Governance Studio
by Adapted Media Pty Ltd

GOOGLE WORKSPACE CONSOLIDATES DRIVE EXTERNAL SHARING FIELDS IN BIGQUERY INVENTORY REPORTING

OPERATIONAL SIGNAL

DOMAIN: DATA — DATA HANDLING I **CONFIDENCE LEVEL:** HIGH
INSTITUTIONAL DIMENSIONS: Authority I Attribution I Visibility I Escalation I Continuity

Signal ID	Platform	Source	Audience	Signal Date
SIG-DATA-012	Google Workspace	Link	Security I Data I Admin	21 August 2026

CAPABILITY SHIFT

Google Workspace Drive Inventory Reporting in BigQuery now includes granular external sharing fields that consolidate direct permissions, group memberships and public links into clearer signals of external exposure. Google says the update is designed to simplify complex permission structures for administrators using Drive Inventory Reporting in BigQuery.

ORGANISATIONAL CONSEQUENCE

External access that may previously have required separate interpretation across permission types can now be reviewed through a more consolidated reporting view. Security, data and administration teams may be able to identify externally exposed Drive content more consistently, but existing queries, dashboards and review processes may need adjustment to reflect the new fields.

WHAT TO WATCH

- New external sharing fields appearing in Drive Inventory Reporting exports to BigQuery
- Differences between existing permission queries and the consolidated sharing signals
- Previously overlooked external access becoming visible through group or public-link paths

WHY THIS MATTERS NOW

The update was announced on 21 August 2026 for administrators using Drive Inventory Reporting in BigQuery. Organisations should check whether existing exposure-monitoring logic still matches the new consolidated fields.

WHAT TO REVIEW

- Which queries and dashboards consume Drive Inventory Reporting data
- How external-sharing thresholds map to the new fields
- Who validates changes to security and data reporting
- Whether reviews cover direct, group and public-link exposure consistently

GOVERNANCE CONTEXT

Visibility improves because external sharing paths are presented more clearly in reporting. Governance attention shifts to validating the new fields and integrating them into existing monitoring, not to a new access-control mechanism.

Scope Boundary: This artefact translates observed platform capability changes into operational considerations. It does not constitute policy, legal advice, or enforcement guidance.