ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار التاسع – العدد التاسع والثمانون
تاريخ الإصدار: 2 – آذار – 2026م
www.ajsp.net

"Measuring Google Cloud Platform Capabilities Against NDMO Governance-Foundation Tool-Dependent Specifications: Coverage, Gaps, and Adoption Challenges for Saudi Financial Institutions"

Researcher:

Mohammed Kamel AbdulRahim Asaad

Abdul Latif Jameel United Finance (ALJUF), Jeddah, Saudi Arabia

Certification: Master Certified Data Management Professional (CDMP)

1. Abstract

Saudi financial institutions increasingly adopt Google Cloud Platform (GCP) to modernize analytics and AI, while also facing audit expectations under the National Data Management Office (NDMO) Data Management and Personal Data Protection Standards issued by SDAIA. Some NDMO specifications are largely organizational (policies, roles, committees), while others explicitly require tool-generated evidence such as catalog records, metadata attributes, lineage graphs, profiling scans, data quality rules and results, and operational dashboards and alerts. This paper focuses on those tool-dependent evidence expectations and evaluates how far a GCP-based governance foundation can satisfy them, and where additional governance automation or third-party tooling remains necessary.

We propose a pragmatic rubric that separates (i) native GCP evidence capabilities, (ii) native capabilities that require significant configuration and operating model maturity, and (iii) expectations that typically require external governance workflow/case-management tooling or bespoke integration (common in banks). Using the official NDMO standards as the primary reference and mapping atomic evidence expectations to concrete GCP artifacts, the study shows that a well-implemented GCP governance foundation can cover most tool-dependent evidence needs in the core governance domains (catalog/metadata, classification, profiling, lineage, data quality, monitoring). However, "tool coverage" is not equivalent to "compliance": organizations must still operationalize stewardship, issue management, evidence retention, and audit traceability. The study concludes with an implementation blueprint and challenges for (a) organizations already running on GCP versus (b) organizations adopting GCP primarily to "check the compliance box."

Keywords: SDAIA; NDMO; Data Management and Personal Data Protection Standards; Data governance foundation; Dataplex Universal Catalog; Data lineage; Data profiling; data quality KPIs; Governance workflow automation; Saudi financial services; Cloud compliance.

3. Introduction

The SDAIA-NDMO Data Management and Personal Data Protection Standards establish national expectations for how entities govern data assets, measure data quality, manage metadata, protect personal data, and demonstrate accountability through evidence. In regulated financial services, audit-readiness is not achieved by having policies alone; regulators and internal auditors frequently require proof that controls operate (e.g., catalog entries exist, classification labels are applied, quality rules run on schedule, exceptions are tracked, and operational KPIs are monitored).

Cloud platforms introduce an additional layer: infrastructure and cybersecurity compliance (for example, cloud provider licensing/certification) is necessary to host workloads, but it does not automatically satisfy the NDMO evidence expectations around data governance operations. This paper therefore distinguishes between:
• Platform compliance (where the cloud environment is permitted for the sector), and
• Governance evidence compliance (where an organization must produce tool-generated artifacts to prove control execution).

GCP provides a broad set of services that can be composed into a governance foundation—especially Dataplex Universal Catalog, BigQuery metadata, audit logs, and monitoring capabilities. The central question is whether these capabilities are "enough" to satisfy NDMO specifications that require a tool, and what the realistic challenges are in production banking environments. These governance evidence expectations are interpreted in this paper using the official NDMO standards text as the normative source (National Data Management Office, 2021), while GCP capability statements are based on Google Cloud product documentation (Google Cloud, n.d.).

4. Study Problem

Many NDMO specifications implicitly or explicitly require tool-based evidence (for example: data catalog records, lineage diagrams, profiling statistics, data quality KPIs, and monitoring dashboards). Organizations often ask whether adopting a major cloud platform such as GCP is sufficient to cover these requirements, particularly when GCP is already approved for use in the country. The study problem is to measure the practical coverage of GCP's governance foundation against NDMO tool-dependent evidence expectations, and to identify the remaining gaps and challenges.

5. Study Hypotheses

H1: A GCP governance foundation (Dataplex Universal Catalog + BigQuery metadata + monitoring/logging) can satisfy the majority of NDMO tool-dependent evidence expectations in catalog/metadata, classification, profiling, lineage, and data quality.

H2: A non-trivial subset of NDMO expectations remains outside "pure GCP," especially governance workflow automation (issue/case management, approvals, and policy conflicts) and domains that require specialized enterprise tooling (e.g., MDM, records/content management).

H3: Organizations already using GCP can achieve compliance evidence faster due to existing telemetry and metadata, while compliance-driven adopters face higher first-year effort due to inventorying, classification rollout, and operating model maturity.

6. Study Objectives

- Extract and isolate NDMO statements that realistically expect tool-generated evidence (excluding purely organizational roadmap/budget artifacts).
- Define a practical coverage rubric that separates native evidence, native-with-configuration, and platform-plus-external-tool expectations.
- Map NDMO tool-dependent evidence expectations to concrete GCP artifacts (catalog, lineage, profiling, DQ rules/results, and monitoring dashboards/alerts).
- Compare implementation challenges for (a) existing GCP organizations and (b) compliance-driven adopters.
- Provide an implementation blueprint and governance-automation recommendations for Saudi financial services.

7. Study Significance

The contribution is practical: it helps financial institutions avoid a common compliance anti-pattern—treating a cloud platform approval as a substitute for data governance evidence. It provides an evidence-oriented mapping that can be reused in audits, platform design reviews, and governance operating model discussions. It also clarifies what must be complemented by governance workflow automation, third-party catalog/MDM platforms, or enterprise ITSM tools. This framing is consistent with data governance accountability principles and evidence-oriented control operation discussed in DAMA-DMBOK and reflected in NDMO implementation expectations (DAMA International, 2017; National Data Management Office, 2021).

8. Study Limits

- The study evaluates capability coverage at the level of "evidence artifacts," not at the level of each organization's unique processes, legacy systems, or audit interpretations.
- Some NDMO requirements are intentionally high-level; interpretations may vary by regulator, auditor, and sector.
- GCP capabilities evolve; the mapping reflects publicly documented capabilities at the time of writing and assumes standard enterprise configurations (Google Cloud, n.d.).
- The analysis does not benchmark performance or cost, except where cost influences feasibility of continuous scanning and monitoring.
- The governance-foundation domain selection in this paper is purposive and evidence-oriented. Domains were included in the strict quantitative set when the NDMO clauses contained recurring tool-evidence expectations (catalog/metadata, lineage, profiling, data quality results/KPIs, and governance workflow/monitoring evidence). The exclusion of other domains from quantitative scoring should not be interpreted as lower regulatory importance.
- NCA Cloud Cybersecurity Controls (CCC) are treated in this study as platform-control prerequisite context for cloud hosting in Saudi Arabia, not as a substitute for NDMO data governance evidence requirements (National Cybersecurity Authority, n.d.).

9. Key Terms and Definitions

- Tool-dependent evidence: An NDMO expectation that is most reasonably satisfied by artifacts produced by a software tool (e.g., catalog record, lineage graph, scan report, DQ result, monitoring dashboard).
- Governance foundation: The minimum set of capabilities required to operationalize data governance at scale—catalog/metadata, classification, lineage, profiling, data quality measurement, monitoring, and issue handling.
- Coverage tier (rubric): N = Native evidence available directly; N+C = Native but requires configuration, integration, and operating model maturity; P+E = Platform plus external tool or bespoke integration typically required.

10. Theoretical Framework and Previous Studies

This study is grounded in two complementary perspectives: (1) data governance as an organizational accountability function and (2) platform capabilities as technical enablers of governance evidence. From a DAMA perspective, data governance requires defined roles, decision rights, controls, policies, stewardship, and measurable oversight, while metadata, quality, and lineage capabilities support execution and monitoring (DAMA International, 2017). In the Saudi context, the NDMO standards operationalize these expectations by requiring governance structures, disciplined metadata management, measured data quality, and evidence of control operation (National Data Management Office, 2021).

Prior practitioner and platform documentation widely describes cloud-native capabilities for metadata management, monitoring, audit logging, orchestration, and policy enforcement (Google Cloud, n.d.). However, such sources primarily describe product features and implementation patterns rather than evaluating whether those capabilities are sufficient as compliance evidence against a structured national governance framework. Existing discussions on data observability similarly emphasize reliability and operational monitoring more than governance-evidence sufficiency.

The research gap addressed by this paper is therefore the absence of a practical assessment model that distinguishes between: (a) platform-native evidence that can directly support governance requirements, (b) platform capabilities that require additional governance controls and operating processes, and (c) requirements that remain primarily process- and policy-dependent. This study contributes a practical assessment rubric (N, N+C, P+E) and applies it to a defined subset of NDMO governance-foundation requirements to evaluate the role of GCP as a governance evidence foundation in a regulated context.

11. Methodology

11.1 Primary reference

The primary normative reference for this study is the SDAIA-issued NDMO Data Management and Personal Data Protection Standards (Version 1.5, January 2021). All interpretation, domain classification, and compliance reasoning in this paper are anchored to the official standard text. A working analysis matrix may be used internally only to enumerate atomic statements; it is not a normative source and is not cited as evidence.

11.2 Evidence-oriented extraction

To avoid unrealistic technology mapping (for example, mapping roadmap, planning, or policy-drafting requirements to cloud technical controls), this study applies a strict 'tool-evidence' filter. Only statements that can be evidenced by data-governance tooling outputs are included in the quantitative coverage analysis. These outputs include catalog records, metadata tags, lineage graphs, profiling outputs, data-quality KPI results, monitoring alerts/logs, and governed issue-workflow records. Process-only and planning-only requirements remain in scope for overall compliance, but are excluded from the tool-evidence scoring.

11.3 Coverage rubric

Each tool-evidence statement is mapped to one of three tiers: -

• N (Native): GCP can directly produce the evidence artifact.

• N+C (Native + Configuration): GCP can produce the artifact, but only with configuration and governance operating discipline (taxonomies, stewardship, schedules, thresholds, retention).

• P+E (Platform + External): Evidence typically requires external workflow/ITSM/GRC tooling, enterprise process integration, or specialized platforms beyond core GCP governance services.

11.4 Governance-foundation scope for this version

This revised version narrows the quantitative charts and appendix mapping to governance-foundation domains most directly tied to data-governance tooling evidence: Data Catalog and Metadata; Data Quality (including profiling and DQ KPIs); Data Governance (issue and policy workflow evidence); governance monitoring and KPI evidence where applicable (cross-cutting, not treated as a separate NDMO domain in this version); and the lineage-relevant subset of Data Architecture and Modelling.

11.5 Two adoption scenarios

Scenario A: Existing GCP organization: data assets already reside in supported services and telemetry/metadata exist; governance foundation can be enabled incrementally.
Scenario B: Compliance-driven adopter: GCP is adopted primarily to meet tool-dependent NDMO evidence expectations; additional effort is needed to inventory, classify, and integrate non-GCP sources.

11.4.1 Scope justification for governance-foundation domain selection

The selected domains were defined using an evidence-first screening of the official NDMO Data Management and Personal Data Protection Standards (National Data Management Office, 2021). A domain/sub-clause was included in the strict quantitative set only when the requirement reasonably expects repeatable tool-generated governance evidence (e.g., catalog records, metadata attributes, lineage traces, profiling scans, data quality rule results, issue-workflow records, or governance KPI dashboards/logs). Domains and clauses whose primary evidence is policy text, committee decisions, budgets, appointments, or organizational mandates were not quantitatively scored in this version, even though they remain essential for overall NDMO compliance. This scope is therefore a purposive governance-foundation subset designed for tool-evidence assessment, not a claim that the selected domains are the only important NDMO domains.

11.6 Methodological transparency and classification procedure

The assessment was performed using a structured review process. First, selected NDMO requirements were screened and limited to statements relevant to governance implementation evidence and operating controls within the defined scope. Second, each statement was assessed against the availability of demonstrable GCP-native capabilities and evidence artifacts. Third, each statement was classified into one of three categories: N (Native), N+C (Native + Configuration), or P+E (Platform + External). Borderline cases were resolved using a conservative rule: if governance ownership, approval workflow, exception handling, or policy enforcement evidence depended primarily on organizational process rather than platform evidence, the statement was not classified as N. The classification was intentionally strict to avoid overstating platform compliance and to preserve the distinction between technical enablement and governance accountability.

The objective of this classification was not to certify compliance, but to evaluate the strength of GCP as a governance evidence foundation under a constrained assessment scope.

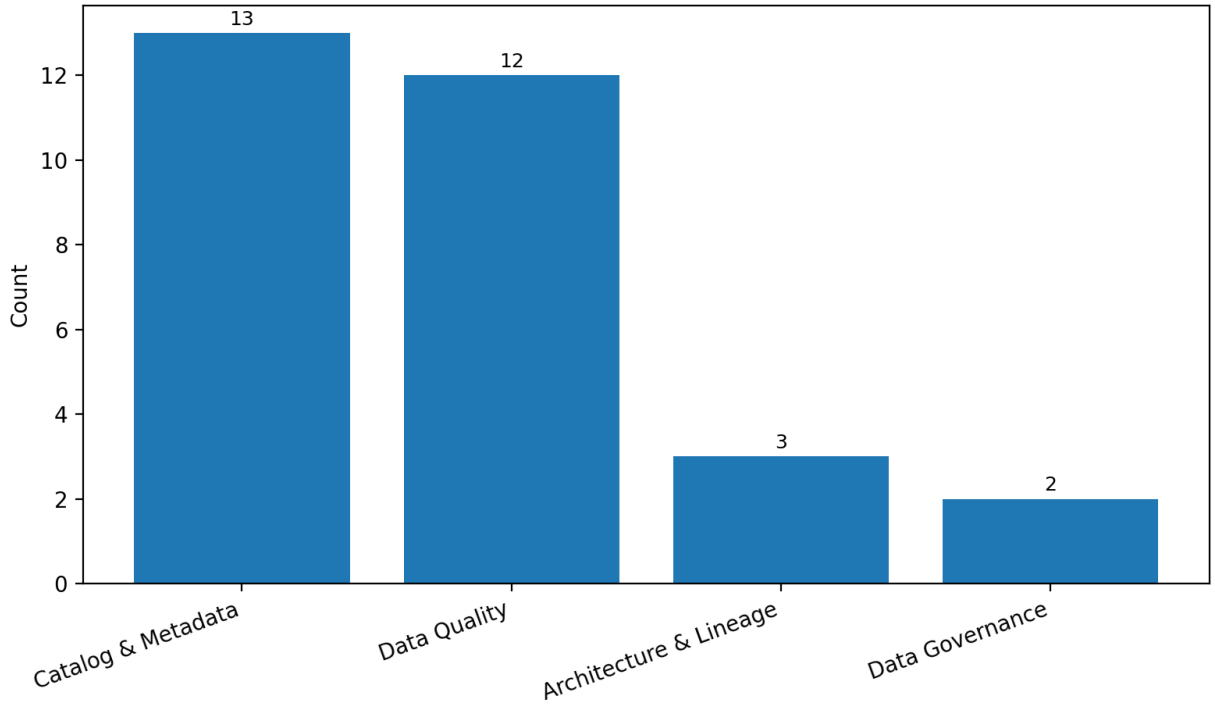
12. Results and Discussion

After applying the stricter governance-foundation scope and excluding roadmap/plan-only statements, the quantitative analysis contains 30 tool-evidence statements across four governance-foundation domains: metadata/catalog, data quality (including profiling), lineage-relevant architecture evidence, and governance workflow evidence, with governance monitoring and KPI evidence treated as a cross-cutting evidence layer (not a separate NDMO domain in this version).

Figure 1 summarizes the distribution of governance-foundation tool-evidence statements by NDMO domain (strict governance set only).

Figure 1. Governance-foundation tool-evidence statements by NDMO domain (strict set).

Figure 1. Domain distribution (governance-foundation strict set)



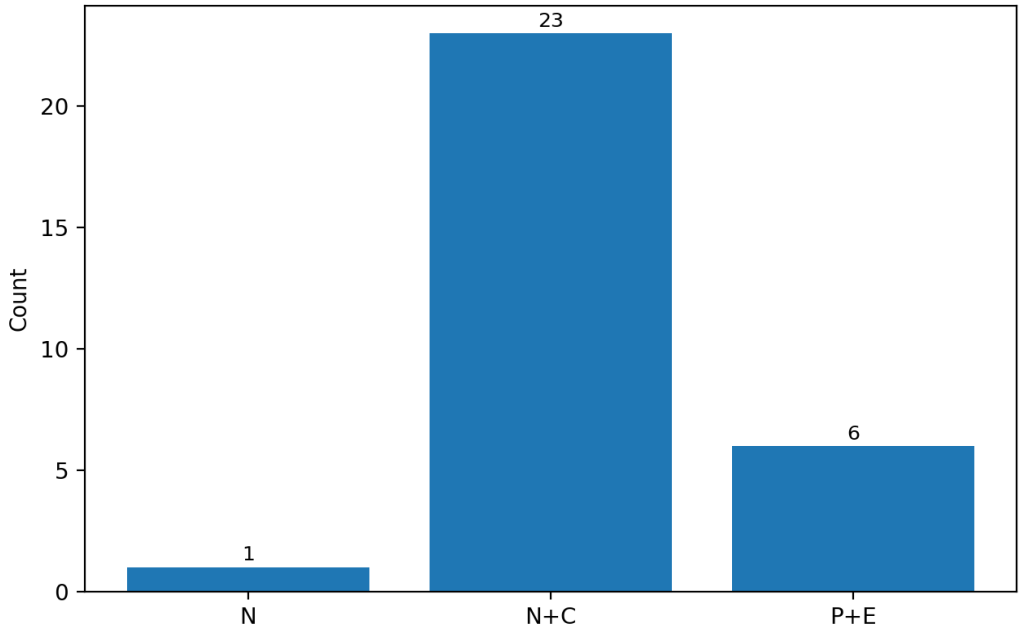
Using the coverage rubric, the governance-foundation strict set is dominated by N+C items, indicating that capability is present but realization depends on taxonomy design, stewardship assignments, scan scheduling, monitoring thresholds, and evidence retention discipline. In this strict set, N = 1 (3.3%), N+C = 23 (76.7%), and P+E = 6 (20.0%).

In addition to the visual summaries, the results indicate that the assessed requirements cluster mainly in the combined support categories (N+C and P+E), with only a small minority qualifying as purely native evidence without additional configuration or operating discipline. This pattern supports the central argument of the paper: GCP provides a meaningful governance foundation, but full compliance evidence remains dependent on governance process design, role accountability, and operating controls. The classification results therefore should be interpreted as a governance-enablement assessment, not a direct compliance certification outcome (National Data Management Office, 2021; Google Cloud, n.d.).

Domain-wise counts and representative mappings are included in Appendix A to support reproducibility and to provide textual backup for the figure summaries.

Figure 2. Coverage tiers for governance-foundation tool-evidence (strict set).

Figure 2. Coverage tiers for governance-foundation tool-evidence (strict se



12.1 Interpreting Coverage for Data Governance Foundation

In financial services, the governance foundation is most often audited through the presence and quality of metadata, lineage, classification, and measured data quality. Within these core domains, GCP performs strongest when Dataplex Universal Catalog is used as the metadata fabric, with BigQuery/BigLake as the governed lakehouse layer. For personal-data discovery and classification evidence within profiling and quality workflows, Sensitive Data Protection (Cloud DLP) is treated as the primary GCP inspection capability.

Table 1 summarizes the governance foundation capability areas, the expected NDMO evidence artifacts, and how GCP typically satisfies them.

Capability area	Typical NDMO evidence expectation	GCP-native building blocks	Common gaps / notes
Catalog & Metadata	Catalog records; tags/attributes; ownership & stewardship fields	Dataplex Universal Catalog; BigQuery policy tags	Taxonomy & stewardship are organizational; non-GCP sources may need connectors.
Data Lineage	Lineage graphs; source-to-target traceability	Dataplex Data Lineage; Data Lineage API	Coverage varies by service; for non-GCP and legacy pipelines, organizations typically need custom lineage ingestion via the Data Lineage API and/or external lineage tooling.
Data Profiling	Profiling statistics; sensitive-data discovery outputs	Dataplex Data Profiling; Sensitive Data Protection (Cloud DLP)	Continuous scanning can be costly; sampling and scheduling must be

			governed; Cloud DLP supports personal-data discovery/classification evidence.
Data Quality KPIs	DQ rules; run results; exceptions; scorecards	Dataplex Data Quality; SQL checks; Dataform tests	Exception handling & remediation workflow typically requires ITSM integration.
Monitoring & Governance KPIs	Dashboards; alerts; logs (where governance evidence is expected)	Cloud Monitoring/Logging; BigQuery INFORMATION_SCHEMA; Audit Logs	Define KPI definitions, retention, and evidence retention for audits.
Governance Automation	Issue/ticket lifecycle; approvals; policy conflict resolution evidence	Workflows + Pub/Sub/Functions (integration)	Case management is not native; banks usually integrate with ServiceNow/Jira/GRC tools.

12.2 Challenges and Realistic Limitations

- Operating model maturity: Dataplex can store metadata, but compliance requires that owners, stewards, and governance responsibilities are defined and actively used.
- Lineage completeness: cloud-native lineage is strongest for native pipelines; heterogeneous toolchains often require custom lineage ingestion via the Data Lineage API and/or external lineage tooling. Without this, source-to-target trace evidence will be incomplete for non-GCP and legacy pipelines.
- Evidence retention: audit expectations may require longer retention than default log windows; exporting logs and scan results to a governed repository is essential. In practice, institutions should explicitly address the retention delta by using log sinks to route Cloud Logging evidence to long-term storage (for example Cloud Storage Coldline/Archive classes) under governed retention and access controls.
- Exception management: DQ scans and profiling produce findings, but NDMO often expects controlled exception handling (triage, approval, remediation, and closure). This typically requires workflow/ticket integration.
- Scope boundaries: some NDMO domains (MDM, document/content management) are not satisfied by GCP alone and usually require specialized platforms.

12.3 Existing GCP Users vs Compliance-Driven Adopters

Scenario A: Existing GCP users can treat compliance as “instrumentation and governance activation.” They often already have BigQuery datasets, IAM groups, and logs, so the incremental work is to establish taxonomies, enable Dataplex scanning, formalize stewardship, and build KPI dashboards.

Scenario B: Compliance-driven adopters face a different reality: most effort is not in enabling a tool, but in discovering and onboarding data sources, building a minimal catalog, aligning classification labels, defining DQ rules, and integrating remediation workflows. Attempting to “buy compliance” by enabling a platform without governance processes typically leads to superficial artifacts that fail audit scrutiny.

13. Recommendations and Implementation Blueprint

- Start with a governance foundation backlog: (1) catalog + taxonomy, (2) classification tagging and policy tags, (3) profiling scans for top data domains, (4) lineage for critical pipelines, (5) DQ rules + KPI scorecards, (6) monitoring dashboards for operational KPIs.
- Make governance automation explicit: integrate scan findings and DQ exceptions with the bank's ticketing/ITSM tool (e.g., ServiceNow) using Workflows/Pub/Sub, and define SLA-based escalation.
- Design for audit evidence: export and retain scan results, lineage exports, and monitoring snapshots in a controlled evidence repository with access controls and retention policies. Where Cloud Logging/Monitoring data is used as evidence, configure log sinks to long-term archival storage (for example Coldline/Archive) so evidence remains available for multi-year audit and regulatory review windows.
- Prioritize high-risk data domains first (customer, credit, finance, HR) and treat "coverage %" as a risk-based rollout metric rather than a vanity metric.
- For non-GCP sources, adopt a connector strategy (batch metadata ingestion or third-party catalog integration) to avoid a 'GCP-only' governance blind spot.

13.1 Governance Foundation Assessment Logic

To make the study more realistic for banks and finance companies, the governance-foundation assessment should be interpreted as an evidence-maturity assessment rather than a binary cloud feature checklist. A high N+C score does not mean weak capability. It means the platform can produce the evidence, but the institution must still define the governance operating model that makes that evidence reliable, repeatable, and audit-defensible.

For this reason, each tool-dependent specification should be evaluated on two axes: platform capability sufficiency (can GCP produce the evidence artifact?) and governance operating sufficiency (can the institution repeatedly produce, approve, retain, and explain that evidence?). This two-axis logic reduces the risk of over-claiming compliance based on technical enablement alone.

13.2 Data Governance Automation and Workflow Integration

A key gap in many cloud-led governance programs is the distance between detection and resolution. GCP services can support detection of metadata gaps, profiling anomalies, data-quality failures, and monitoring exceptions. However, NDMO-aligned governance maturity usually requires a managed lifecycle for triage, assignment, remediation, exception approval, escalation, and closure evidence. This is why governance automation is treated in this paper as part of the governance foundation rather than an optional enhancement.

In regulated organizations, a practical pattern is event-driven integration between governance evidence and enterprise workflow systems (for example ServiceNow, Jira, or a GRC / ITSM platform). The platform produces evidence signals, and the workflow system records accountable decisions, due dates, approvers, and closure history.

- Detection event: profiling scan, DQ rule execution, metadata validation, or monitoring alert produces an issue signal linked to a specific asset or data product.
- Case creation: a workflow case or ITSM ticket is created with asset identifiers, domain, severity, and links to evidence artifacts.
- Assignment and SLA: the case is routed to the data owner, steward, engineering team, or control owner based on stewardship mapping.
- Decision branch: remediate, approve exception, or document accepted risk with approver identity and validity period.
- Closure evidence: timestamps, actions, and attachments are retained and linked back to the originating governance signal.
- KPI feedback loop: aging, SLA compliance, recurrence rate, and reopened cases feed governance dashboards.

This workflow layer is also where policy conflicts are handled (for example retention vs analytics reuse, or access minimization vs operational necessity). GCP can support metadata and logging evidence, but the conflict-resolution process itself normally depends on a governed workflow and therefore is often classified as P+E in realistic assessments.

13.3 Data Value Realization as a Governance-Foundation Outcome

This revised version explicitly frames data value realization as an outcome of governance foundation maturity. When catalog coverage, lineage visibility, profiling, DQ KPIs, and issue workflow discipline improve, organizations should see measurable improvements in analytics delivery speed, report trust, and audit response efficiency. Therefore, governance tooling should be evaluated not only by technical outputs but also by business and compliance outcomes.

Examples of value-realization indicators include: time to onboard a dataset into the governed catalog, percentage of priority data elements with assigned owners and quality rules, mean time to close recurring data issues, reduction in manual evidence preparation time, and percentage of BI / analytics products using lineage-backed governed sources. GCP can support calculation and visualization of many such metrics, but institutions must define metric ownership and measurement rules.

13.4 Existing GCP Organizations vs Compliance-Driven Adopters

Existing GCP organizations typically have a structural advantage because telemetry, IAM patterns, and partial metadata already exist. Their primary challenge is standardization: enterprise taxonomies, stewardship roles, scan schedules, alert thresholds, evidence retention rules, and workflow discipline. Compliance-driven adopters face a different challenge: they must establish both the platform and the governance operating model while also integrating non-GCP and legacy sources.

For compliance-driven adopters, a narrow high-value pilot is usually the safest starting point. A practical first scope is one regulated domain (for example customer, finance, or risk reporting data) and one end-to-end evidence chain: catalog -> tags/classification -> lineage -> profiling -> DQ rules -> issue workflow -> KPI dashboard. This produces visible audit-ready outputs early and avoids large but shallow enterprise-wide rollouts.

13.5 Implications for Audit Readiness and Evidence Packaging

For NDMO assessments, organizations should package evidence as repeatable bundles instead of ad hoc screenshots. A governance-foundation evidence bundle should usually include dated exports or snapshots of catalog entries and tags, lineage outputs, profiling and DQ run summaries, monitoring and alert logs for the assessed period, workflow records showing assignment and closure, and a KPI dashboard with metric definitions and accountable owners.

This reinforces the central conclusion of the paper: GCP is a strong enabler for governance-foundation evidence production in Saudi-regulated environments, especially for institutions already operating on GCP. However, compliance quality depends on how the organization operationalizes governance design, workflow automation, and evidence management around the platform. The practical question is not whether GCP alone is 'compliant', but how much of the required governance evidence chain it can natively support and where external workflow or specialized tools remain necessary.

14. Conclusion

GCP can support a strong portion of NDMO tool-dependent evidence expectations when approached as a governance foundation (not only as an analytics platform). Dataplex Universal Catalog, profiling, lineage, and data quality capabilities combined with Cloud Monitoring/Logging—provide practical artifacts for audits in the core governance domains. Nevertheless, GCP is not a complete substitute for governance operating model maturity, nor does it provide end-to-end governance case management by itself. For Saudi financial services, the most realistic path is a hybrid: cloud-native governance evidence for catalog/lineage/profiling/DQ/monitoring, complemented by enterprise workflow/ticketing and, where needed, specialized platforms for MDM and content management. This study does not claim that GCP alone achieves NDMO compliance; rather, it evaluates the extent to which GCP provides a verifiable governance evidence foundation when combined with organizational controls, ownership, and operating processes.

References:

DAMA International. (2017). DAMA-DMBOK: Data management body of knowledge (2nd ed.). Technics Publications.

Google Cloud. (n.d.). Cloud Audit Logs overview. Google Cloud Documentation. Retrieved February 22, 2026, from https://cloud.google.com/logging/docs/audit

Google Cloud. (n.d.). Cloud Monitoring documentation. Google Cloud Documentation. Retrieved February 22, 2026, from https://cloud.google.com/monitoring/docs

Google Cloud. (n.d.). Dataplex Universal Catalog overview. Google Cloud Documentation. Retrieved February 22, 2026, from https://docs.cloud.google.com/dataplex/docs/universal-catalog-overview

Google Cloud. (n.d.). Manage data quality with Dataplex (auto data quality overview). Google Cloud Documentation. Retrieved February 22, 2026, from https://docs.cloud.google.com/dataplex/docs/auto-data-quality-overview

Google Cloud. (n.d.). Use data profiling in Dataplex. Google Cloud Documentation. Retrieved February 22, 2026, from https://docs.cloud.google.com/dataplex/docs/use-data-profiling

Google Cloud. (n.d.). Workflows documentation overview. Google Cloud Documentation. Retrieved February 22, 2026, from https://docs.cloud.google.com/workflows/docs

National Cybersecurity Authority. (n.d.). Cloud Cybersecurity Controls (CCC). Retrieved February 22, 2026, from https://www.nca.gov.sa/legislation/CloudCybersecurityControlsEn.pdf

National Data Management Office. (2021). NDMO data management and personal data protection standards (Version 1.5). Saudi Data and AI Authority (SDAIA). https://sdaia.gov.sa/ndmo/Files/PoliciesEn001.pdf

National Data Management Office. (n.d.). NDMO portal (standards library and supporting documents). Saudi Data and AI Authority (SDAIA). Retrieved February 22, 2026, from https://sdaia.gov.sa/ndmo/

ISSN: 2663-5798 || Arab Journal for Scientific Publishing

الإصدار التاسع – العدد التاسع والثمانون
تاريخ الإصدار: 2 – آذار – 2026م
www.ajsp.net

"قياس قدرات منصة Google Cloud Platform (GCP) مقابل المتطلبات المعتمدة على الأدوات ضمن نطاق الأساس الحوكمي في معايير NDMO التغطية، الفجوات، وتحديات التبني في المؤسسات المالية السعودية"

إعداد الباحث:

محمد كامل عبد الرحيم أسعد

شركة عبد اللطيف جميل المتحدة للتمويل – (ALJUF) جدة، المملكة العربية السعودية

الملخص:

تتجه المؤسسات المالية السعودية إلى اعتماد منصة Google Cloud Platform (GCP) لتطوير التحليلات والذكاء الاصطناعي، بالتوازي مع متطلبات الإثبات والالتزام الواردة في معايير إدارة البيانات وحماية البيانات الشخصية الصادرة عن NDMO التابعة لـ SDAIA وبينما تركز بعض المواصفات على الجوانب التنظيمية مثل السياسات والأدوار واللجان، فإن مواصفات أخرى تتطلب أدلة مولدة من أدوات تقنية، مثل سجلات كتالوج البيانات، البيانات الوصفية، نسب البيانات(Lineage) ، نتائج التنميط، قواعد ونتائج جودة البيانات، ولوحات المراقبة والتنبيهات. يركز هذا البحث على متطلبات الأدلة المعتمدة على الأدوات ضمن نطاق الأساس الحوكمي، ويقيس مدى قدرة بيئة GCP على دعمها بصورة واقعية، وأين تبقى الحاجة إلى تكاملات إضافية أو أدوات خارجية، خصوصا في سير عمل الحوكمة وإدارة الحالات وإغلاق الملاحظات. ويستخدم البحث إطار تصنيف عمليا من ثلاث فئات N :(دليل أصلي من المنصة)، و N+C (متاح من المنصة لكنه يتطلب إعدادا ونضجا تشغيليا)، و P+E (يتطلب المنصة مع أدوات خارجية أو تكاملات إضافية). وتبين النتائج أن GCP يوفر أساسا حوكميّا قويا لإنتاج الأدلة في مجالات الكتالوج والبيانات الوصفية والتصنيف والتنميط والنسب وجودة البيانات ومؤشرات المراقبة، لكن التغطية الأداتية لا تعني الامتثال الكامل؛ إذ يتطلب الامتثال الفعلي تشغيل الأدوار والمسؤوليات وسير معالجة الملاحظات وحفظ الأدلة وإمكانية التتبع التدقيقي بشكل مؤسسي.

الكلمات المفتاحية:

SDAIA؛ NDMO؛ معايير إدارة البيانات وحماية البيانات الشخصية؛ الأساس الحوكمي للبيانات؛ Google Cloud Platform (GCP)؛ Dataplex Universal Catalog؛ Data Lineage؛ Data Profiling؛ جودة البيانات (DQ)؛ مؤشرات الأداء (KPIs)؛ أتمتة حوكمة البيانات؛ المؤسسات المالية السعودية؛ الامتثال السحابي.