



Cyber Security Education Awareness and Training

Contracting body

30 Jan 2026

Issue 1.0

© 2026 CGI IT UK Ltd

CGI

Table of contents

1.	Service Description	4
1.1.	Delivery Approach	4
2.	Service Constraints	4
3.	Technical Requirements	4
4.	Hosting Options and Locations	5
5.	Security	5
6.	Service Pricing and Terms and Conditions	5
6.1.	Pricing	5
6.2.	Terms and Conditions	5
7.	Further information	5
PROPRIETARY AND CONFIDENTIAL		7

Service Definition Overview

We are all aware of the growing threat from cyber-attacks to our organisations, but are you aware that the biggest cause may be us, human beings? Threat studies consistently show each year that an organisation's employees are the most prevalent cause of data breaches by malicious or accidental actions.

Threat actors are taking advantage of human behaviour launching planned social engineering attacks (such as phishing) to opportunistic attempts to exploit carelessness, particularly in terms of unsecured devices. Increasingly complex and technical landscapes allow more threats vectors to be used, preying on the adoption of new technologies and services that organisations are rapidly embracing, exploiting the human trust and the potential for errors.

CGI offers a range of Cyber Security Education, Awareness and Training Services which are designed specifically to increase the level of threat awareness through an organisation and thus drive down the chances of an attack being successful.

Our Cyber Awareness education, awareness and training capability is a good foundation to cyber security for all employees in your organisation and gives practical advice on how to 'Operate with Confidence'.

Why CGI?

For over 40 years, CGI has helped secure government and commercial clients and delivered some of the most complex technology projects and services.

Most of us depend on the internet to do our jobs and we may become forgetful about the security implications of the information we store and use every day.

But what if it gets into the wrong hands? Would the organisation be seriously compromised if the data we rely on got into the public domain?

With so many systems and connected devices we use every day, both in our working and private lives, how do we ensure we keep our key information safe?

Consideration of the security implications of our customer's information is at the core of everything CGI does.

CGI has over 250 experienced cyber security professionals in the UK. These professionals are continuously involved in the full spectrum of cyber security activities, across the IT operations of diverse customers, who are using numerous technologies for a wide range of business goals. This includes customers with varied cloud deployment contexts.

Additionally, at CGI, our cyber security teams work in an integrated way with our other technical disciplines, and in close collaboration with our client's own business teams, providing an understanding of cyber security challenges from the non-cyber perspective to the life cycle of IT system delivery and support.

This allows for a deep and current understanding of the key aspects of cyber risk management across numerous operating scenarios, the technology and business challenges posed, and the human and business factors essential to achieving cyber security.

As a result, our collective understanding of threats, vulnerabilities and risks to businesses operating in the cloud, is second none. Drawing on this body of understanding, we deliver realistic and practical security awareness and training, that will be of relevance to all participants, from any organisational background.

1. Service Description

CGI can provide a security awareness package delivered in house for one day, for up to eight employees. While this is introductory training, the focus is upon building individual understanding of the cyber risks posed and best practices required, to a level where it can be understood and relating this to their own organisation's cloud context.

A narrative and interactive approach is taken throughout this cyber security journey, with participants being guided through core aspects they need to be aware of, backed up with real-life scenarios to illustrate these, followed by the group being asked to consider and share their own related circumstances. The training will use this format to build the cyber security narrative and understanding of what practices are essential, and why.

1.1. Delivery Approach

Prior to the delivery the CGI presenter will contact an organisational representative to discuss logistical requirements for the day, to ensure the event runs smoothly, and participants get the most enjoyable and beneficial learning experience. They will also discuss the capture and later communication of collaborative output from the training.

The training is entirely face-to-face classroom style and will be delivered as a narrative sequence of topics, gradually building a holistic understanding of cyber security awareness. Each topic will be addressed in the following way with the participants:

Bulleted topical presentation > multimedia case study > collaborative discussion.

The topics covered are as follows:

- The general cyber security vulnerabilities that organisations face, how such exposures extend to the cloud context, and what additional specific-to-cloud issues there are.
- The nature of the threats exploiting these vulnerabilities; threat objectives and how they achieve these.
- The resulting effect of deliberate and non-deliberate cyber security compromises and long-term impacts.
- Consideration of what constrains threats, reduces impacts and achieves cyber security goals.
- Consideration of what actions can be taken as an individual to help achieve cyber security goals.
- The challenges organisations face to maintain these practices, and how that may be tackled.

The trainer will guide the group to consider how the material discussed relates to their organisational context and capture this situational cyber security realisation on the white boards/flip charts throughout the day. Participants will be advised to keep this discussion at a high level and avoid details that may be confidential. The trainer will ensure discussion remains theme relevant and appropriate. As well as an opportunity to clarify their understanding of the course context, the collaborative discussion and capture will ensure that the course material becomes relatable to the participants organisational context and role.

Following the completion of training courses, we will send out surveys to elicit feedback from all attendees. The final step is to collate the responses to the survey and conduct a reporting session with your senior managers.

2. Service Constraints

The training will be delivered at your organisation premises. A classroom or meeting room suitable for 8 persons will be required, along with a suitably large display screen (and projector if necessary), to present course material from the presenter's laptop.

Flipboards & white boards will also be required to capture collaborative input throughout the day. Participants will only need to bring writing materials for any notes they wish to take.

3. Technical Requirements

A projector with HDMI port.

4. Hosting Options and Locations

All training will be delivered on client premises.

5. Security

CGI has invested significant resources to develop an Enterprise Security Management Framework (ESMF) based on recognised 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 organisation 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 organisational 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.

6. Service Pricing and Terms and Conditions

6.1. Pricing

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

6.2. Terms and Conditions

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

7. 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.

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

- | | |
|---|--|
| 4. A brief description of your business situation. | mandated management information reports to |
| 5. Your preferred timescales for starting the work. | 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

