



Microsoft Purview Information Governance and Records Management

Contracting body

30 Jan 2026

Issue 1.0

© 2026 CGI IT UK Ltd

CGI

Table of contents

1.	Service Description	5
2.	Data backup and restore	6
3.	Service Continuity	7
4.	Onboarding and Offboarding	7
5.	Service constraints	8
6.	Service levels	9
7.	After sales support	10
8.	Technical requirements	11
9.	Outage and maintenance management	12
10.	Hosting options and locations	12
11.	Security	13
12.	Service Pricing and Terms and Conditions	14
13.	Further information	14
PROPRIETARY AND CONFIDENTIAL		15

Service Definition overview

The Microsoft Purview Information Governance and Records Management Advisory is a cloud support advisory service delivered by CGI to help organisations design, assess, and improve their approach to information governance, data protection, and records management within Microsoft 365 using Microsoft Purview.

The service supports organisations in establishing appropriate policy, governance, and operating controls for managing information across Microsoft 365 workloads. This includes advisory coverage of relevant Microsoft Purview capabilities such as sensitivity labels, data loss prevention (DLP) policies, information classification and discovery, retention and records management, and associated compliance and detection policies (for example, communication compliance and insider risk policies), where available and within the agreed scope.

CGI works with customers to assess the current state of their Purview configuration and governance arrangements, identify gaps, risks, and inconsistencies, and define a structured, policy-led approach aligned to organisational objectives, regulatory obligations, and public sector assurance expectations. The advisory considers how Purview capabilities are used collectively, rather than in isolation, to support consistent information control and defensible governance outcomes.

This service is advisory in nature. It does not include the configuration, deployment, or operational management of Microsoft Purview or Microsoft 365 services. CGI provides structured analysis, architectural guidance, and prioritised recommendations to support informed decision-making and to enable customers to plan subsequent implementation activities under separate arrangements, where required.

The service is suitable for organisations seeking to establish or mature their information governance and records management capability, improve assurance and consistency across existing Purview controls, or prepare their Microsoft 365 information landscape to support advanced capabilities such as Microsoft 365 Copilot.

Why CGI?

GI brings deep expertise in information governance, records management, and Microsoft 365 architecture, supporting organisations to design and operate defensible, policy-led governance models using Microsoft Purview. We help organisations apply Purview capabilities in a way that is consistent, proportionate, and aligned with organisational objectives, regulatory obligations, and public-sector assurance expectations.

CGI combines Microsoft platform knowledge with practical experience in governance, risk management, and operating model design. We understand that effective information governance requires more than enabling technical features; it depends on clear ownership, well-defined policies, integration with business processes, and controls that can be evidenced, audited, and sustained over time. Our advisory therefore considers how Microsoft Purview Information Governance and Records Management capabilities work together as part of a coherent framework, rather than as isolated controls.

Our approach covers the full information lifecycle and the way Purview capabilities support it, including:

- Information classification and sensitivity labelling.
- Data Loss Prevention (DLP) policy design and enforcement.
- Retention and disposal policies.
- Records declaration and management.
- eDiscovery and audit considerations.
- Insider risk and communication compliance (where applicable).
- Alignment between policy, technology, and user behaviour.

CGI advises on how these capabilities should be governed, approved, and operated to meet legal, regulatory, and organisational requirements, particularly in public-sector and regulated environments where defensibility and accountability are critical.

Delivery is led by senior consultants and architects with experience advising public-sector and regulated organisations. CGI works closely with information governance, records management, legal, data protection, security, and IT stakeholders to ensure recommendations are realistic, implementable, and aligned with organisational risk appetite. We place particular emphasis on clarity of accountability, decision rights, and lifecycle ownership, recognising these as common failure points in information governance programmes.

CGI delivers this service as an independent advisory engagement. We do not promote proprietary tools, accelerators, or pre-defined solutions. Recommendations are grounded in evidence gathered through stakeholder engagement, documentation review, and agreed technical insight. This ensures that advice is tailored to the customer's environment, maturity, and statutory obligations, rather than based on generic best practice.

This service forms part of CGI's broader capability in digital workplace governance, enterprise architecture, and information management advisory. It can be used independently or alongside related advisory services, such as Microsoft 365 optimisation or Copilot governance and readiness, without overlap or dependency.

How CGI works with customers

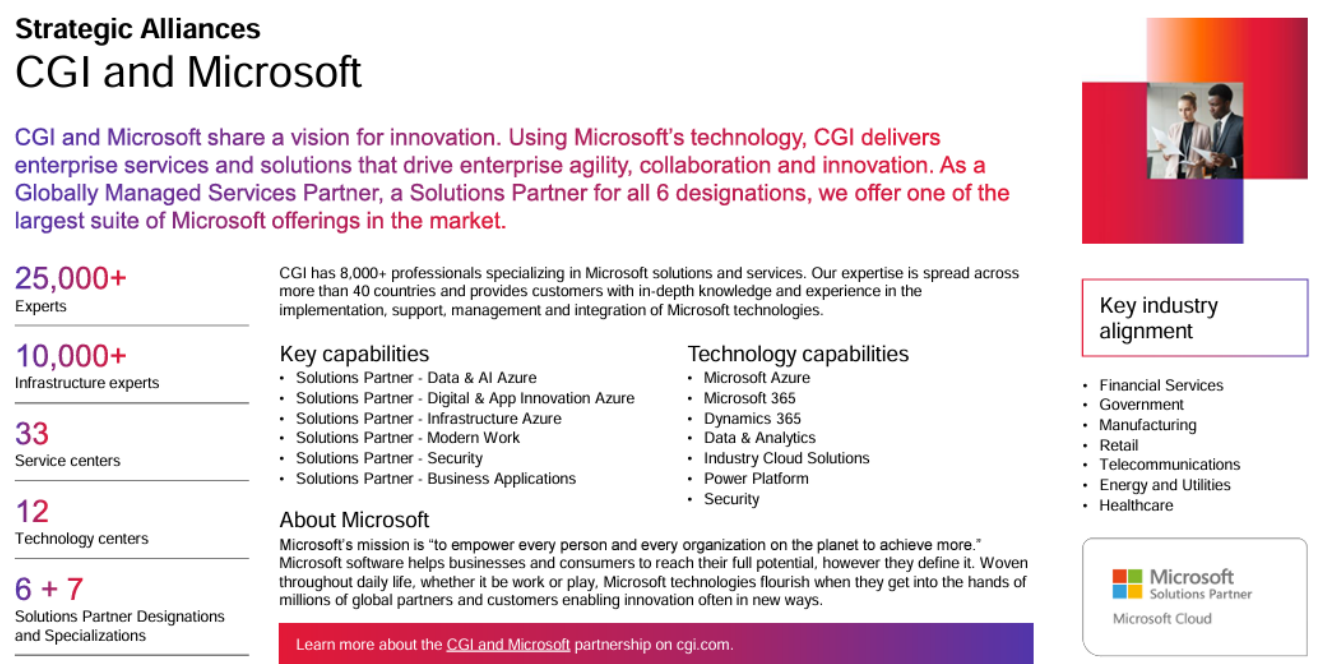
CGI works with multi-disciplinary customer teams to ensure that information governance recommendations are balanced across policy, technology, and operational delivery. Engagement typically involves collaboration with:

- Information governance and records management leads.
- Legal and data protection representatives.
- Security and compliance stakeholders.
- Microsoft 365 platform and service owners.
- Business representatives responsible for regulated or high-risk information.

CGI facilitates structured workshops, evidence reviews, and validation sessions to ensure that findings and recommendations accurately reflect how information is created, used, retained, and disposed of across the organisation.

What differentiates CGI for this service

- Governance-led advisory: Focus on defensible, policy-driven information governance rather than feature enablement.
- Public-sector assurance mindset: Recommendations aligned to regulatory scrutiny, auditability, and accountability requirements.
- Lifecycle-based approach: Coverage of information from creation through retention, records management, and disposal.
- Clear operating models: Emphasis on ownership, decision rights, and sustainable governance structures.
- Independent advice: No dependency on implementation services or proprietary tooling.



Compliance & Oversight	Audit, reporting, and monitoring considerations to support assurance
Detection & Investigation	Advisory considerations for Purview detection and alerting capabilities

The service considers both technical configuration and non-technical factors, including governance structures, accountability, policy ownership, and operational processes. Recommendations are developed with reference to organisational risk appetite, regulatory context, and existing information management practices.

1.2. Advisory Nature of the Service

This service is advisory in nature. CGI does not configure Microsoft Purview, apply labels or policies, declare records, migrate content, or operate records management processes as part of this engagement. All outputs are provided as recommendations and planning artefacts only.

Where organisations choose to proceed to implementation or remediation, this can be supported under separate contracts or service arrangements.

1.3. Delivery Approach

CGI delivers the service through a structured engagement that typically includes:

- Discovery and scoping to confirm objectives, priorities, and constraints.
- Review of governance artefacts and Microsoft 365 configuration (read-only or evidence-based).
- Engagement with information governance, records management, legal, security, and IT stakeholders.
- Development of prioritised, evidence-based recommendations and an improvement roadmap.
- The outputs provide organisations with a clear understanding of their current Microsoft Purview governance maturity and a practical, defensible plan to strengthen information governance and records management in line with public-sector expectations.

2. Data backup and restore

The Microsoft Purview Information Governance and Records Management Advisory is an advisory service and does not include the provision, operation, or management of data backup or data restore capabilities.

Microsoft Purview operates within the customer’s existing Microsoft 365 tenant and relies on the organisation’s configured data protection, retention, and recovery mechanisms. CGI does not provide backup or restore services and does not operate or manage customer data as part of this engagement.

As part of this service:

- CGI does not perform backup, restore, or data recovery activities for Microsoft 365 workloads.
- CGI does not configure, test, or validate backup or restore solutions.
- Responsibility for data protection, backup, retention, and recovery remains with the customer and their platform providers, including Microsoft.
- No service levels are provided for backup or restore under this advisory service.

Where relevant to the agreed scope, CGI may review backup, retention, and recovery arrangements at a high level as they relate to information governance and records management objectives. This may include advisory considerations such as:

- Alignment between retention policies and organisational backup practices.
- Interaction between records retention, legal hold, and recovery processes.
- Risks associated with over-retention, premature deletion, or unsupported restore scenarios.

Any such input is advisory only and is provided to support governance decision-making. CGI does not perform configuration changes, operational testing, or assurance activities, and does not warrant or certify the effectiveness of backup or recovery arrangements.

3. Service Continuity

The Microsoft Purview Information Governance and Records Management Advisory is delivered as a time-bound, advisory engagement. Service continuity in this context relates to CGI's ability to continue delivery of the advisory service and to handle customer information securely, rather than the continuity or availability of the customer's Microsoft 365 environment or data.

CGI maintains internal arrangements to ensure continuity of advisory delivery throughout the engagement. These arrangements are designed to minimise disruption and ensure that agreed outputs can be delivered even where delivery circumstances change.

Key aspects of service continuity include:

- Delivery managed through an agreed engagement plan, with defined milestones, deliverables, and responsibilities.
- Use of appropriately resourced delivery teams, with documented approaches and artefacts to support continuity.
- Internal knowledge sharing and handover processes to mitigate the impact of staff absence or change.
- Secure handling of customer information and artefacts in line with CGI's information security policies.

As this service is advisory in nature:

- CGI does not provide business continuity or disaster recovery services for customer systems or data.
- CGI does not operate, manage, or support Microsoft 365, Microsoft Purview, or associated workloads.
- Continuity of customer platforms, data, and services remains the responsibility of the customer and their technology providers, including Microsoft.

In the event that circumstances arise which may affect delivery of the advisory service, CGI will communicate with the customer in a timely manner and agree any necessary adjustments to delivery approach or timelines.

4. Onboarding and Offboarding

This section describes onboarding and offboarding arrangements for the advisory service only. It does not relate to onboarding or offboarding of Microsoft 365 users, administrators, or operational services.

4.1. Onboarding

CGI supports onboarding to the service through a structured initiation process designed to confirm scope, access, and governance arrangements prior to delivery. This typically includes:

- Introductory discussions to confirm objectives, scope, priorities, and success criteria.
- Identification of key stakeholders across information governance, records management, security, legal, compliance, and IT.
- Agreement of documentation and evidence required to support the advisory assessment.
- Confirmation of access arrangements to Microsoft 365 administrative information (read-only where possible).
- Establishment of agreed collaboration mechanisms (for example, a Microsoft Teams workspace).
- Scheduling of workshops, interviews, and validation sessions.
- Confirmation of delivery governance, reporting cadence, and escalation routes.

CGI does not require privileged or persistent administrative access to customer systems. Where access is required, this is limited to read-only access or the provision of exported configuration, reports, or documentation, agreed in advance.

4.2. Offboarding

At completion of the engagement, CGI supports a controlled and orderly service exit. This typically includes:

- Delivery of final advisory outputs, including governance assessments, findings, and recommendations.

- Provision of information governance and records management recommendations relevant to Microsoft Purview, where in scope.
- Knowledge transfer sessions to support customer understanding of outputs and next steps.
- Handover of all deliverables agreed within the Statement of Work.

CGI ensures that the service concludes without creating ongoing operational or support dependencies on CGI resources.

4.3. Access to Data Upon Exit

CGI does not store or retain customer production data as part of this advisory service.

Upon exit from the service, the customer retains full ownership and control of:

- All documentation and artefacts produced during the engagement.
- All Microsoft 365 and Microsoft Purview configurations.
- Any workshop outputs, assessments, or governance frameworks developed.

Any temporary access, collaboration workspaces, or document-sharing permissions granted to CGI for the purposes of the engagement are removed in accordance with CGI's internal data-handling policies and the customer's security requirements.

5. Service constraints

The Microsoft Purview Information Governance and Records Management Advisory is delivered as a time-bound, advisory-only service and is subject to the following constraints.

5.1. Advisory Scope Constraints

- The service is advisory in nature. CGI provides assessment, analysis, design guidance, and recommendations only.
- The service does not include configuration, deployment, remediation, implementation, or operational management of Microsoft Purview, Microsoft 365, or related workloads.
- CGI does not enable or modify sensitivity labels, retention labels, retention policies, records management settings, DLP policies, or audit configurations as part of this service unless explicitly agreed under a separate contract.

5.2. Access and Dependency Constraints

- Delivery is dependent on the availability of appropriate customer stakeholders for workshops, interviews, validation sessions, and decision-making.
- Recommendations are based on evidence gathered through agreed access to documentation, exported configuration data, and read-only access to Microsoft 365 or Purview administrative portals where permitted.
- Where access to systems, documentation, or stakeholders is limited, CGI documents assumptions and constraints and tailors recommendations accordingly.

5.3. Scope and Coverage Constraints

- The depth and breadth of the advisory are constrained by the agreed scope, duration, and effort defined in the Statement of Work.
- CGI does not provide a comprehensive review of all Microsoft 365 workloads, Purview capabilities, or third-party systems unless explicitly included in scope.
- Advice relating to third-party applications, repositories, or integrations is limited to information provided by the customer and does not include technical validation or assurance.

5.4. Licensing and Platform Constraints

- Recommendations are provided based on the customer's existing Microsoft 365 and Microsoft Purview licensing and feature availability.
- CGI does not procure, enable, modify, or manage Microsoft licences as part of this service.
- The availability and behaviour of Microsoft Purview features remain subject to Microsoft's product roadmap, service limits, and platform constraints.

5.5. Assurance and Compliance Constraints

- The service does not provide formal security accreditation, compliance certification, penetration testing, or legal assurance.
- CGI does not provide binding legal advice; recommendations relating to regulatory or legal requirements are provided for governance planning purposes only.
- Responsibility for compliance decisions, risk acceptance, and operational controls remains with the customer.

5.6. Operational Constraints

- CGI does not provide 24/7 support, incident management, or operational monitoring as part of this advisory service.
- No changes are made to live production environments as part of delivery unless explicitly agreed under a separate implementation engagement.
- CGI will communicate any material constraints, risks, or dependencies identified during delivery and will work with the customer to agree appropriate mitigations or adjustments within the bounds of the advisory service.

6. Service levels

The Microsoft Purview Information Governance and Records Management Advisory is delivered as a time-bound professional advisory service. As such, traditional operational service levels (for example, system availability, incident response times, or platform performance SLAs) do not apply.

Service levels relate to the management and delivery of the advisory engagement, rather than the operation or performance of Microsoft Purview, Microsoft 365, or associated workloads.

6.1. Advisory Service Levels

CGI delivers the service in accordance with an agreed engagement plan and Statement of Work, which defines scope, duration, milestones, and deliverables. Service levels are agreed during onboarding and are proportionate to the size and complexity of the engagement.

Key service level characteristics include:

- Delivery during standard UK business hours, unless otherwise agreed.
- A named CGI engagement lead responsible for coordination, delivery, and stakeholder communication.
- Delivery of agreed milestones and advisory outputs within the agreed timescales.
- Regular progress updates provided through agreed governance and reporting mechanisms.
- Structured management of risks, issues, and dependencies throughout the engagement.

6.2. Quality and Governance

CGI applies internal quality assurance and governance processes to ensure that advisory outputs are:

- Accurate, evidence-based, and aligned with the agreed scope.
- Consistent with Microsoft Purview capabilities and documented platform behaviour.
- Aligned with public-sector information governance, records management, and assurance expectations.

- Clearly documented and suitable for onward use by the customer.

6.3. Exclusions from Service Levels

As this is an advisory service:

- CGI does not provide service level agreements (SLAs) for Microsoft Purview, Microsoft 365, or any related platforms.
- CGI does not provide incident response, break-fix support, or operational monitoring.
- CGI does not guarantee specific business outcomes, compliance outcomes, or platform performance.
- Service levels for Microsoft 365 and Purview remain the responsibility of Microsoft under the customer's subscription.

6.4. Change Management

Any changes to scope, timelines, or delivery approach are managed through agreed change control arrangements and documented accordingly.

This approach ensures transparency, predictability, and clear accountability for delivery of the advisory service, while avoiding any overlap with operational or managed service responsibilities.

7. After sales support

The Microsoft Purview Information Governance and Records Management Advisory is delivered as a time-bound professional advisory engagement. After-sales support is limited to clarification and knowledge transfer associated with the outputs produced during delivery and does not constitute ongoing operational, technical, or managed support.

7.1. Scope of After-Sales Support

Following completion of the engagement, CGI provides a defined and proportionate period of after-sales support to:

- Clarify findings, recommendations, and deliverables produced as part of the advisory.
- Respond to reasonable questions relating to the interpretation and intended use of the outputs.
- Support customer understanding of the recommended governance model, records management approach, and roadmap.
- Assist with handover of documentation to relevant operational, governance, or assurance teams.

This support is intended to ensure that advisory outputs can be understood, socialised, and taken forward by the customer without dependency on CGI.

Exclusions from After-Sales Support.

7.2. After-sales support does not include:

- Additional assessment or discovery activities.
- Rework or expansion of agreed deliverables.
- Configuration, deployment, or implementation of Microsoft Purview features.
- Operational support, monitoring, or administration of Microsoft 365 or Purview.
- Records operations, retention execution, or content remediation.
- Break-fix support or incident handling.

Any requirement for further advisory input, implementation services, or ongoing governance support can be discussed separately and, where appropriate, contracted under a new or extended engagement.

7.3. Ongoing Support Options

CGI does not provide ongoing managed services or operational support as part of this advisory. However, customers may choose to engage CGI separately for:

- Extended information governance or records management advisory.
- Implementation support for Microsoft Purview capabilities.
- Ongoing governance operating model support.
- Assurance, maturity reviews, or optimisation activities.

This ensures a clear separation between advisory guidance and operational responsibility, in line with G-Cloud expectations.

8. Technical requirements

This advisory service does not require the installation of software, deployment of tooling, or changes to the customer's Microsoft 365 or Microsoft Purview environment.

Delivery is dependent on the availability of appropriate access, information, and collaboration facilities, agreed during onboarding.

8.1. Customer Technical Requirements

To enable effective delivery of the Microsoft Purview Information Governance and Records Management Advisory, the customer is expected to provide:

- Access to relevant Microsoft 365 and Microsoft Purview administrative portals, read-only where possible, appropriate to the agreed scope.
- Availability of configuration exports, reports, or screenshots where direct portal access is not permitted.
- Existing documentation relating to:
 - Information governance and records management policies.
 - Data classification and retention models.
 - Microsoft Purview configuration (e.g. sensitivity labels, retention labels, DLP policies, records management settings).
 - Identity, access control, and sharing governance where relevant.
- High-level information on content locations in scope (e.g. SharePoint Online, OneDrive, Microsoft Teams, Exchange Online).

Where documentation or access is limited, CGI will document assumptions and tailor recommendations accordingly.

8.2. Access Principles

- CGI does not require privileged, persistent, or administrative access to customer systems.
- Read-only access or exported configuration information is preferred and agreed in advance.
- No changes are made to live systems as part of this advisory unless explicitly agreed under a separate contract.

8.3. Collaboration and Delivery

- The service is delivered remotely using agreed collaboration tools (for example, Microsoft Teams).
- Workshops, interviews, and review sessions are conducted with nominated customer stakeholders.
- Secure document sharing is used for exchange of advisory artefacts and supporting evidence.

8.4. Constraints and Assumptions

- Advice is based on the customer's existing Microsoft 365 licensing, feature availability, and tenant configuration.
- CGI does not enable, configure, modify, or validate Microsoft Purview features as part of this service.
- CGI does not perform operational testing, records remediation, or policy enforcement activities.
- Responsibility for system configuration, data governance decisions, and operational execution remains with the customer.

This approach ensures the service can be delivered efficiently while maintaining clear separation between advisory guidance and operational responsibility, in line with G-Cloud requirements.

9. Outage and maintenance management

This advisory service does not involve the operation, maintenance, or management of customer systems, platforms, or services.

CGI does not manage outages, incidents, or maintenance activities for Microsoft 365, Microsoft Purview, or any related workloads as part of this engagement. Responsibility for system availability, incident management, and maintenance remains with the customer and their platform providers, including Microsoft.

As this is an advisory service:

- CGI does not introduce changes to the live Microsoft 365 or Microsoft Purview environment.
- CGI does not require planned maintenance windows.
- CGI does not provide incident response, break-fix support, or operational remediation.

Where relevant to the agreed scope, CGI may consider outage and maintenance arrangements at a high level when advising on governance, operating models, or records management responsibilities. Any such consideration is limited to:

- Clarifying ownership and accountability for information governance controls.
- Highlighting dependencies between governance processes and platform availability.
- Identifying risks or assumptions that may affect records management or compliance.

This guidance is provided for planning and governance purposes only and does not include execution, validation, or operational support.

If an outage or maintenance activity affects the availability of customer systems during the engagement, CGI will work with the customer to reschedule workshops or review activities as required, without assuming responsibility for the underlying issue.

10. Hosting options and locations

This advisory service does not provide hosting services and does not require the deployment of infrastructure, platforms, or environments by CGI.

All customer data, systems, and services reviewed as part of the engagement remain hosted within the customer's existing Microsoft 365 tenant and any associated customer-managed or third-party platforms.

Hosting locations are determined by the customer's Microsoft 365 configuration and contractual arrangements with Microsoft and other providers.

As part of this service:

- CGI does not host, operate, or manage Microsoft 365 or Microsoft Purview services.
- CGI does not introduce new hosting locations or migrate data.
- CGI does not store or process customer production data outside agreed collaboration tools.

Any documentation, analysis artefacts, or advisory outputs produced during the engagement are stored and handled in accordance with CGI's internal information security policies and the customer's requirements where agreed. These artefacts do not contain customer production data.

The service is delivered remotely and does not require access to or use of CGI-hosted environments. CGI consultants typically operate from the United Kingdom unless otherwise agreed.

11. Security

Security is a core consideration of the Microsoft Purview Information Governance and Records Management Advisory. The service is delivered in accordance with CGI's internal information security policies and applicable UK data protection legislation.

This is an advisory service. Security considerations relate to the protection of customer information accessed or produced during delivery of the advisory, rather than the operation, configuration, or security management of the customer's Microsoft 365 or Microsoft Purview environment.

11.1. Security Classification

- This service is suitable for use at:
- OFFICIAL.
- OFFICIAL-SENSITIVE (where the customer applies appropriate access controls and data-handling measures).

The service does not require access to, or handling of, information classified above OFFICIAL-SENSITIVE.

11.2. Data Handling and Protection

CGI applies strict data-handling and confidentiality controls throughout delivery of the service:

- CGI does not extract, copy, or store customer production data from Microsoft 365 or Microsoft Purview.
- Information reviewed during the engagement remains within the customer's Microsoft 365 tenant or within documentation explicitly provided by the customer.
- Where configuration insight is required, CGI uses read-only access or customer-supplied exports, reports, or screenshots wherever possible.
- Advisory outputs and working documents are stored and transmitted using CGI-approved secure systems.
- CGI does not retain customer data beyond the period required to deliver the service and removes access in line with internal retention and disposal policies.
- No customer data is transferred outside the United Kingdom unless explicitly agreed with the customer.

The customer remains responsible for the security, configuration, and operational management of their Microsoft 365 tenant, including Microsoft Purview controls.

11.3. Security Activities Within the Service

As part of this advisory engagement, CGI may provide security-related advisory support, including:

- Review of information governance and records management controls from a security and assurance perspective.
- Advisory input into data classification, sensitivity labelling, retention, and records management alignment.
- Guidance on data loss prevention (DLP), insider risk, and compliance policy considerations as they relate to information governance.
- Support with inputs to Data Protection Impact Assessments (DPIAs), where relevant to Purview governance.
- Identification of governance, ownership, and accountability gaps affecting secure information management.

All security-related activities are advisory only. CGI does not implement, modify, test, or validate security controls as part of this service.

11.4. Security Standards and Frameworks

The service is delivered in alignment with recognised security and assurance standards and principles, including:

- ISO 27001 – Information Security Management.
- ISO 9001 – Quality Management.
- UK GDPR.
- NCSC Cloud Security Principles.
- UK public-sector information assurance expectations.
- G-Cloud 15 Information Assurance requirements.

The service supports customers in aligning Microsoft Purview Information Governance and Records Management capabilities with these standards but does not provide formal certification, accreditation, or assurance.

11.5. Security Responsibilities

For clarity:

- CGI provides advisory guidance only.
- CGI does not operate, monitor, or secure customer environments.
- CGI does not provide security operations, incident response, penetration testing, or compliance certification.
- Responsibility for security controls, monitoring, and compliance remains with the customer.

12. Service Pricing and Terms and Conditions

12.1. Pricing

Please refer to the G-Cloud 15 portal for the rates available.

12.2. Terms and Conditions

Please refer to the associated Terms and Conditions Document relevant for this Service including termination by the Buyer or Supplier.

13. Further information

For more information about this or any of our G-Cloud services, please contact us:

Phone: +44 0845 070 7765. Ask to speak to the G-Cloud team.

Email: uk.gen.ccsframeworks@cgi.com, including the following information:

1. The name of this service.
2. The name of your organisation.
3. Your name and contact details.
4. A brief description of your business situation.
5. Your preferred timescales for starting the work.

We will prepare a quotation for you. Once the quotation is agreed upon, we will issue you the necessary documentation (as required by the G-Cloud Framework) and ask you to provide us with a purchase order.

Once we have received your purchase order, the services will be configured to the requirements agreed with invoices issued to you for the services procured. On a monthly basis, we will also complete the mandated management information reports to Government Procurement.

PROPRIETARY AND CONFIDENTIAL

The information contained in this document is confidential to CGI and/or CGI group companies. This document shall not be reproduced in any form or by any mechanical or electronic means, including electronic archival systems, or submitted to a generative AI tool without the prior written approval of CGI. The receiving party may use this document and the information contained in it for the purpose of evaluating CGI's proposal only. Any personal data included in this document must not be replicated, stored or distributed beyond the immediate recipient or used for any purpose other than evaluating the document.

This proposal is subject to contract and shall not be binding unless and until execution by CGI and Contracting body of a final agreement to the proposal, containing the terms and conditions that will govern the relationship between the parties. Any final agreement is conditional (inter alia) upon due diligence and customary business investigations by CGI. The results of such due diligence and/or investigations may impact upon content of this proposal, including the business structure, business terms and financial arrangements.

If you have received this document by mistake, note that the reading, the reproduction or the distribution of this document is strictly forbidden. You are hereby requested to inform us by telephone at +44 0845 070 7765 and to return this document by special delivery marked for the attention of Simon Figg.

Except where indicated otherwise, all names, trademarks, logos and brands (registered or not) referred to in this document are the property of a company in the CGI group or its licensors.

The information in this proposal is submitted on 30 Jan 2026 - Issue 1.0 on behalf of CGI by the following authorised representative:

Simon Figg

Frameworks Manager

CGI IT UK Ltd

14th Floor, 20 Fenchurch Street, London, EC3M 3BY

Tel: +44 0845 070 7765

