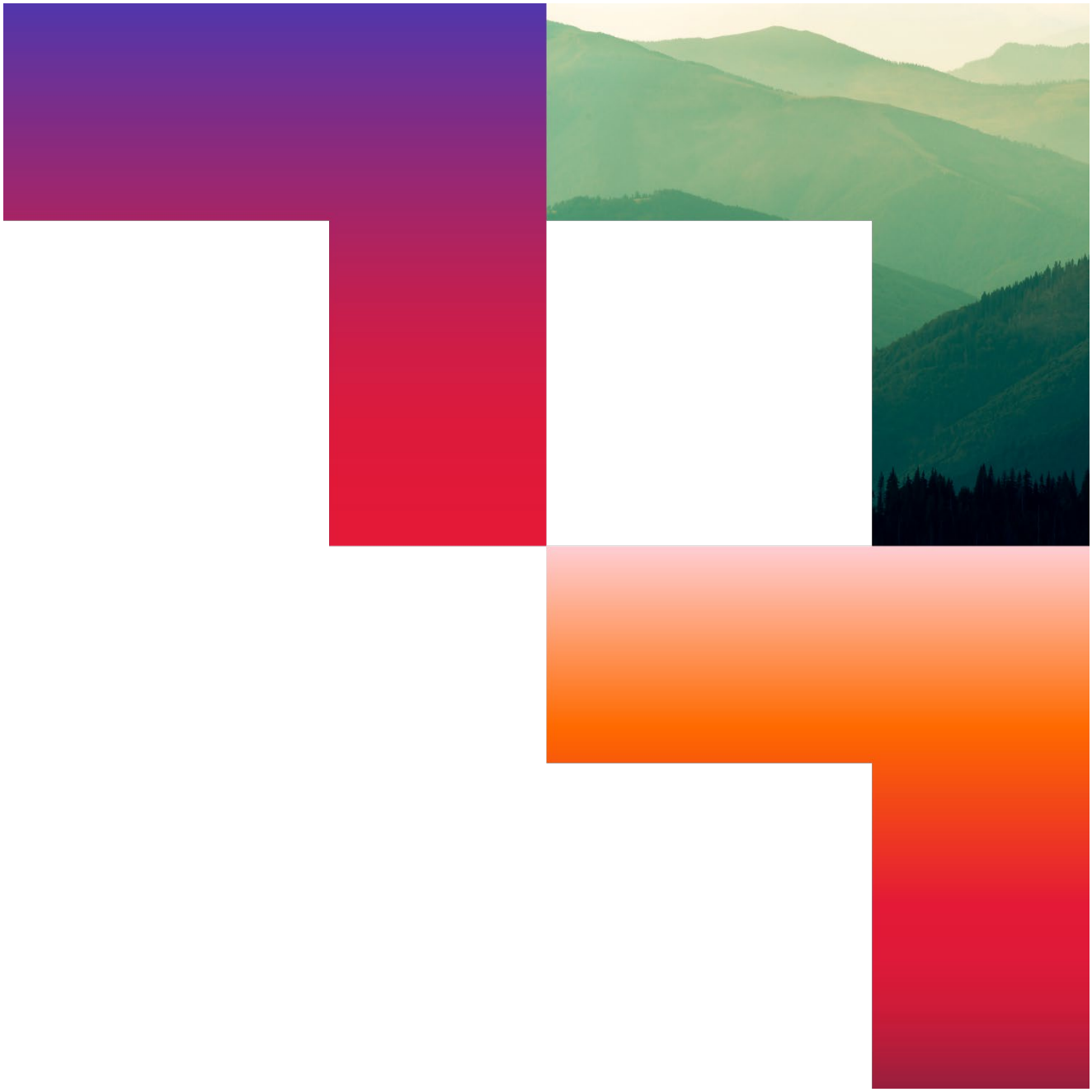


Industrial Control Systems (ICS) - Operational Technology (OT) Penetration Testing

Contracting body

07 May 2024

Issue 1.0

Table of contents

Service Definition overview

CGI provides a thorough, objective, and independent ICS testing service that has the flexibility to test a wide range of ICS components safely. We work alongside our clients to agree upon which methodologies and services most suit their environment.

Why CGI?

CGI have significant experience in the ICS/OT, specifically in Energy & Utilities, as well as Maritime Platforms. Additionally, the CGI UK Penetration Testing Team have built and maintain ICS demonstrators for both Allen-Bradley and Siemens equipment, which we are able to use to provide real-time demonstrations for tools and techniques used to assess, as well as the consequences of an attack.

For over 45 years, CGI has helped secure government and commercial clients and delivered some of the most complex technology projects and services. CGI's Cyber Security has significant in-house expertise in delivering penetration testing, red and blue team services for a wide variety of organisations, ranging from highly sensitive government organisations, through regulated industries, to large commercial enterprises and technology-oriented entrepreneurial businesses.

We have over 260 qualified cyber experts in our Cyber Consultants practice. In Cyber, we maintain a depth of employee experience, ranging from Cyber graduates, to CISOs with over 20 years' experience within Cyber Security.

Our Cyber Managed Services host a number of specialist teams, including Cyber Threat Intelligence (CTI), Phishing and Digital Forensic and Crest accredited Incident Response (DFIR) and Penetration Testing Teams, all of which are 100% UK-based, SC and DV cleared.

- We have experienced consultants holding SANS Global Industrial Cyber Security Professional certification (GICSP). We maintain and evolve our understanding through specialist in-house and external training.
- A CREST approved accredited member company for penetration testing, we have qualified staff performing OWASP and OSSTMM security testing, as well as targeted engagements on the MITRE framework.
- CGI is an NCSC approved green-light CHECK company offering penetration testing of IT systems to identify potential vulnerabilities and recommend effective security countermeasures.
- Accredited List X - UK Government site security scheme for suppliers required to hold sensitive information.

Figure 1 - CGI's CHECK and CREST accreditations

1. Service Description

Mechanical and heavy industry organizations in the UK manage and uphold intricate and vital infrastructure through Operational Technology (OT), serving various sectors in both public and private domains. In this fast-evolving sector, operating efficiently, effectively, and safely is paramount. The deployment and oversight of Industrial Control Systems (ICS) ensure continuous monitoring and adjustments for seamless and secure operations. However, weak environmental designs, along with several protocols and procedures within ICS, often exhibit vulnerabilities due to inadequate configurations and insufficient testing to verify proper implementation or suitability for their intended purposes. Frequently, equipment that is known to be insecure is inadvertently connected to wider organisational networks, significantly increasing the risk to ICS components. It is also recognised that ICS equipment does not prioritise security, which can lead to multiple inherent vulnerabilities. This can leave the organisation open to safety breaches, regulatory fines, financial and reputational damage or theft of business-critical information or intellectual property.

The sensitivity and critical importance of Industrial Control Systems, combined with inadequate attention to security, make them prime targets for malicious actors aiming to seize control and inflict disruptions or physical damage. It's a common occurrence for equipment initially considered insecure, even when isolated within a network, to inadvertently integrate into broader organizational networks, greatly amplifying the risk to ICS components. Additionally, the insufficient prioritisation of security in ICS equipment can lead to multiple vulnerabilities, leaving organizations vulnerable to safety breaches, regulatory penalties, financial and reputational losses, or the theft of crucial business information and intellectual property.

CGI understands the significance of giving priority to safety while also staying flexible to embrace new systems, technologies, and methodologies for improved competitiveness and efficiency. Our penetration testing service assesses the existing configuration of the OT network design and examines insider and outsider threats customized to the particular implementation and usage scenario of each system, ranging from Purdue level 0 to level 5.

Our approach to testing industrial control systems provides a thorough, objective, independent service whilst allowing the flexibility necessary to test a wide range of IT systems safely. Our primary objectives for all security testing that we carry out are:

- To evaluate whether or not specific weaknesses in security leave the organisation open to attack.
- Ensure the safety systems implemented cannot be bypassed maliciously.
- To provide clear recommendations for vulnerability mitigation that are simple to implement and tailored to the required functionality of the system under test.
- To help increase our client’s confidence in the security of their systems.

2. Service Delivery and Approach

CGI follow a defined process for service delivery and to determine the testing approach, including the scope, associated pre-requisites, objectives (whether defined by CGI, or you as the client) and the methodologies in use. Upon receiving your requirements, a senior tester experienced in ICS testing will collaborate with your project team to understand the context of the engagement (i.e., the purpose of the system, outward/inward connections) as well as the operational state of the system (i.e., live, test-bench) to recommend a scope that can be executed safely while meeting the primary security concerns conveyed to us by your requirements.

Scoping and proposals are completed by qualified penetration testers using a set of non-prescriptive scoping metrics defined over hundreds of engagements, ensuring that the appropriate amount of time, and skilled resources are deployed for engagements. Each of CGI's documents also goes through an in-depth internal Quality Assurance (QA) process before release, which probes into every part of the proposed engagement, ensuring that CGI fully understand the system in scope.

A flow-chart of the initial engagement process has been included for reference.

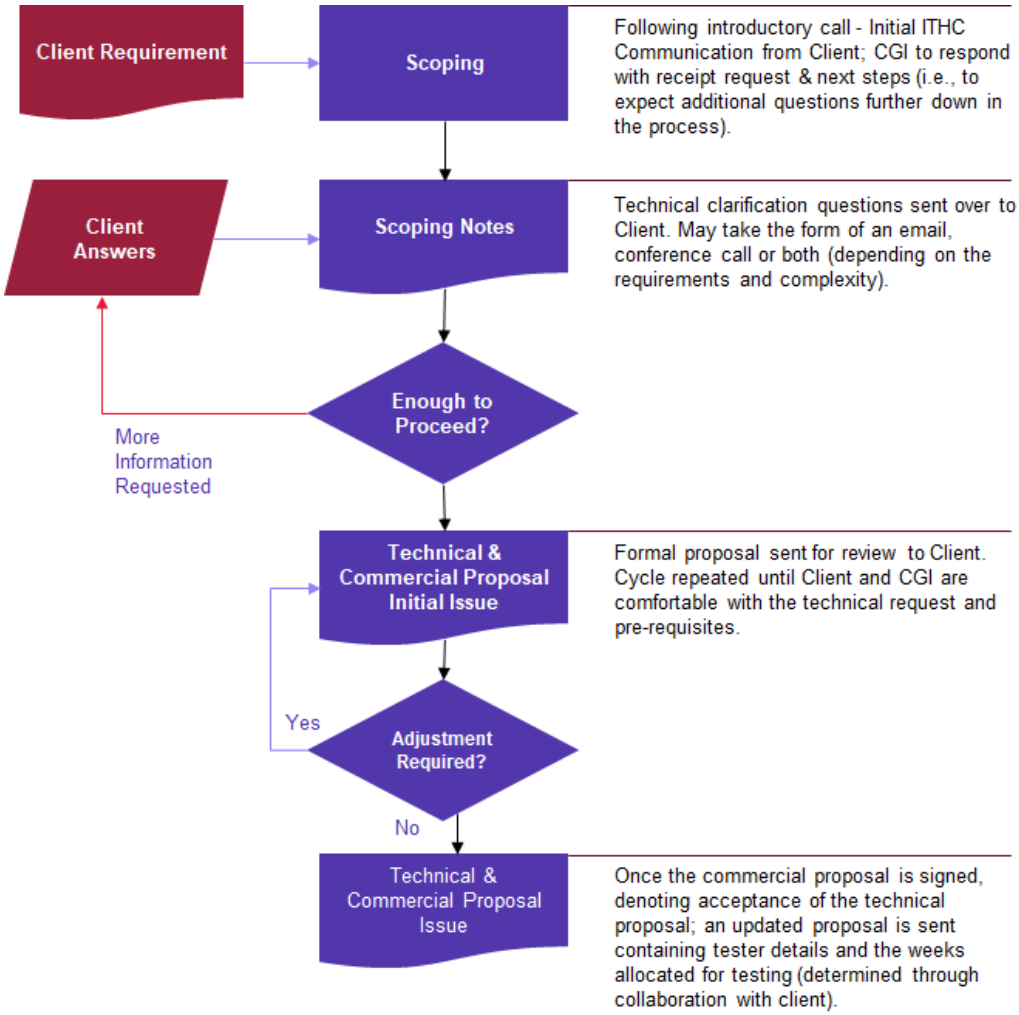


Figure 2 - Penetration Testing Engagement Process

The scope of experience and capabilities of assessing Operational Technology and Industrial control systems within production, supervision and corporate networks includes but is not limited to:

- Industrial Control System Design
- Safety Instrumented Systems (SIS)
- Network Segregation
- Authentication, Authorisation and Accounting functions (AAA)
- Software Defined Networks (SDN)
- Programmable Logic Controllers (PLC)
- Data Historians
- Human-Machine Interface (HMI)
- Remote Terminal Units (RTU)
- Supervisory Control and Data Acquisition (SCADA) and Distributed Control System (DCS) systems
- ICS specific and proprietary protocols.

2.1. Information Assurance

CGI uses our Management Foundation including our Integrated Management System (IMS) for information assurance. These IMS processes are independently certified to BS/EN/ISO 9001:2008.

CGI is committed to retaining our current range of UK-based certifications and will extend these to meet client expectations as required.

The CGI Management Foundation design allows incorporation of best practice from across all our Public Sector and Commercial engagements.

Our accreditations and certifications include:

- Cyber Essentials Plus
- ISO9001, ISO27001:2018, ISO22301:2019, ISO45001:2018, ISO14001, ISO27701:2019
- CREST Penetration Testing
- NCSC CHECK approved
- SANS Global Industrial Cyber Security Professional certification (GICSP).

All information is handled at the appropriate security level for this service.

3. Onboarding and Offboarding

3.1. Onboarding

CGI has proven and effective on and off boarding skills, tools and methodologies. CGI will engage directly with the client to ensure the full scope of the requirements is understood and agreed in advance of any engagement. We will work with senior stakeholders to define the necessary business outcomes and ensure the services are aligned accordingly.

For all services CGI, understands the client's requirements and makes on-boarding specific to these needs.

3.2. Offboarding

Off-boarding is instigated by a client request or after expiration of the service agreement. Deletion of data will occur in line with the service agreement. Any required data will be made available using appropriate media, in line with the data security classification.

3.2.1. Access to data upon exit

CGI retains data pertinent to the penetration test for a maximum of three months. After this time, test data will be destroyed. This does not include the final report, which will be securely stored in accordance with NCSC guidelines.

4. Service constraints

Our testing is designed to be non-disruptive, and, at most, users and clients experience a very minor degradation in standard service. If, however, it is perceived that some specific tests may cause instability, then this will be discussed with the point of contact before proceeding with those tests.

It is best practice to ensure that full system backups have been made in the event of unforeseen circumstances. By its nature, penetration testing can never be guaranteed to be entirely non-detrimental, however, the CGI UK Penetration Testing Team will use reasonable endeavours to ensure that any risk of system failure is mitigated.

Restoring the system to its pre-test state is the responsibility of the system owner, although we will remove items that were intentionally created during testing wherever possible and inform the point of contact where this has not been possible.

During testing, a large number of network connections are usually created. Similarly, when fuzzing parameters in a web application, many HTTP requests will be generated. These activities are bound to create a number of logs or events on system hosts and can cause Intrusion Detection or Prevention Systems to generate alerts. Where security incidents are identified, the CGI UK Penetration Testing Team will strive to make their testing logs and data output available to both the client security team and any investigative partners engaged by them.

The CGI UK Penetration Testing Teams standard working hours are 09:00-17:30. If alternative hours are required, please notify the team as soon as possible to arrange this.

5. Service levels

The overall accountability for the relationship with the client lies with CGI's Executive Sponsor and CGI Account Manager and they provide strategic governance to the service working closely with the client's Senior Executive team. The purpose of this team is to ensure that the relationship is healthy, the service is delivering, the governance model is working, and best practice is being applied.

6. Hosting options and locations

CGI has a network of 21 offices across the United Kingdom and Northern Ireland, with our UK members having the capability to deliver as hybrid-workers. Through our engagements we also understand that for some clients it is essential that our members are physically present on their sites, our distributed network of offices makes this possible. Whatever your requirements are the options for hosting and locations will be agreed at contract negotiations.

7. Security

CGI has invested significant resources to develop an Enterprise Security Management Framework (ESMF) based on recognized industry standards and applicable regulations or legislation such as ISO 27001, ISO27701, NIST, COBIT, CIS, CCPA and GDPR to name but a few. This framework is used across the global organization to protect information assets, technologies, facilities, and CGI members, including the data managed across the business, and is supported by CGI's security and privacy policies, standards and controls (Security Baseline) which are implemented through our processes, practices, services, solutions and our interactions with any third parties working on behalf of CGI.

Across the CGI business, the technical and organizational measures are defined using a risk-based approach. This considers the nature, scope, context and purposes of processing as well as the risk to the rights and freedoms of natural persons, where CGI is acting as either the data controller or data processor. This ensures a level of security and privacy appropriate to the risk, in situations where CGI holds responsibility and accountability for personal data processing.

CGI's ESMF Security Baseline is the minimum-security standard for all CGI offerings (including cloud-based services) to be applied by both CGI and clients. In some cases, CGI Security or Data Privacy may wish to add additional controls e.g. where sensitive personal data is involved. Where CGI or our clients agree to strengthen the level of security or privacy to consider specific requirements (risks, regulatory requirements, etc.) these additional security or protective measures will be defined within the CGI contracted services, particularly where CGI may be acting as data processor on behalf of a client.

8. Service Pricing and Terms and Conditions

8.1. Pricing

Please refer to the associated Pricing Document relevant for this Service.

8.2. Terms and Conditions

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

9. 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 Chris Sims.

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 07 May 2024 - Issue 1.0 on behalf of CGI by the following authorised representative:

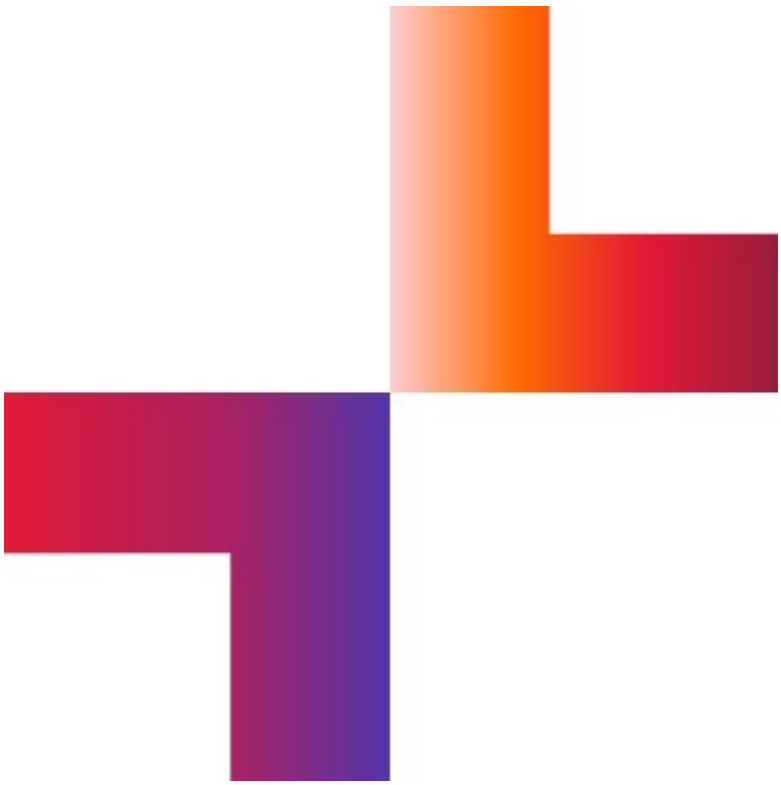
Chris Sims

Frameworks Director

CGI IT UK Ltd

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

Tel: +44 0845 070 7765



cgi.com/uk