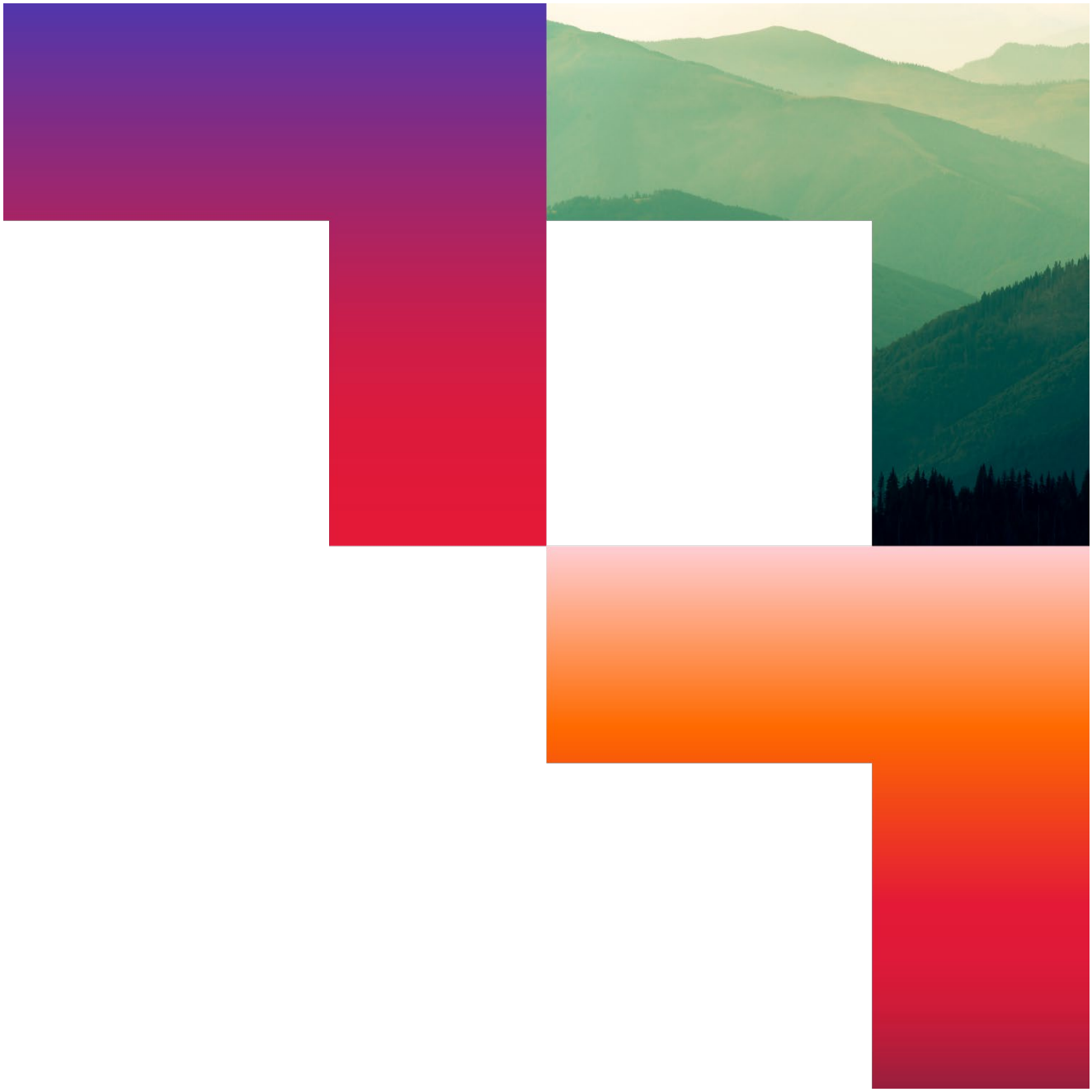


Insider Threat Advisory

Contracting Body

30 Jan 2026

Issue 1.0

Table of contents

Service Definition overview

Our Insider Threat Advisory Service enables organizations to proactively identify, investigate, and mitigate risks from malicious, negligent, or compromised insiders. By combining Microsoft Purview Insider Risk Management, SOC monitoring, structured playbooks, and deception techniques, we provide a holistic approach to insider threat defence.

We help organisations establish governance, integrate insider threat monitoring into the SOC, and deploy deceptive assets to deter malicious insiders and surface threats earlier—while maintaining compliance and employee privacy.

Why CGI?

For over 40 years, CGI has supported government and commercial organisations in delivering complex, high-assurance digital services and operating in highly regulated environments. This experience underpins CGI's approach to Responsible AI and AI governance, which combines strategic advisory capability with practical, audit-ready assurance.

CGI brings together in-house expertise across policy development, risk management, data, analytics, digital delivery, assurance and regulation to support the responsible adoption of AI. Our approach recognises that effective AI governance is not achieved through policy alone, but through clear accountability, proportionate controls and demonstrable evidence that risks are understood and managed in practice.

CGI has significant experience working with public sector organisations to establish governance frameworks, maturity models and assurance mechanisms that stand up to board scrutiny, audit and regulatory review. Our Responsible AI Consultancy and AI RMF service builds on this background by providing an end-to-end offering that supports organisations from initial AI strategy and use case identification through to ongoing assurance, maturity assessment and regulatory readiness.

1. Service Description

Our Insider Threat Advisory Service enables organizations to proactively identify, investigate, and mitigate risks from malicious, negligent, or compromised insiders. By combining Microsoft Purview Insider Risk Management, SOC monitoring, structured playbooks, and deception techniques, we provide a holistic approach to insider threat defence.

We help organisations establish governance, integrate insider threat monitoring into the SOC, and deploy deceptive assets to deter malicious insiders and surface threats earlier—while maintaining compliance and employee privacy.

Key Objectives

- Establish Insider Threat Program – policies, governance, and roles aligned with business and compliance needs.
- Deploy Microsoft Purview – configure Insider Risk Management to detect data leaks, misuse, and risky behaviours.
- Operationalize Insider Threat Playbooks – guide SOC analysts through standardized investigation and response workflows.
- Enhance SOC Monitoring & Automation – integrate insider risk alerts with SIEM/SOAR for continuous monitoring and enrichment.
- Implement Deception Techniques – deploy decoy data, credentials, and systems to detect and deter malicious insiders.
- Align with Legal & HR Requirements – ensure monitoring is ethical, defensible, and compliant.

Our Approach

Phase	Activities
Assessment & Framework	Review current insider threat capabilities, policies, and SOC integration. Define governance model.
Microsoft Purview Enablement	Configure insider risk policies (IP theft, data exfiltration, policy violations). Tune detection thresholds and enable case management.
Playbook Development	Build scenario-driven playbooks, e.g.: – Data exfiltration via email/USB – Privileged user abuse – Anomalous system access – Departing employee activity
SOC Monitoring Integration	Feed Purview alerts into SIEM/SOAR, enrich with user context, and build dashboards for insider activity monitoring.
Deception Deployment	Implement deceptive controls such as: – Honeyfiles (fake sensitive documents) – Honeytokens (decoy credentials/identities) – Deceptive shares or systems monitored by the SOC – Canary alerts to detect attempts at unauthorized access
Validation & Exercises	Conduct red team/insider threat simulation exercises to validate playbooks, SOC readiness, and deception coverage.
Roadmap & Advisory	Provide a maturity roadmap for evolving insider threat defenses over time.

Deliverables

- Insider Threat Program Framework – governance, escalation paths, legal/HR integration.
- Microsoft Purview Configuration Guide – optimised insider risk detection policies.

- SOC Playbooks – standardized response workflows for key insider scenarios.
- Deception Layer Design – blueprint and deployment of honeyfiles, tokens, and canaries.
- SOC Integration Guide – SIEM/SOAR playbooks for Purview and deception alerts.
- Gap Analysis & Maturity Roadmap – prioritised improvement plan.
- Executive Briefing Pack – board-level reporting on insider threat posture.

Benefits to Clients

- Earlier Detection of Insider Activity – deception surfaces malicious activity before it escalates into damage.
- Actionable Playbooks – SOC analysts gain repeatable, scenario-based workflows for faster resolution.
- Maximized Microsoft Investment – unlock value from Microsoft Purview by aligning it with SOC operations.
- Comprehensive SOC Coverage – insider alerts integrated with SIEM/SOAR improve detection and response efficiency.
- Proactive Deterrence – deception increases the risk of discovery for malicious insiders, discouraging harmful actions.
- Regulatory & Legal Assurance – align insider monitoring with compliance requirements while protecting employee privacy.
- Reduced Risk & Impact – faster detection, clearer workflows, and proactive deterrence reduce financial, reputational, and regulatory damage.

2. Service Pricing and Terms and Conditions

2.1. Pricing

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

2.2. Terms and Conditions

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

3. 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:

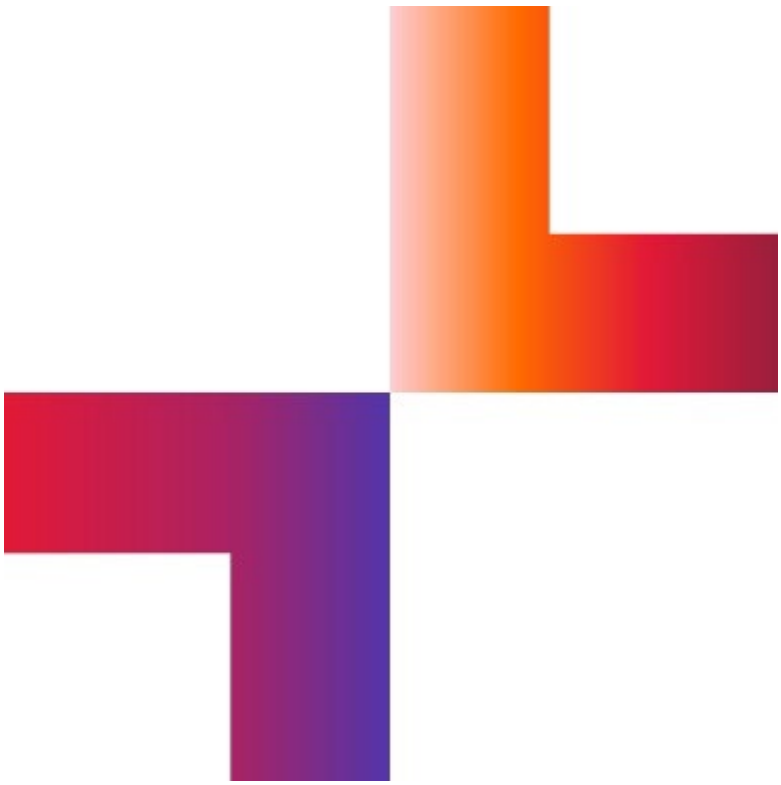
Simon Figg

Frameworks Manager

CGI IT UK Ltd

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

Tel: +44 0845 070 7765



cgi.com/uk