Consumer Data Right

Google Security

Overview

The purpose of this white-paper is to provide a complete how-to-guide for achieving accreditation with the Consumer Data Right using Google Cloud Platform and Google Workspace for your cloud software product.

Scoping

For the purposes of implementing and auditing the required security practices, we split them into four types or levels that these practices are implemented and managed:
- **Infrastructure:** the Google Cloud Platform suite of products.
- **Application:** Your own software product(s) and any other third-party software directly supporting the CDR Environment.
- **Endpoint Devices:** mobiles, laptops and external media devices used by your people that support or interact with the CDR Environment.
- **Organisational:** governance level practices that apply broadly across the underlying systems, processes and people.

Implementation

There are four implementation steps that are best followed in order:
1. **Cloud Identity:** Implement the identity and access management solution for access control practices that apply to your organisation and cloud environments.
2. **Cloud Platform (GCP):** Navigate to each of the Google Cloud knowledge base links below to implement the related security configurations, licenses and products.
3. **Endpoint Management:** Use advanced endpoint management and follow each of the links below to set up the related security practices for end user devices.
4. **AssuranceLab Knowledge Base:** A comprehensive suite of how-to-guides, examples, tips and links for the required organisational practices that bring it all together.

CDR Schedule 2 Part 1

Schedule 2 Part 1 of the CDR includes five governance requirements for accreditation. These are not specific to the underlying Google products or your systems. Each area is covered as a topic in AssuranceLab's knowledge base with guidance on what to consider and how to implement these in your environment.

1. **Security governance**
2. **Define the boundaries of the CDR environment**
3. **Information security capability**
4. **Controls Assessment Program**
5. **Manage and report security incidents**

CDR Schedule 2 Part 2

Minimum controls	Description of minimum controls	Infrastructure	Software	Endpoint devices	Organisational
Multi-factor authentication	Multi-factor authentication or equivalent control is required for required for all access to CDR data.	Enforce MFA	Enforce MFA	N/A	Access Control Policy
Restrict administrative privileges	Administrative privileges are granted only on an as needs basis for users to perform their duties and only for the period they are required for. Privileges granted on an ongoing basis are regularly reviewed to confirm their ongoing need.	Temporary Access OR Access Management	Access Management	N/A	Access Control Policy
Audit logging and monitoring	Critical events are identified, logged and retained to help ensure traceability and accountability of actions. These logs are reviewed regularly to identify irregularities and deviations from expected processing.	Audit logs	N/A - Refer to organisational controls	N/A	Access Control Policy

Network Security |
| **Access security** | Processes, including automatic processes, are implemented to limit unauthorised access to the CDR data environment. At the minimum these include:
a. provision and timely revocation for users who no longer need access; and
b. monitoring and review of the administrative access rights at least monthly and user access reviewed at least quarterly. | Identify & Access Management AND Managing Access | N/A - Refer to organisational controls | N/A | Access Control Policy

Joiner and Leaver Checklists

User Access Reviews |

Minimum controls	Description of minimum controls	Infrastructure	Software	Endpoint devices	Organisational
Limit physical access	Physical access to facilities where CDR data is stored, hosted or accessed (including server rooms, communications rooms, and premises of business operation) is restricted to authorised individuals.	Google Cloud Platform SOC 2 Report	N/A	N/A	Physical Security
Role-based access	Role-based access is implemented to limit user access rights to only that necessary for personnel to perform their assigned responsibilities. Role-based access is assigned in accordance with the principles of least necessary privileges and segregation of duties.	Role-Based Access Control	N/A - Refer to organisational controls	N/A	Access Control Policy Segregation of Duties
Unique IDs	Use of generic, shared and/or default accounts is restricted to those necessary to run a service or a system. Where generic, shared and/or default accounts are used, actions performed using these accounts are monitored and logs are retained.	Understanding service accounts AND Managing Service Accounts	N/A - Refer to organisational controls	N/A	Access Control Policy Acceptable Use Policy
Password authentication	Strong authentication mechanisms are enforced prior to allowing users to access systems within the CDR data environment, including, but not limited to, general security requirements relating to password complexity, account lockout, password history and password aging.	Password Configuration	N/A - Refer to organisational controls	Endpoint Password Enforcement	Access Control Policy

Minimum controls	Description of minimum controls	Infrastructure	Software	Endpoint devices	Organisational
Encryption	Encryption methods are utilised to secure CDR data at rest by encrypting file systems, end-user devices, portable storage media and backup media. Cryptographic keys are securely stored, backed-up and retained. Appropriate user authentication controls (consistent with control requirement 1) are in place for access to encryption solutions and cryptographic keys.	Encryption-at-rest Encryption-in-transit	N/A	Enforce Device Encryption	Encryption
Firewalls	Firewalls are used to limit traffic from untrusted sources. This could be achieved by implementing a combination of strategies including, but not limited to: a. restricting all access from untrusted networks; b. denying all traffic aside from necessary protocols; and c. restricting access to configuring firewalls, and review configurations on a regular basis.	Firewall Management	N/A	N/A	Network Security

Minimum controls	Description of minimum controls	Infrastructure	Software	Endpoint devices	Organisational
Server hardening	Processes are in place to harden servers running applications, databases and operating systems in accordance with accepted industry standards.	Cluster Hardening	N/A	N/A	Hardening and Patching
End-user devices	End-user devices, including bring-your-own-device (BYOD) systems, are hardened in accordance with accepted industry standards.	N/A	N/A	Device Approval & Tracking AND Security Checklist	Access Control Policy CDR Policy
Data loss prevention	Data loss and leakage prevention mechanisms are implemented to prevent data leaving the CDR data environment, including, but not limited to: a. blocking access to unapproved cloud computing services; b. logging and monitoring the recipient, file size and frequency of outbound emails; c. email filtering and blocking methods that block emails with CDR data in text and attachments; and d. blocking data write access to portable storage media.	N/A	N/A	Device Approval & Tracking AND Security Checklist	Data Loss Prevention Acceptable Use Policy Hardening and Patching

Minimum controls	Description of minimum controls	Infrastructure	Software	Endpoint devices	Organisational
CDR data in non-production environments	CDR data is secured from unauthorised access by masking data, prior to being made available in non-production environments.	Data Masking	Data Masking	N/A	Change Control Policy and Environment CDR Policy
Information asset lifecycle (as it related to CDR data)	The accredited data recipient must document and implement processes that relate to the management of CDR data over its lifecycle, including an information classification and handling policy (which must address the confidentiality and sensitivity of CDR data) and processes relating to CDR data backup, retention, and, in accordance with Rules 7.12 and 7.13, deletion and de-identification.	Data Retention Settings	N/A	N/A - Refer to organisational controls	Information Classification Policy and Environment Backup, Retention, Disposal Policy Data Loss Prevention
Security patching	A formal program is implemented for identifying, assessing the risk of and applying security patches to applications and operating systems as soon as practicable.	OS Patch Manager	N/A	Device Approval & Tracking AND Security Checklist	Hardening and Patching

Minimum controls	Description of minimum controls	Infrastructure	Software	Endpoint devices	Organisational
Secure coding	Changes to the accredited data recipient's systems (including its CDR data environment) are designed and developed consistent with industry accepted secure coding practices, and are appropriately tested prior to release into the production environment.	Web-Security Scanner	Web-Security Scanner	N/A	Change control Policy and Environment Segregation of Duties Release Management Checklist
Vulnerability Management	A formal vulnerability management program is designed and implemented, which includes regular vulnerability scanning and penetration testing on systems within the CDR data environment.	Vulnerability Scanning Overview Web-Security Scanner	Vulnerability Scanning Overview Web-Security Scanner Cloud Build Static Code Analysis ClusterFuzz Opensource	N/A	Vulnerability Management

Minimum controls	Description of minimum controls	Infrastructure	Software	Endpoint devices	Organisational
Anti-malware and anti-virus	Anti-virus and anti-malware solutions are implemented on endpoint devices and on servers to detect and remove malware from the CDR data environment and are updated on a regular basis. End-user systems are updated with the latest virus definitions when they connect to the network. Reports or dashboards highlighting compliance metrics are regularly generated and monitored, and non-compliant items are actioned as soon as practicable.	Malware Scanning for Document Uploads	N/A	Anti-Virus Software AND Device Approval & Tracking AND Security Checklist	Acceptable Use Policy Anti-malware Practices Anti-Virus Software
Web and email content filtering	Solutions are implemented to identify, quarantine and block suspicious content arising from email and the web.	N/A	N/A	Website filtering AND Email Content Filtering	Acceptable Use Policy
Application Whitelisting	Download of executables and installation of software on infrastructure and end-user devices (including on BYOD devices) is restricted to authorised software only.	Third-Party Infrastructure Software	N/A - Refer to endpoint devices and organisational controls	Application Whitelisting	Application Whitelisting Acceptable Use Policy

Minimum controls	Description of minimum controls	Infrastructure	Software	Endpoint devices	Organisational
Security training and awareness	All users undergo mandatory security and privacy training prior to interacting with the CDR data environment, with 'refresher courses' provided at least annually.	N/A	N/A	N/A	Security Awareness Training
Acceptable use of technology	A policy relating to the CDR data environment is created, implemented, communicated and agreed to by all personnel prior to being able to access the CDR data environment. This policy sets out the responsibilities of these personnel in interacting with the CDR data environment and is regularly made aware to personnel.	N/A	N/A	N/A	Acceptable Use Policy CDR Policy
Human resource security	Background checks are performed on all personnel prior to being able to access the CDR data environment. These may include, but are not limited to, reference checks and police checks.	N/A	N/A	N/A	Background Checks