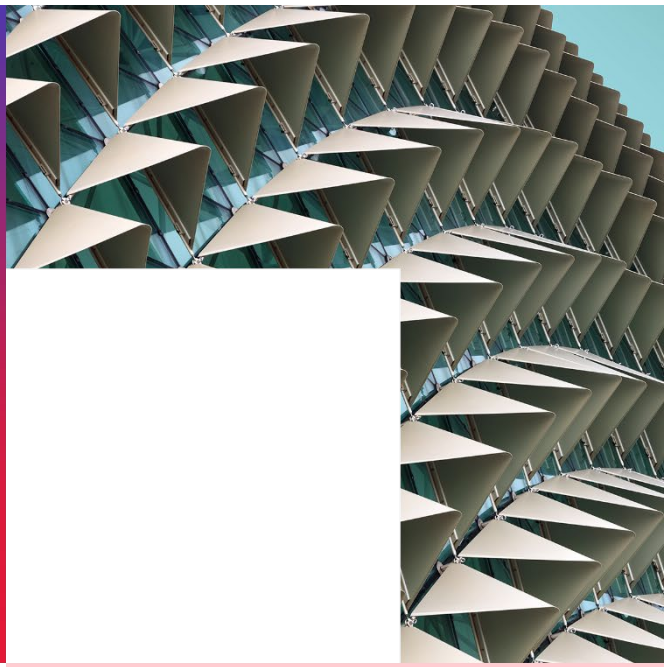


BCR C – CGI – Appendix C CGI Data Privacy Internal Audit Process

1. INTRODUCTION

CGI's BCR-C and the commitment of CGI Entities to comply with the BCR-C demonstrate that CGI intends to provide a high level of protection for the Personal Data it Processes.

The BCR-C defines a set of principles and requirements that apply to CGI's Processing of Personal Data. It is CGI's responsibility to ensure that these principles and requirements are implemented within the organization and, in particular, to verify that CGI Entities commit to complying and actually comply with the requirements.

In this context, this document defines how CGI audits its Processing of Personal Data to assess compliance with the BCR-C. Please note that definitions for specific terms used in this document can be found in the BCR-C.

2. PURPOSE

This document covers audits conducted by CGI for CGI Entities regarding their Processing of Personal Data. It does not apply to audits that CGI may conduct for third parties or to audits that are performed by third parties for CGI.

The purpose of privacy audits is to provide CGI with an understanding of the practices employed by CGI Entities when Processing Personal Data and their adherence to CGI's BCR-C.

Where a privacy audit demonstrates that one or several entities do not comply with the BCR-C, remedial measures will be identified and an action plan will be adopted.

3. SCOPE

A. WHAT CAN BE AUDITED?

CGI audits the Processing of Personal Data relating to CGI Partners, its agency staff, sub-contractors, suppliers, and clients.

The following areas may be considered as part of the scope of a privacy audit:

i. Governance structure

- Roles and responsibilities
- Policies and standards
- Derogations/exceptions to the BCR-C, as per applicable local law
- Enterprise security/privacy risk assessments
- Training and awareness
- Compliance with client and third-party contractual agreements
- New privacy laws and regulations monitoring

ii. Personal data management

- Personal Data holdings (Processed, accessed, transferred, hosted) and inventory records
- Records of the transfer mechanism used for cross-border data flows
- Legal and physical mechanisms for data transfer
- Lawfulness of the Processing purposes
- Legal basis for the Processing (including alignment with all Processing purposes)
- Data protection/privacy impact assessments
- Data retention requirements

iii. Embedding of data privacy into the operations

- Privacy obligations (e.g., privacy by design) and rights (e.g., response to privacy requests and complaints)
- Proportionality of Personal Data Processed
- Application of data retention requirements
- Transparency and information provided to Data Subjects
- Data subject consent management
- Logical and physical security measures in place for the protection of the data at rest/in transit
- Privacy breach response and reporting
- Self-assessments of privacy compliance

Privacy audits can be targeted locally, at the corporate level or by function. The appropriate target must be determined before the audit begins and must be expressly defined in the scope memorandum as described below.

Privacy audits will be performed by qualified CGI auditors who are supported by subject matter experts as required.

Privacy audits may be conducted in the following ways:

- **Unscheduled audits**: Cover certain points of compliance and for a limited geographical scope

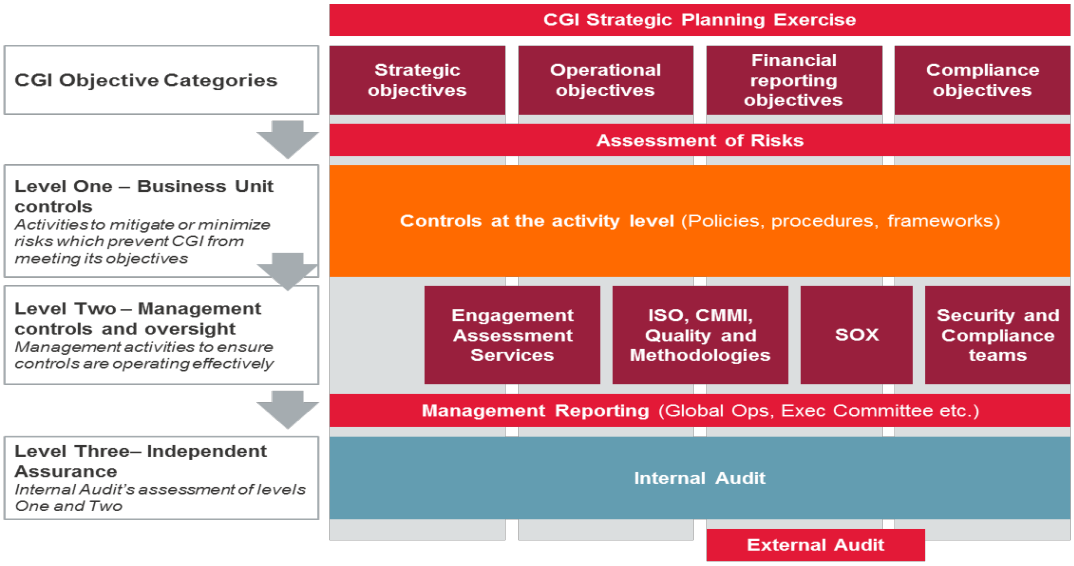
- **Scheduled audits**: Cover general compliance with the BCR-C based on the following:
  - Limited geographies and/or entities and/or functions
  - Client contract(s)

B. WHO CAN LAUNCH THE AUDIT?

Privacy audits can be initiated as follows:

- As unscheduled audits by CGI Privacy Team for specific Processing or for the deployment of the Data Privacy Program
- By Internal Audit and Enterprise Risks for the governance of and compliance with the BCR-C and the Data Privacy Program
- As part of CGI's Quality System Management and the Client Partnership Management Framework (CPMF)
- At the request of executive management (e.g., following an incident of concern)
- For a client or a Supervisory Authority to meet the requirements of an external body

The following diagram defines CGI's three lines of defense:



The Business Unit or Corporate Services leader must take management responsibility to facilitate the audit and ensure that issues are addressed in a timely fashion.

C. FREQUENCY

Privacy audits will be launched as follows:

- At least once a year for scheduled privacy audits that cover general compliance for limited geographies, entities and/or functions
- At least every two years for scheduled global privacy audits that cover general compliance with the BCR-C
- As scheduled engagement compliance audits aligned with the sampling requirements specified in the Quality System Management Manual

Privacy audits also may be launched as follows:

- As unscheduled audits with a specific focus as determined by the Chief Privacy Officer
- When a complaint is received from a Data Subject
- During the launch of a new project

Where possible, privacy audits will be combined with security and quality audits. Audit teams will share their annual plans to optimize coverage and value.

D. WHAT INFORMATION AND PROCESSES CAN BE AUDITED?

Auditors must have access to all documentation and systems necessary to perform the audit. They also must be able to conduct interviews with the auditees, as reasonably required, and may perform unscheduled floor inspections.

The following evidence may, among other things, be audited:

- Privacy and data protection related policies, standards and procedures
- Derogations/exceptions from the BCR-C
- Privacy notices
- Inter-BU agreements
- Data inventory
- Data transfers agreements
- Client contractual agreements/requirements
- Physical and logical security measures in place to protect Personal Data

The audit team may visit key departments and sites relevant to the scope of the privacy audit.

E. METHODOLOGY

When privacy audits are performed by established CGI teams, such as Internal Audit, the team's methodology will apply. However, CGI Privacy Team will in such cases:

- Receive notice of impending privacy audits
- Receive draft reports with the opportunity to review and comment
- Receive copies of final audit reports
- Monitor and validate closure of audit defects relating to compliance with the BCR-C

The following sub-sections describe the recommended approach for conducting a privacy audit.

F. AUDIT NOTIFICATION

When CGI decides to launch a privacy audit, the following information must be documented and communicated prior to the audit's launch. This notification should contain, but not be limited to, the following:

- Scope and objectives of the audit (material and geographical)
- Functions and roles to be interviewed
- When, where and by whom details
- Duration of the audit
- Documentation, computerized systems and/or processes to be reviewed

Unless otherwise decided by CGI Privacy Team for specific Processing, the scope memorandum must be communicated to the auditees and appropriate leadership before the privacy audit begins and, at the latest, at the beginning of the first interview. No minimum notice period is mandated.

G. AUDIT FIELD WORK

During the audit field work, the audit team must collect sufficient information to draw relevant conclusions in accordance with the processes applied by the auditing team's function and, among other things, through the sampling of evidence and interviews. No minimum/maximum sample size is mandated. However, sampling as per the Quality System Management Manual Appendix A may be taken as a guide. The team must endeavor to minimize the impact on day-to-day business operations.

The audit can take the following forms:

- Questionnaire
- Documentation/computerized systems review
- Floor inspection
- Interview
- A combination of the above

Sample questions are provided in Appendix 1 to illustrate the type of questions asked as part of a privacy audit.

H. AUDIT CONCLUSION

Based on observations and the information collected, an audit report must be drafted. The report must include, but not be limited to, the following:

- Objective and scope of the audit
- Documents, processes, computerized systems reviewed and/or persons interviewed
- Description of the Processing and/or procedures audited
- Summary of the level of compliance of the processes and/or computerized systems audited
- Root causes for non-compliance and recommendations
- Agreed upon action plans to remediate the observations of non-compliance
- Action plan owners and target implementation dates

Each draft audit report, irrespective of the scope of the audit, shall be reviewed by a Data Protection Officer who will validate the proposed remediation measures and timelines.

Once the report, defects and remedial actions are agreed upon with the auditees, the final audit report must be distributed to the following:

- Business unit or Corporate Services leader(s)
- Process/system owners
- Chief Privacy Officer
- "Action owners"
- Local data protection officer(s)

In the event of a lack of agreement on the findings and/or actions resulting from the audit, the Chief Privacy Officer will be the final arbiter.

I. ACTION PLAN FOLLOW-UP AND ESCALATION

With the remedial measures and timelines defined, following confirmation from the "action owners" that the actions are completed, the audit function must verify that the measures are effectively implemented.

A status report must be produced, at minimum, halfway between the beginning of the remediation plan and the scheduled end of implementation in order to monitor the progress of the remediation measures. If insufficient progress is made or target dates are likely to be missed, this shall be brought to the attention of Senior Management (BU leader) and the Chief Privacy Officer who shall determine measures to address any issues.

If deemed necessary, the Chief Privacy Officer may escalate the issue to the SBU President and the Executive Vice-President, Legal and Economic Affairs, and Corporate Secretary.

J. COMMUNICATION

All requests regarding this process should be addressed to privacy@cgi.com.

K. REFERENCES

DOCUMENT	LOCATION/OWNER
BCR-C	Corporate Legal Services – Chief Privacy Officer
Quality System Management Manual Appendix A	Enterprise Audit
Client Partnership Management Framework (CPMF)	CGI Management Foundation

L. REVISION HISTORY

VERSION	DATE	DESCRIPTION
1.0		Initial release
1.1	01.2020	Review – No Changes
1.2	03.2021	Title change Chief Data Protection Officer to Chief Privacy Officer
1.3	11-2022	Annual Review – No changes applied
1.4	03-2025	Annual Review – minor textual changes; update of the contact email
1.5	06-2026	Annual review – No changes

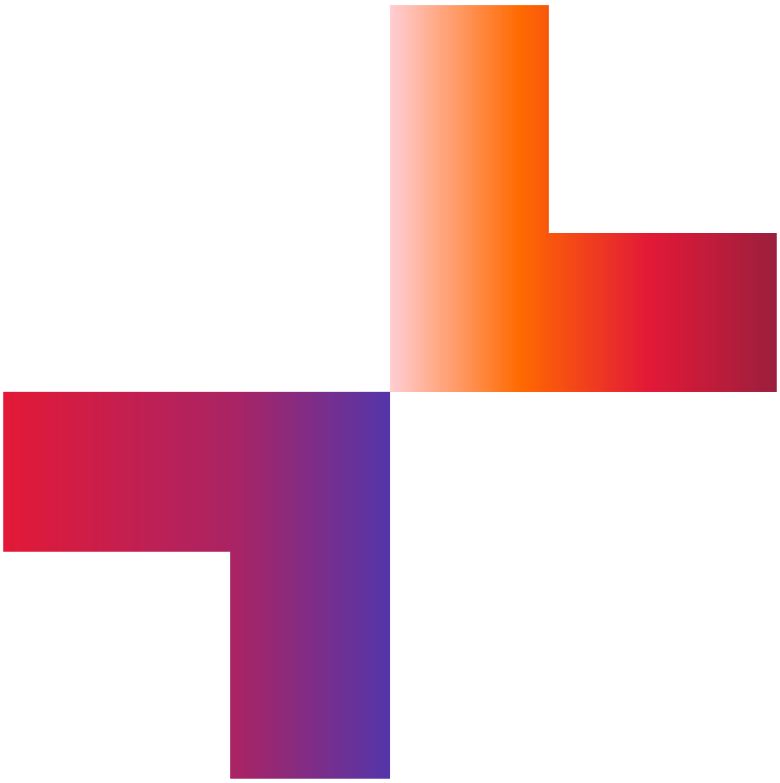
APPENDIX 1: SAMPLE QUESTIONS

SAMPLE QUESTIONS (Set 1 – focusing on a specific Processing)

- Explain for what purpose Personal Data is being Processed.
- List the Personal Data collected for this specific purpose.
- How long does your team or the business need to Process the data?
- To your knowledge, how long is the Personal Data being kept?
- Is the Personal Data shared (either for hosting, maintenance or performance of the service itself) with third parties (i.e., other CGI Entities or external service providers)?
- If yes, the following is required:
    - Provide the names of these third parties.
    - Specify the reasons why they access the data.
    - Is there a data protection clause in the contract or a specific data Processing agreement with such third parties?
    - If yes, please specify and provide evidence.
    - Are these third parties located in a different country? If yes, list the countries where the data is being sent to or from where the data is being accessed.
- If Personal Data is transferred or accessed from Third Countries, please specify for what purpose they need to access this data.
- Do you have contractual agreements with third parties? If yes, please provide evidence.
- Have Data Subjects been informed about the Processing of their Personal Data? If yes, please provide evidence.
- Do you know whether any prior formalities in relation to this Processing have been filed with the relevant Supervisory Authority? If yes, please provide evidence.
- What are the security commitments taken in relation to this Processing? Do they rely on the IT/enterprise security policies and standards? If not, please specify whether the deviations have been approved and documented by CGI IT/security team.

SAMPLE QUESTIONS (Set 2 – focusing on general compliance)

- Has a privacy impact assessment been performed for the Processing of Personal Data?
- If yes, under what conditions is the assessment being performed?
- Are Data Subjects duly informed about the Processing? If yes, how are they being informed?
- Is there a data retention policy in place?
- If yes:
    - How is the implementation of this retention policy being monitored?
    - Are there controls in place to ensure that the data retention is effectively implemented? If yes, specify what they are and provide evidence.
- How is consent obtained?
- How is consent monitored?
- How is access to the data monitored?
- How are transfers out of the European Union (EU) monitored?
- Are there EU model clauses signed for EU data transfers?
- If yes, are they easy to retrieve?
- Is there mandatory data protection training in place?
- If yes:
    - What topics are being covered?
    - Which population receives such training?
    - Specify what controls are in place to ensure full participation? Provide evidence.
- Are data protection clauses defined in contractual agreements with third parties?
- Does CGI have the right to prevent a transfer to a sub-processor?
- Is the role of the respective parties expressly defined in the contract with third parties (i.e. Which entity acts as Data Controller or as Data Processor?)
- Where CGI processes Personal Data on behalf of clients, do clients require to be informed about the transfer to sub-processors?



cgi.com