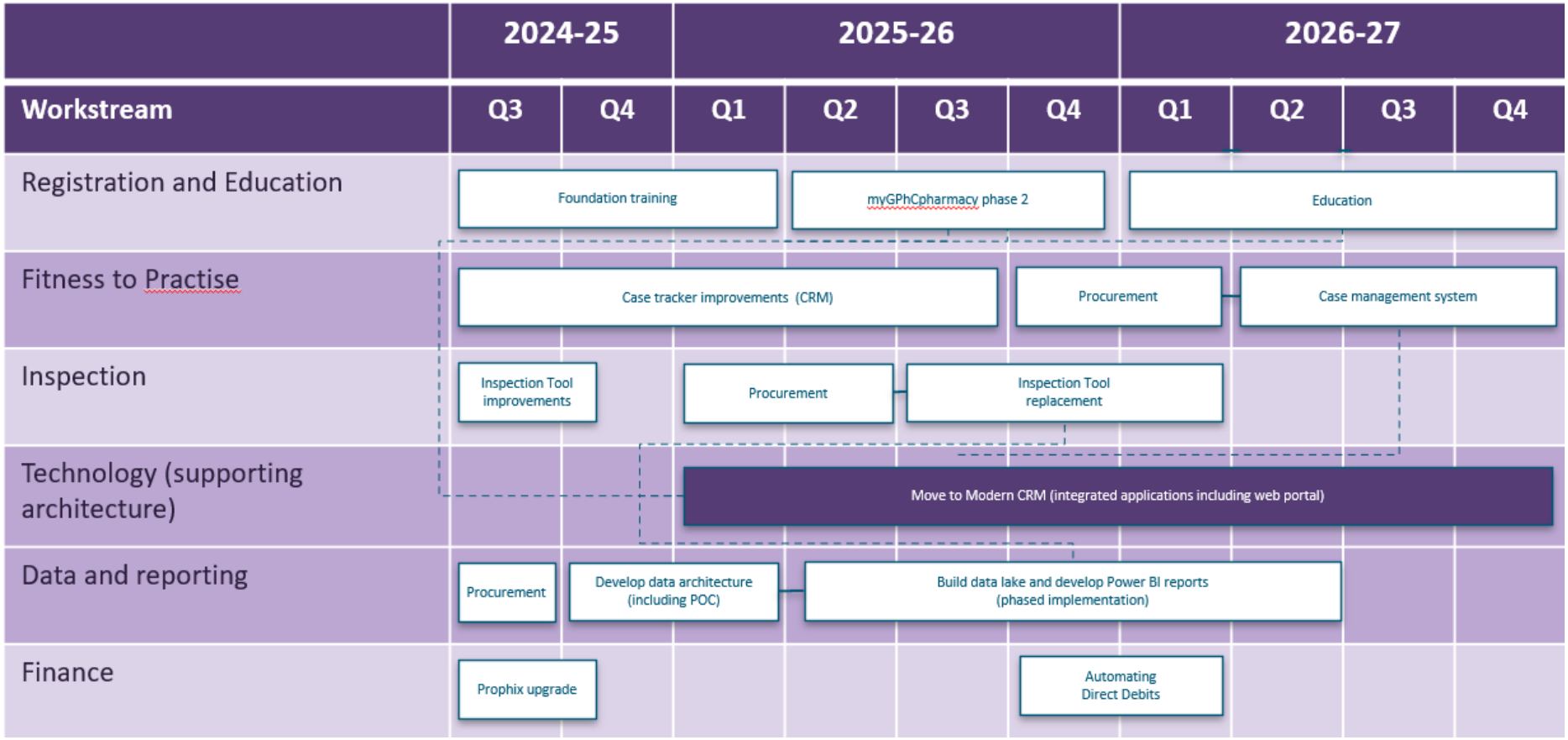
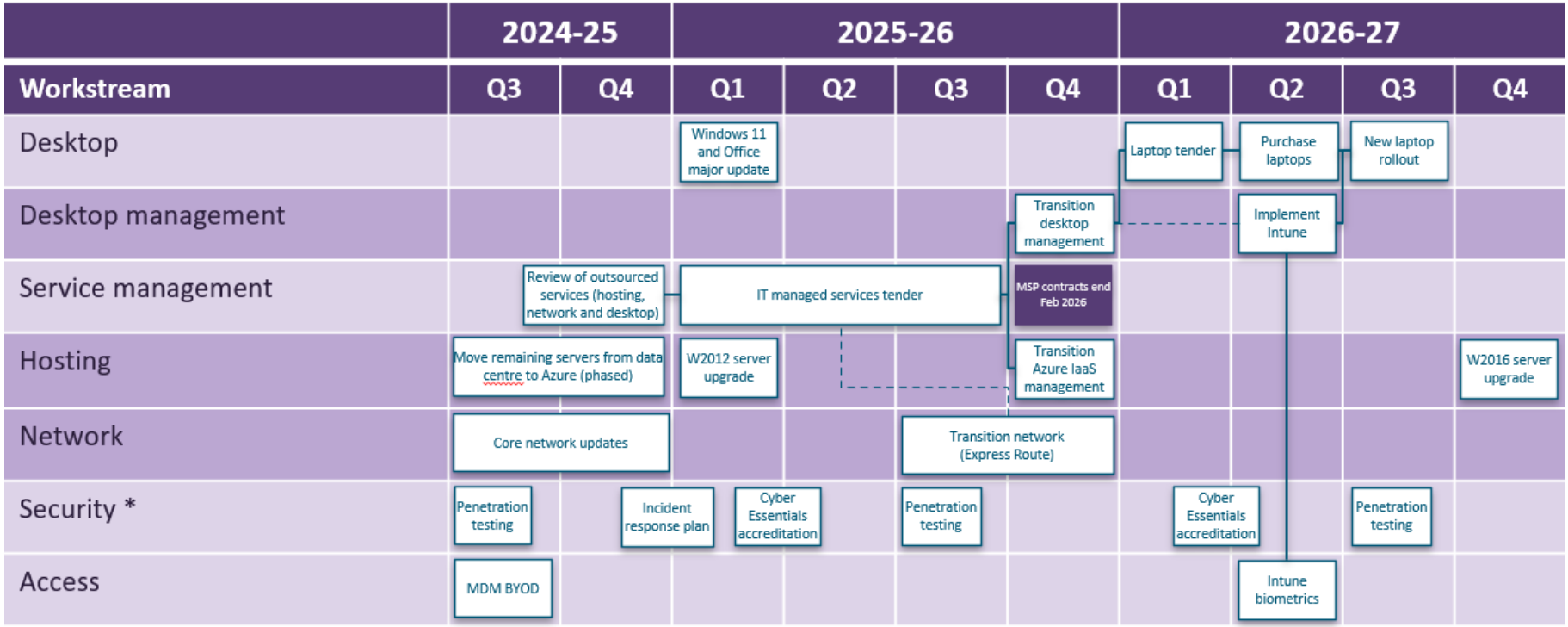


Figure 2 Draft High level Technology roadmap Business systems, public facing services & data and reporting

Technology Roadmap for IT services shown below



* Security workstream also includes horizon scanning, regular checkpoint reviews and development covering vulnerability scanning, ransomware containment, network security, email security and anti virus

Figure 3 Technology roadmap: IT Services

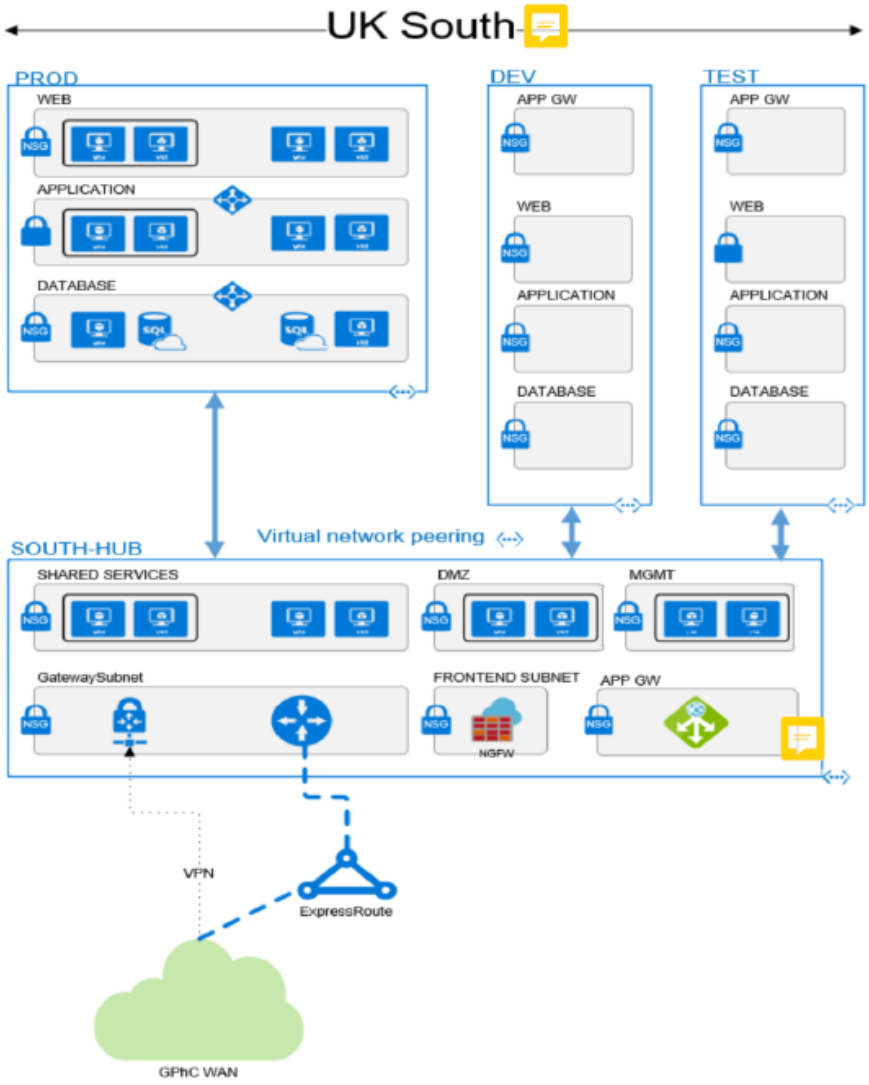


Figure 4 High level Azure Architecture

1.4 Network Architecture

1.4.1 Overview

The network architecture for GPhC comprises the 1 Cabot Square LAN and GPhC's Azure.

In order to achieve high availability, resilient network services are provisioned encompassing WAN circuits, Firewalls, Switches and WLCs. Thus, enabling GPhC to recover quickly and continue operating even when there has been an equipment failure, power outage or other disruptions.

The Supplier will need to provide the internet connections, manage network, provide WIFI access at GPhC's office through their network provider. Current supplier's Network provider is Colt.

1.4.2 LAN

Presently the LAN infrastructure at GPhC office “1 Cabot Square” is based on a two-tier network model, Core and Edge. This includes the services layer, leveraged to host perimeter security, Internet access, Wireless LAN Controller, SAN and WAN Optimisation.

1.4.3 Wireless Access (Wi-Fi)

Presently GPhC uses a wireless LAN controller with a total of twenty-one wireless access points. The controller is trunked off the Distribution switch in the current provider’s Data centre. This is a single controller and a single point of failure. There are four profiles configured on the WLC.

1.4.4 WAN

The 1 Cabot Square Office is provisioned with 2 x 1Gb LES circuit.

1.5 Application overview

1.5.1 Services and platforms are supported and managed within the Azure environment and couple of on-site servers to be moved to new provider’s data centre

Applications are supported by GPhC application team, and the new providers will manage the supporting infrastructures, the core business application service groups include the following:

- MyGPhC Pharmacy (Azure PaaS), Registrant Search (Azure Iaas)
- Finance & HR (solutions
- Education (SharePoint – O365)
- Intranet & Workflow (SharePoint – O365)
- Registrant Services (Dynamics CRM, Xperido, SharePoint (CRM), Doris,
- Business Intelligence (Tableau, Data Warehouse) (all IaaS)
- IT (System Center Service Manager, WSUS, Network Policy, Domain Controllers, Proxy services
- NetScaler

1.5.2 **Future Requirements**

The GPhC has services hosted in Microsoft Azure Platform-as-a-Service (PaaS) that is currently owned and managed by GPhC IT. The Managed Service Provider should demonstrate experience in managing and supporting Microsoft Azure Platform-as-a-Service (PaaS) offerings, including but not limited to Azure App Services and Azure SQL Database. The provider should also have capabilities in proactive monitoring, performance tuning, cost optimization, and incident management within Azure environments. In addition, the provider must offer comprehensive services in resource management, networking, security, data management (including databases), backup and disaster recovery, and scalability and performance optimization. Experience with compliance and security best practices in cloud-native architectures will be essential.

1.5.3 Though these are not part of this RFP, this will be a requirement once the services are up and running. the tenderer should include provision for consultant days post-launch, to enable

technical scoping and planning for a future PaaS migration.

1.5.4 The future scope may also include our Data Lake environment: options will be discussed with the new supplier at right time post contract to how best we can manage the Data Lake at optimum cost. High Level volumetrics (cloud environment)

1.5.5 Virtual Machines

Virtual Machines	OS	dev	hub	production	sbc-eicc	test	Grand Total
Standard_B2ms	Windows			1			1
Standard_B2s	Linux				2		2
Standard_D2as_v5	Windows		2				2
Standard_D2ds_v5	Windows		3				3
Standard_D2s_v5	Windows		1				1
Standard_D4ads_v5	Windows			6		6	12
Standard_D4as_v5	Windows		2				2
Standard_D4ds_v5	Windows		6	2			8
Standard_D4lds_v5	Windows				1		1
Standard_D4s_v5	Windows		1	2			3
Standard_D8ds_v5	Windows	1		3			4
Standard_E8ads_v5	Windows			1			1
Grand Total		1	15	15	3	6	40

In addition, we expect to have approx. five small servers (e.g. for SCCM, etc) still in our current datacentre provider environment, details given in 1.7.3

1.6 Statement of requirements

1.6.1 High level scope

The new supplier will be responsible for:

1. Providing a resilient and secure IaaS platform with automated provisioning solution in place which will include but not limited to hosting, database management, runtime support, middleware, operating system (OS) management. virtualisation, servers, storage, and shared network and security services.
2. Be responsible for support of the IaaS platform and keep it up to date with regular patching, upgrades as needed and fully optimised.

3. Be responsible for End User Computing e.g. desk top management for circa 300 users, Mobile device management which includes BYOD. Laptop refresh is expected to be done in 2026.
4. Adhere to technology, governance and service standards which align to ITIL and security standards. a
5. Seamlessly transitioning current Azure tenants and continually maintain and optimise the environments.
6. Ensure a strong change and release management process.
7. Ensure a strong governance model is in place which will include operational as well as strategic governance and ensure SLAs/OLAs are monitored continually and maintained.
8. Ensure strong security, disaster recovery and business continuity.
9. Support GPhC development teams as needed
10. Support the GPhC Cyber Security team
11. Assist GPhC in maximising return on investment.
12. Be innovative and assist GPhC in keeping their solution modern and be responsive.
13. Consultancy and advisory services: Provide expert resources and/or advise for project delivery in Infrastructure, Security, desk top management, Mobile device management and security and other areas as requested by GPhC.

1.6.2 End user computing

Scope includes desktop management and mobile device management. We have BOYD option for our resources

Further information on our current services is provided in the table below

Item	Further information
Laptops	Circa 300 Dynabook laptops (various models) Specification will change during the life of the contract.
Standard desktop build	• Windows 11 Cloud licence Annual update • Office 365 Semi-Annual channel update • Egress • Software Centre • eCopy PDF Pro • MS Defender • Chrome • VLC Media Player • Adobe Reader • Cisco AnyConnect Secure Mobility Client • Forcepoint • Any other as needed
Main ‘by request’ applications	• Visio • Project • Adobe DC Pro • Adobe Creative Cloud

Item	Further information
Desktop deployment and maintenance	• Rollout for refresh • By SCCM (Microsoft Endpoint Configuration Manager) • Asset lifecycle management including warrantee management
Patching	• By WSUS • Monthly patching cycle, 4 patch groups for end-user devices, 5 for servers • Critical patching separate cycle when required
Mobile device management	• By Intune
Security	• Endpoint protection, detection and response • Device encryptions • Ransomware protection (GPhC managed) • Access Control & Multi-Factor Authentication (MFA) • Intrusion detection and prevention • Vulnerability scanning and remediation • VPN and secure remote access • Any other as needed
End user support	• Multi-channel Service support as per SLA • Support Joiner and leaver management • User security awareness trainings (GPhC provided)

1.6.3 Data centre and office services

Items in current provider B scope

Item	Further information
Firewalls and switches	• 3 Cisco firewalls • 13 Cisco wireless access points • 2 Cisco data centre switches • 4 Cisco office data switches
Servers in primary data centre	• 5 servers
Servers in secondary data centre	• 5 servers

1.6.4 Cloud environments

Current GPhC environments are hosted in Azure and environments are:

- Azure fully managed service for:
  - Production environment
  - Test environment
  - Development environment
- Ownership Information: Current provider owned.
- Location: UK
- BC/HA/DR: associated redundancy / failover and recovery mechanisms as per SLA.

Resource details for VM

Cloud Resource Distribution

- Total VMs: 40

Refer to 1.5.5. for the full details.

Managed Disk

Server/Disk Type	Count	Size (GB)	Total Size (GB)	Typical DISKIOPS ReadWrite	Typical DiskMBps ReadWrite	Notes
Application Servers						
Application Data Disks	3	50	150	240 - 500	50 - 100	Includes - application-d disks
OS Disks	6	1 - 256	765	120 - 500	25 - 100	Includes standard OS disks
SQL Servers						
SQL Data Disks	8	1 - 400	1444	120 - 1100	25 - 125	Significant size and performance variation
SQL Log Disks	4	1 - 100	202	120 - 500	25 - 100	
SQL Backup Disks	4	1 - 100	202	120 - 500	25 - 100	
System DB Disks	4	Oct-16	52	120	25	Smaller, consistent performance
OS Disks	6	127	762	500	100	Standard OS disks
SSRS Servers						

Server/Disk Type	Count	Size (GB)	Total Size (GB)	Typical DISKIOPS ReadWrite	Typical DiskMBps ReadWrite	Notes
SQL Data Disks	2	100	200	500	100	
SQL Log Disks	2	128	256	500	100	
System DB Disks	2	16	32	120	25	
OS Disks	2	127	254	500	100	Standard OS disks
Web Servers						
Application Data Disks	2	50	100	240 - 500	50 - 100	Includes -application-d disks
OS Disks	2	127	254	500	100	Standard OS disks
Storage Servers						
Data Disks	12	20 - 4000	9210	500	100	Significant size variation
OS Disks	4	127 - 128	510	500	100	Standard OS disks
Domain Controllers						
OS Disks (C:)	2	127	254	500	100	
Backup Servers						
LUNs	2	4	8	120	25	
OS Disks	2	1	2	120	25	Very small OS disks
Other Servers						
Data/SSD Disks	4	50 - 128	356	500	100	Includes -data1, -data2, -ssd-data-1 disks
OS Disks	10	127 - 256	1665	500	100	Includes various named OS disks
Physical Drives	40	Jan-96	10783	120 - 7500	25 - 250	Variety of sizes and performance, often with ASR replicas
Upgrade Disk	1	10	10	500	60	
ASR Replica Disks	50	Jan-96	11359	120 - 7500	25 - 250	Corresponding ASR replicas for many of the above disks

Server/Disk Type	Count	Size (GB)	Total Size (GB)	Typical DISKIOPS ReadWrite	Typical DiskMBps ReadWrite	Notes
Total (Excluding ASR)			11890			
Total (Including ASR)			23249			

Database and Data Management

The MSP shall support all GPhC databases, mainly SQL Server as detailed in this document. Network connectivity between the Cluster and internal servers is via the VPN Gateway or private link service (for other GPhC production Azure VNET's).

For events, the database cluster will be scaled as appropriate and failed over as determined to be necessary in support of the expected event traffic.

SQL Server: need managed services for

D2s_v5	No of Instances
Standard edition	9
Enterprise edition	1
Enterprise edition (Always on)	2
Developer edition (Always on)	2
Developer edition	1

Azure Storage Account

Purpose/Workload	StorageAccountName	ResourceGroup	Kind	Tier	Notes
DR Cache	StorageAccount-DR1	DR-RG-Primary	Storage	-	Disaster Recovery Region
	StorageAccount-DR2	DR-RG-Primary	Storage	-	Disaster Recovery Region
	StorageAccount-DR3	Primary-RG	StorageV2	Hot	Primary Region

Purpose/Workload	StorageAccountName	ResourceGroup	Kind	Tier	Notes
	StorageAccount-DR4	DR-RG-Secondary	StorageV2	Hot	Secondary DR Region
Diagnostics	StorageAccount-Diag1	Primary-RG	StorageV2	Hot	Primary Region
	StorageAccount-Diag2	DR-RG-Secondary	StorageV2	Hot	Secondary DR Region
SQL Backups (Hot)	StorageAccount-SQL1	Primary-RG	StorageV2	Hot	Primary Region - Hot Tier
SQL Backups (Cool)	StorageAccount-SQL2	Primary-RG	StorageV2	Cool	Primary Region - Cool Tier
Disk Snapshots	StorageAccount-Snap1	Primary-RG	StorageV2	Cool	Primary Region
Archive/Long-Term	StorageAccount-Arch1	Primary-RG	StorageV2	Cool	Primary Region - Archive/Long-Term Data
Dev/Test	StorageAccount-Dev1	Dev-RG	StorageV2	Hot	Development/Testing Environment

- Hybrid Tiering: utilises both Hot and Cool storage tiers within StorageV2 in the primary region.
- Disaster Recovery Focus: Multiple storage accounts are located in designated Disaster Recovery Resource Groups.
- Primary Region Centrality: The majority of storage accounts reside in the primary resource group.
- Mixed Storage Account Kinds: Both newer StorageV2 and older Storage account kinds are in use.
- Workload Specificity: dedicated storage accounts for DR cache, diagnostics, SQL backups, and potentially archival data.
- Development Environment: A separate storage account exists for the development environment.

Service Bus

Total Active Service Bus Instances: 17

All instances are currently in Active state.

Service Tier Distribution:

- Standard Tier: 16 instances
- Basic Tier: 1 instance

Environment Coverage:

- Development: 4 instances
- UAT: 2 instances
- SIT: 1 instance
- PPD (Pre-Production): 4 instances
- Production: 6 instances

Disaster Recovery (DR) Instances:

A subset of services include DR versions deployed in geographically separate regions

Notes

- Use of DR instances reflects high availability and resilience planning.
- All production and critical pre-production services use the Standard tier, aligning with enterprise-grade requirements.

Network Security Group

Name	ResourceGroupName	Interface
NSG-Production-A	RG-Production-Primary	Multiple subnets, 0 network interfaces
NSG-Hub-Primary	RG-Hub-Primary	Single subnet, 0 network interfaces
NSG-DMZ-Primary	RG-Hub-Primary	Single subnet, Single network interface
NSG-DR-A	RG-DR-Primary	Multiple subnets, 0 network interfaces
NSG-Hub-Secondary	RG-Hub-Secondary	Multiple subnets, Single network interface
NSG-DMZ-Secondary	RG-Hub-Secondary	Single subnet, Single network interface
NSG-Development	RG-Development	Multiple subnets, 0 network interfaces
NSG-Management	RG-Hub-Primary	Single subnet, Single network interface
NSG-Test-A	RG-Test-Primary	Single subnet, 0 network interfaces
NSG-Test-B	RG-Test-Primary	Multiple subnets, 0 network interfaces
NSG-DR-Testing	RG-DR-Primary	Single subnet, 0 network interfaces

Key Vault

Total Active Key Vault Instances: 9

Environment Coverage:

- Development: 1 instance
- UAT: 1 instance
- SIT: 1 instance
- PPD (Pre-Production): 2 instances
- Production: 2 instances
- Core Services (T0): 1 instance
- gphc-sub-csp-primary: 1 instance

Tag Usage:

- Standard environments use consistent tags such as environment, serviceTag, templateref, and projectTag.
- One instance includes extended tagging for operational governance (e.g., monitoring, patching, support hours, billable status).

Notes:

- All environments are equipped with dedicated Key Vaults.
- Use of consistent naming conventions and tagging promotes operational clarity.
- Extended metadata in some environments shows enhanced governance and support capabilities.

These services are provided by the GPhC's current managed services provider. We are looking for

- a partner to provide IT infrastructure manged services covering all services as stated in section 1.4.1
- Ideally a single partner to deliver these services.
- a partner whose services facilitates the GPhC's compliance with data protection legislation.
- Business Application development, deployment, release management is currently done using DevOps methodology and new provider will support the DevOps teams in all aspect of deployment including release management.
- Incoming provider maximise deployment automation and aligned to CI/CD pipeline, including version control, and any automated testing frameworks as needed in place.
    1. Source code repository will be GPhC owned and managed, and shared access with supplier.

1.6.5 Service Management Specification

The GPhC is looking for a managed service provider who can provide the following services

1.6.5.1 Ongoing Hybrid

Operational services	Description
Managed intelligent monitoring	Security incident, capacity and availability monitoring of all services to include • Proactively monitor and manage the environments at Azure cloud environments, Data Centres and Customer Site • Monitor the utilisation of physical components • Perform analysis of utilisation data, forecasting and identification of trends • Leverage cloud native scalability • Automation and Remediation • Advanced threat detection across cloud resources • Raise Incidents with the Service Desk when an Incident is identified by the monitoring systems • Ensure the database environment is available and operating at the optimum levels • Monthly reporting and online dashboard access
Infrastructure as a Service (IaaS)	Providing platform management for the GPhC to include • manage the lifecycle of VMs, including provisioning, scaling, and decommissioning, ensuring optimal performance and resource utilisation and all associated firewalls and networking components as Infrastructure as a Service • Backup (automated) and recovery • Anti-virus • Availability and capacity monitoring • Event and incident management • Storage provision and management (as appropriate scalability and high performance) • O/S and component patching and upgrades • Disaster recovery provision, testing and enactment • Continue ensuring compatibility with GPhC's other infrastructure. • Hosting provided from UK Azure data centres
Hosting and rack management	Providing platform management for the GPhC to include • Racking of physical servers, gateway devices, firewalls and network components as applicable • Management of physical MS Windows servers • Backup and recovery • Anti-virus • Availability and capacity monitoring • Event and incident management

Operational services	Description
	• Storage provision and management • O/S and component patching and upgrades • Disaster recovery provision, testing and enactment • Hosting must be provided in UK data centres
Database administration	Provision of database administration to ensure the capacity, performance and supportability of the GPhC's databases to include: • Index rebuilds and adaptions • Reloads and reorganisation • Patching and version upgrades • Performance analysis and reporting • Performance Monitoring and Optimisation • Monitoring • Capacity analysis and reporting • Preventative action planning • Automated back-up and Recovery from backup • Recovery in the event of a DR activation • Right sizing databases as per actual usage • Implementing elastic pools for SQL Database when appropriate • Automation and DevOps Integration • FULL back up to Azure storage on a daily basis, retention period of 6 months for production and 4 months for UAT. and monthly/quarterly backups retained for up to 7 years as applicable for compliance purposes. • Log backups every hour, retained for 6 months for production and 4 months for UAT. • All stored data encrypted both at rest and in transit. • Approx 36TB of backup storage
WAN management	Oversight of suppliers delivering WAN services to include: • Provide a WAN Management Service to Customer's and the applications and services located within the Data Centre(s) • Traffic monitoring to detect when WAN links or components are not functioning correctly • Alerting WAN supplier(s) to issues that require their diagnosis and attention • Facilitation and assistance with procurement of new WAN services from third parties • Provision of any internal WAN services between the supplier's data centres that are part of the supplier's backbone that may be required for DR or other purposes

Operational services	Description
Internet	Provision of reliant internet break out to include: • Management of the GPhC's traffic filtering services • Burstable capacity to allow for variable load • Traffic analysis and reporting • Availability and capacity management • Monitoring • Provide redundant internet connectivity
LAN and WLAN management	Management of the GPhC's LAN and WLAN infrastructure to include: • Identity and Access Management and integration with onsite AD • Quality of service rules • Network segmentations • Switches • Bridges • Routers • Firewalls • Wireless access point • Guest and corporate Wi-Fi • Office switch racks and patching • Firmware updates • Configuration changes • Firewall rules • VLAN and IP ranges • Traffic routing • Traffic monitoring, analysis and optimisation including right sizing • WLAN controller integration with Azure management platforms • Wi-Fi analytics data integration with Azure data services • Intrusion prevention and detection • Data loss prevention and detection • Reserved capacity planning • Data classification and protection • Automation and Orchestration • BCDR • VPN connections to third party services
Managed domain controllers	Management of domain controllers and associated services to include: • Azure AD integration • Active Directory

Operational services	Description
	• DNS • DHCP • LAPS
Microsoft Software as a Service (SaaS)	Management of the configuration, deployment and updating of cloud software products to include: • Exchange online • Office 365 • SharePoint Online • Intune • OneDrive • Teams

1.6.5.2 End User Computing Services

Area	Description
Mobile device management	Provide profile management for DLP, registered and unregistered devices to include mobile phones, laptops and other PC hardware.
Desktop management	Management of user desktops to include: • Management of packaging of new and updated desktop components. Currently achieved using SCCM. • Provide and maintain a driver library to support all approved desktops and laptops • Gold build task sequence including standardised applications • Apply critical, security and recommended operating system patches • Desktop Application patching • Versions updates • Antivirus and malicious software management software provisioning, monitoring and event management • BOYD policy application, monitoring and management • VPN client installation and maintenance Ability to remote support (Currently SCCM & SfB)

1.6.5.3 Shared services (Hybrid and EUC)

Operational services	Description
Security management	Implement robust network security measures, including firewalls, intrusion detection/prevention systems (IDS/IPS), and

Operational services	Description
	DDoS protection. Configure and maintain a Security Service to include: • An up-to-date anti-virus and malicious software service for all Windows Operating System based desktops, laptops and servers • Patch management of servers and desktops • Security policy documents • Regular security audits • Email security to include encryption, anti-spam and virus scanning • Network vulnerability scanning, action planning and reporting • Week and compromised password scanning, resetting and reporting • Certificate management • Access control • Supporting penetration testing activities • Application and maintenance of Intune, DLP, Firewall and conditional access server policies and rules • Security incident and event management • Monthly and ad-hoc reporting • Configuration and deployment of anti-virus and malicious software management software including scanning schedules and performance management • identify any known security vulnerabilities or areas of concern that need to be addressed, e.g. outdated software ensure compliance with GDPR, and any other relevant data protection regulations, ensuring the secure handling of personal data.
Software deployment and version management	Software deployment for servers, laptops and desktops to include: • Deployment of O/S to servers, laptops and desktops • Deployment of version updates to installed software to servers, laptops and desktops Creation and maintenance of deployment packages such as SCCM MSI's
Asset management	The recording and management of logical and physical assets in all services to include • Accurate recording and maintenance of asset details • Identification of action required such as end of life assets • Identification of warranty and extended warranty expiration on assets • Identification of third-party support arrangements for assets

Operational services	Description
	Assistance with procuring third-party support
Service management	Management and oversight of the provision of all services to the GPhC to include • Monthly and quarterly service reviews and reporting against performance and availability SLA targets and KPI's • Service improvement plan management • Service change and adaption proposal management • Operation service escalation management • Root cause analysis and preventative action planning for major incidents • Asset registers • DR testing • Support from Level 3 onwards
Technical account management	Technical oversight of all services provided to the GPhC, whether operational or change, to ensure the quality and design of services provided by the supplier to include • Architectural documentation and governance • DR design • Preventative maintenance planning • Technical oversight of project and change proposals • Technical oversight of improvement actions • Member of the GPhC's CAB with responsibility for the quality of CAB proposals from the supplier Proposals and suggestion for technical improvements
Incident management	Management of break fix activity across all services to ensure minimum disruption with end-to-end ownership of all incidents and requests to include • Event / outage Management • Major incident management • Escalation processes • Progress communications • Service Desk • Service management systems • Accurate resolution details • Knowledge base • Root cause analysis • Communication management • Known issues register • Only level 3 and where appliable level 4 support. Level 1 and level 2 will be provided by GPhC

Operational services	Description
	• Service desk solution will need to be integrated with GPhC ServiceNow instance and supporting GPhC team with no end client calls. Currently approx. 2.5 calls are raised per month
Problem management	Management of problems arising from incidents or repetitive events to include • Analysis trends • Proposals for improvements and preventative actions • Tracking and reporting of problem resolution activity • Knowledge management Proactive problem management
Third party management	Management of tickets with suppliers of logical or physical infrastructural, network and desktop components to include • Performance Monitoring and management services provided by third parties • Raising support calls with suppliers • Gathering information requires by suppliers to assist with resolution • Tracking and escalation of tickets • Apply changes as required • Continuous Improvement • Documenting and addressing performance issues Assisting with procurement of third-party services
Operational change management	The management of the design, build and testing of changes to be applied to the GPhC operational environment to include • Standard changes for repetitious activity (requests) • Minor changes for low complexity low workload tasks (changes) • Major change / projects for complex and/or time-consuming changes (projects) • Assist in Change Assessment and Planning Supporting GPhC Change Advisory Board as needed
Release management	The management of the deployment of changes to the operational environment to include • Deployment scheduling and planning • Implementation planning • Backout strategies • Change sequencing and grouping • Post implementation testing • Physical and logical assets Training

1.6.5.4 Project Services

Projects	Description
Resources	The GPhC requires the partner to provide resources to deliver and support project work to include • Full delivery resources that will deliver projects through the full lifecycle including project management, design, build, testing, implementation and post go-live support. • Specified resources to support the delivery of projects managed by the GPhC's IT team
Approach	The partner will have standard approach/methodology for commissioning and delivering project work.
Cost models	The partner should have different cost options for projects including fixed cost, capped cost and time and materials.

Consultancy and advisory services	Description
Scope	The GPhC requires the partner to provide consultancy and advisory services to support the ongoing development and review of our IT service strategy and design, including helping to identify emerging or current • technology opportunities for the GPhC. • supplier services opportunities for the GPhC, • functional improvements to technologies and services used by the GPhC, • upcoming depreciation / retirement of services, technology or functionality in use in the GPhC and possible alternatives, • security threats and preventative actions. As part of this, the supplier should be capable of delivering technology gap assessments, road maps, technology architectures and operational modelling.

1.6.5.5 Transition

Transition	Description
Service transition	The partner must be able to deliver a project to transition services from the current partner.

Additional notes:

- The MSP shall track and report on key performance metrics, including uptime, response times, and resource utilisation.
- The GPhC Cyber Security team shall be provided the access to configure Event Hub and Event Hub Namespaces (or similar services) within the Azure tenant which will allow for log export from all Azure resources for GPhC review.
- Additionally, should the GPhC Cyber Security team's monitoring requirements change, then rights to amend the monitoring configuration within Azure will be permitted via the request of the formal change control process.
- The GPhC Cyber Security team shall be provided the access to configure Event Hub and Event Hub Namespaces (or similar services) within the Azure tenant which will allow for log export from all Azure resources for GPhC review.
- Additionally, should the GPhC Cyber Security team's monitoring requirements change, then rights to amend the monitoring configuration within Azure will be permitted via the request of the formal change control process.
- Reporting and monitoring from a Virtual Machine Cyber Security aspect will also be mandated, to ensure that the coverage of any Anti-Virus product is fully compliant and up to date, and that the Access Control requirements (as detailed in the SLA) are compliant.
- Reporting and monitoring from a Virtual Machine Cyber Security aspect will also be mandated, to ensure that the coverage of any Anti-Virus product is fully compliant and up to date, and that the Access Control requirements (as detailed in the SLA) are compliant.

Security Vulnerabilities

The MSP shall identify and address issues such as outdated software versions, unpatched systems, and lack of encryption.

Along with this, the GPhC ITD Cyber Security team will need to be granted the ability to perform both scheduled and ad hoc nonservice impacting Vulnerability Management scans on all Virtual Machines hosting GPhC data or services. The GPhC security team also must have visibility and report running capability on all Virtual Machines hosting GPhC data or services.

All vulnerabilities that are identified would need to be triaged between the MSP and the GPhC Cyber Security team, and if deemed appropriate then further action would need to be taken via Change Control to resolve the vulnerability.

If “Zero Day” vulnerabilities are discovered, then a fast-track process would need to be established between the MSP and the GPhC Cyber Security team, in line with the SLA, to allow the rapid controlled deployment of any fixes that are required via Change Control.

All security patches, fixes, upgrades, etc. will need to be implemented in line of the requirements the in-place Cyber Security Frameworks and accreditations (i.e. CE+).

Access Control

The MSP must implement strict access control policies, including multi-factor authentication (MFA) for administrative access, this should also include Conditional Access policies that restrict admin access to known locations.

Additionally, a formal approval process must be in place that allows for administrative access to any GPhC data.

Once granted, the administrator should be granted a pre-determined role using standard RBAC functionality. High level privileges have to be se as “Eligible”. Every role and permission need to be set for the period of time while the project or task requires and remove them once they completed.

Administrative access will be monitored to any GPhC data, and any unexpected logins from unexpected locations will be challenged by the GPhC Cyber Security team and will result in a high priority incident being logged, in line with the SLA.

A process must exist with the provider to ensure auditability and transparency that users who no longer require access to GPhC data are restricted from further access.

Security Practices

In line with GPhC Cyber Security architecture standards, we require a layered approach to Cyber Security, including but not limited to an Azure based firewall, DDoS protection and secure encryption protocols for data in transit and at rest.

- Additionally, items such as a Web Application Firewall and Azure Key Vault within Azure should be fully supportable, if deemed as required by the GPhC Web Support team.
- Best practice Items such as Azure Storage Key rotation policies should be managed and controlled via standard change control processes.
- Standard items such as Network security items including, NSG and Azure Firewalls should be fully inspected regularly for signs of misconfiguration that expose the GPhC servers,
- services unnecessarily to the internet.
- A supported and managed Anti Malware software package should be deployed across all hosts that contain GPhC data and/or services, the Anti Malware packed must be updated in real time and must be operational 24*7*365 in line with the SLA.
- Continue supporting GPhC’s layered existing cyber security tolls and solutions. (I.e. Proxy solution, Spam filtering)

2 SLA/KPIs

2.1 Generic

- Root Cause Analysis (RCA) – published within 14 days of the incident resolution.
- Monthly Service Reporting including monthly review meetings with near real time dashboard availability.
- Service availability calculations to include outages caused by unplanned maintenance.

2.2 System Availability

- Uptime system percentage:
    - 99.95%.measured monthly.
    - Service credit

  Service Level <99.95%, >99.7% Service Credit = 4% of Monthly Charge

  Service Level <=99.7% >98% Service Credit = 6% of Monthly Charge

  Service Level <=98% >97% Service Credit = 10% of Monthly Charge

    - Service Level <=97% Service Credit = 15% of Monthly Charge
- Internet availability:
    - 99.95%. measured monthly.
    - Service credit

  Service Level <99.95%, >99.7% Service Credit = 3% of Monthly Charge

  Service Level <=99.7% >98% Service Credit = 4% of Monthly Charge

  Service Level <=98% >97% Service Credit = 5% of Monthly Charge

    - Service Level <=97% Service Credit = 10% of Monthly Charge
    -
- Scheduled maintenance windows: 120 min per month outside working hours or during weekends.
- Support Hours:
    - 24x7x365 – Critical Support.

2. 8 to 6 PM – Non-Critical Support.

3 Anti-virus and patching

- No server with Anti-Virus signature versions out of date: measured monthly.
- Critical security patches as soon as possible maximum within 24 hours and for any other event within 2 Days unless otherwise agreed to by the Parties.
- None of the Servers with 2 or more MS Security Patch versions out of date: measured monthly.

4 Anti Malware system

Fully managed, monitored and up to date in place with real time updates, stop known Malware attacks via dictionary updates and behavioural attacks via kill chain process for 24*7*365.

5 Business continuity and Disaster Recovery

- Recovery Time Objective (RTO): less than 4 hours.
- Recovery Point Objective (RPO): Critical data less than 1 hours. Semi-critical less than 4 hours.
- Regular disaster recovery testing: annually.

5.1 Incident Management

Priority	Definition	Response Time	Resolution Time
P1 Severe	A complete failure of the production environment has occurred, or a critical business process is at risk due to an issue in the system. (e.g. Month end reporting, access to system for all users). There is no work around and the impact is likely to go on for a protracted period. P1 incidents take priority over all other requests. Hours considered are calendar hours 24x7x365 excluding Bank Holidays.	100% within 30 minutes	100% in 4 hours
P2 Major	Major problem within production environment. Incident affects a large portion of the GPhC community. Includes high visibility problems and time-sensitive issues. Examples include month end transaction generation, reporting not working, and interfaces are not functioning. Hours considered are working hours between 8AM to 6PM Mon-Fri inclusive.	100% within 60 min	100% in 8 hours
P3 Moderate	Problems exist with production, and it affects a few users on a regular basis, thereby preventing work from being completed. Inability to access a specific function that has been implemented might be an example here. Full failure of a non-production environment. Normal working hours.	100% within 2 hours	85% in 48 hours, 100% in 5 days
P4 Minor	An informational inquiry or non-recurring incident in production that affects a few non-critical users or process, and a workaround is readily available. Normal working hours.	85% within 4 hours	5 working days

- Response times are measured from the time an incident is raised by a user and captured in the ticketing system. Resolution times are based upon the time an incident first occurs up to the point that service is restored, either via a workaround or a permanent fix in Production.
- Incident Management statistics provided weekly for review and available on a dashboard online.
- All resolved P1 incidents must result in a Problem ticket being created so that full RCA work can be tracked and completed.
- Security Incident Notification:

3. Immediate Alerts: notified of any critical incidents within 30 minutes of detection.
4. Detailed Incident Reports: Within 4 hours of an incident, a preliminary report should be provided, with a full incident report, including root cause analysis, delivered within 72 hours.

- Escalation Process: An escalation path for unresolved issues must be in place, including contact points and processes to involve senior leadership.
- Communication channels are dashboard, phone, WhatsApp/SMS, appropriate incident update calls, etc.
- Post-Incident Review: A comprehensive post-incident review should be conducted within 3 days of incident resolution to identify lessons learned and prevent recurrence.

5.2 Service Requests

Priority	Definition	Response Time	Resolution Time
1 Critical	A service request that needs to be addressed the same working day to meet business deadlines. e.g.: user access at a business-critical time Emergency chart of Account change Unscheduled unlocking of database users accounts and passwords Emergency deployment of a business-critical application /patch to remediate a business-critical defect Data fixes of transactions impacting month end close timetable Firewall changes	2 hours	4 hours
2 High	Supporting account creation and administration, etc.	6 hours	24 hours
3 Medium	Requests that have a low impact on the day-to-day business as usual activities (such as a minor modification to a report)	24 hours	10 days

Priority	Definition	Response Time	Resolution Time
	Security audit changes SSL cert renewals changes		Virtual servers 2-5 days Physical severs 5-10 days
4 Low	Information requests System monitoring – adds/removes/changes Additional servers to be added to environment	48 hours	20 days

Production SLAs for Service Request Management run from 8AM to 6PM, Monday to Friday inclusive.

5.3 Pricing and Billing

Transparent Pricing: MSP will provide clear, detailed pricing information, including what is covered under the SLA.

5.4 Documentation and Knowledge Transfer

Documentation: Ensure the MSP provides comprehensive documentation of your environment, configurations, and procedures.

5.5 Core Resourcing

MSP will ensure that core resources are identified and are changed in agreement with us. If any need to be replaced, detailed handover plan will be shared and implemented without any impact on service.

5.6 Other security SLAs to consider:

5.6.1 Data Protection and Encryption

Data at Rest Encryption: AES-256.
Encryption Management: encryption keys managed using a secure, centralised key management system (KMS). A tool such as Azure Key Vault to safeguard encryption keys.
Data in Transit Encryption: Encryption Protocols: encrypted using protocols such as TLS 1.2 or TLS 1.3. No earlier version of encryption should be used Mutual TLS: Where applicable.
Encryption Key Management: Key Lifecycle Management: - keys must be rotated at least every 12 months or as specified by GPhC.
Key Access Control: Azure based keys should be stored in a secure environment such as an Azure Key Vault, with access restricted to admin personnel.

5.6.2 Firewall Control

A fully managed Firewall solution – potentially compromising of multiple layers must be enforced and maintained in order to protect GPhC data and services.
Industry IOC Feeds: The fully managed Firewall solution must be updated regularly (maximum 48 hours) with current Live IOC feeds from the internet, to ensure attack traffic is blocked.
The Firewall must have an industry tried and tested IDS/IPS system in use as well as standard port and IP blocking which is applied regulatory on a schedule.

5.6.3 Access Control and Identity Management

Multi-Factor Authentication (MFA): Is mandated for all admin connections.
Role-Based Access Control (RBAC): Must be in place.
Joiner/Mover/Leaver process in place and access hygiene maintained via a full audit trail.
Periodic Review of access rights and roles used ideally quarterly.

5.6.4 Vulnerability Scanning

Automated scans conducted at least weekly and manual scans done monthly or quarterly, depending on complexity and sensitivity with access to GPhC scan as needed.
Remediation SLA: critical issues resolved within 24 hours.

5.6.5 Penetration Testing

External penetration tests conducted annually, and internal penetration tests conducted semi-annually.
Remediation and Reporting: address critical issues within 20 days and detailed report provided.

5.6.6 Security Event Monitoring

Security Log Retained for minimum of 90 days online and up to 1 year in archive.
Immutable Logs stored in an immutable format to prevent tampering or unauthorised modifications.

5.6.7 Log Access

On-Demand Access: GPhC should be able to access relevant logs within 24 hours of request to conduct its own investigations or audits as needed.

5.6.8 Compliance Audits

MSP will complete a GPhC Cloud Host Security Questionnaire prior to hosting any data.

The MSP undergoes third-party audits, such as SOC 2, ISO:27001, or PCI DSS, annually or as applicable with audit results and remediation plans, made available within 30 days of audit's completion, mitigation discussed and in place.

5.6.9 Regulatory Compliance

Complies with all applicable regulations, e.g. GDPR, CCPA, including data handling practices, breach notifications, and rights of data subjects (AS APPLICABLE).
Will maintain up-to-date compliance certifications and provide evidence of compliance upon request.

5.6.10 Audit Logging

Logging Integrity: All actions within the cloud environment, particularly those affecting security and compliance, should be logged in an auditable manner. These logs should be accessible to customers for compliance verification, and system logs will be transferred to the GPhC SIEM environment.

5.6.11 Data Residency

Geographic Location: Data must be stored in UK geographic regions.
If data must be transferred across borders, the MSP must ensure that appropriate legal safeguards, such as Standard Contractual Clauses (SCCs), are in place with prior approval from GPhC.

5.6.12 Data Anonymisation

As applicable, sensitive data to be anonymised or pseudonymised before processing.
Ensure that anonymisation techniques comply with relevant data privacy laws and standards.

5.6.13 Data Deletion

Data deletion requests are processed within a specific timeframe, such as within 30 days and certification or confirmation provided once data has been successfully deleted, or disk crushed.

5.6.14 Service Availability and Security

Ensure protection against DoS and DDoS attacks, including the time to mitigate such attacks.
Notify immediately in the event of a data breach (within 4 hours of detection).

5.6.15 Third-Party and Supply Chain Management

Ensure that the entire ecosystem is secure including vetting and monitoring third-party service providers.

5.6.16 Training and Awareness

Annual training sessions for all involved personnels, with availability of completion certificates.

5.6.17 Service Credit

Service Credit Cap In the period from the Call Off Commencement Date to the end of the first Call Off Contract Year 15% of the monthly Call Off Contract Charges per month; and during the remainder of the Call Off Contract Period, 15% of the monthly Call Off Contract Charges per month in the period of twelve (12) Months immediately preceding the Month in respect of which Service Credits are accrued.

SERVICE LEVEL NOTIFICATION In the event that the Supplier fails (or believes that it is likely to fail) to meet any Target Service Level, the Supplier will:

- notify the GPhC of such actual or anticipated Service Failure;
- investigate the underlying causes of such Service Failure;
- take whatever reasonable action is necessary to prevent such a Service Failure from occurring or recurring; and
- advise GPhC of the status of preventative or remedial efforts being undertaken with respect to the underlying cause of such a Service Failure, and regularly keep GPhC so advised.

- The Supplier shall measure its performance against the Target Service Levels and shall report on Actual Service Levels to GPhC.

SERVICE CREDITS GPhC shall use the Service Review meeting to verify the calculation and accuracy of the Service Credits, if any, applicable to each relevant Service Period.

- Service Credits are a reduction of the amounts charged to the GPhC by the Supplier in respect of the Services. Service Credit entitlement shall be calculated by the Supplier at the end of each Service Period and discussed with the GPhC at the Quarterly Service Review Meeting that next follows the end of the Service Periods in question.
- Service Credits will be paid to the GPhC, or subsequent invoices reduced to reflect Service Credits. If DR is invoked for one or more individual services as the quickest method to recover the Service in the event of an Incident, the Incident Target Fix and Service Credits apply. If DR is invoked due to a total failure, then the RTO / RPO targets, as defined in the DR Plan will be used instead of the Incident Target Fix when assessing levels of Service Credits that apply.

6.0. Social Value

Social value is about making sure that what we buy creates an overall positive impact on our people and communities. The way we intend to use social value in our tenders takes into account the Government National Procurement Policy Statement. Our chosen policy outcome is to Kick start economic growth. To secure the highest sustained growth in the G7 - with good jobs and productivity growth in every part of the country making everyone, not just a few, better off for creating employment and training opportunities. As a supplier bidding for public contracts, we require you to make commitments to meeting the social value agenda as part of the contract delivery. A model answer is applied, and bidders can select from the illustrations as set out in the evaluation criteria.