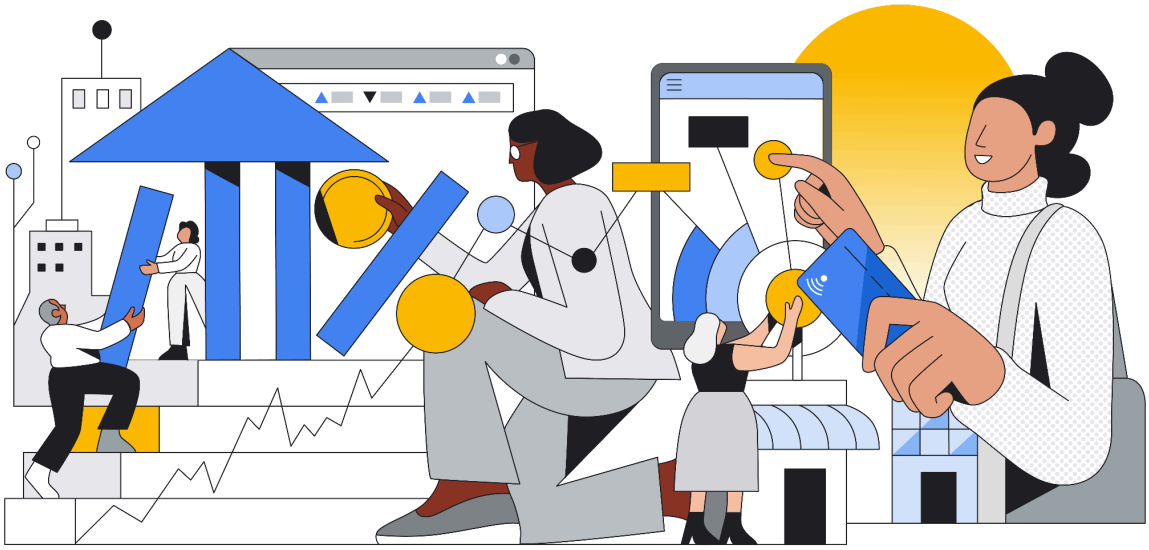
Google Cloud: Navigating the Kuwait's NCSC National Basic Cybersecurity Controls



Author: Akshay Dalal

Table of Contents

Abstract	**3**
Google Cloud's Commitment to Security and Compliance	**3**
Shared Responsibility and Shared Fate on Google Cloud	**4**
Compliance Mapping: NBCC Appendix A – Cloud Security Minimum Controls	**5**
Partnering on Your Compliance Journey	**13**

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of October 2026 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Abstract

The State of Kuwait recognizes that a strong cybersecurity posture is essential to protect national interests, public services, and economic stability. In alignment with this vision, the Kuwait National Cyber Security Center (NCSC) issued Decision No. 2 of 2026, establishing the National Basic Cybersecurity Controls.

Appendix A of this regulation specifically outlines the "Cloud Security Minimum Controls" (CLD-1 through CLD-16) that regulated entities must implement when utilizing public cloud services, including Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

Google Cloud is committed to supporting our customers in Kuwait through their digital transformation journeys. In 2023, Google Cloud announced a strategic alliance with the Government of Kuwait to roll out a comprehensive digital transformation roadmap. This guide is designed to help regulated entities in Kuwait understand how Google Cloud Platform (GCP) capabilities, features, and contractual commitments can support them in meeting the NCSC's Cloud Security Minimum Controls, providing actionable implementation links for engineering and compliance teams. While Google Cloud maintains a secure foundation through adherence to international standards, the regulated entity remains responsible for achieving compliance with NCSC controls using the platform's capabilities.

Google Cloud's Commitment to Security and Compliance

At Google Cloud, security and compliance are integral to the design and operation of our platform. We understand that for financial institutions, trust is paramount, and independent verification of security, privacy, and compliance controls is essential. Our fundamental approach is to deliver a highly secure and resilient infrastructure, complemented by a comprehensive suite of tools and services that empower you to protect your data and applications effectively.

To offer this assurance, Google Cloud undergoes regular, independent third-party audits. We are committed to adhering to key international standards that provide a robust framework for meeting the requirements of the public sector institutions. These include: ISO/IEC 27001 (Information Security Management Systems), ISO/IEC 27017 (Cloud Security), ISO/IEC 27018 (Cloud Privacy), PCI DSS, SOC 1, SOC 2, SOC 3, etc. You can access Google's current certifications and audit reports at any time via our Compliance Reports Manager, which provides streamlined, on-demand access to these crucial compliance resources.

Shared Responsibility and Shared Fate on Google Cloud

A foundational principle of cloud security - and a specific requirement under the NCSC controls (CLD-7) - is the Shared Responsibility Model. Operating in the cloud involves a shared responsibility model, where Google Cloud and our customers both play essential roles in ensuring security and compliance.

Google is responsible for the security of the cloud, meaning we secure the underlying infrastructure, network, and foundational services that support your operations. This includes our global data centers, hardware, software, networking, and the processes and controls for maintaining these systems.

Conversely, you, the customer, are responsible for security in the cloud. This entails the security of your configurations within the cloud environment, the security of your applications and data, identity and access management, network configurations, and the overall security posture of your cloud deployments.

Our shared fate model signifies that we succeed together; your compliance is a collective objective, and we provide the platform and tools to assist you in achieving it. While Google Cloud furnishes a secure platform and comprehensive tools, the ultimate responsibility for achieving and maintaining compliance with the local laws and regulations rests with your organization, based on your specific implementation and operational practices. For more details on this model, refer to the Shared Responsibility and Shared Fate documentation.

Compliance Mapping: NBCC Appendix A – Cloud Security Minimum Controls

The following table details how Google Cloud Platform (GCP) capabilities and features can assist and facilitate regulated entities in aligning with the specific requirements outlined in Appendix A of the NCSC National Basic Cybersecurity Controls (NBCC). Google Cloud adheres to rigorous international security standards (e.g., ISO/IEC 27001, SOC 2) to provide a resilient platform; however, each entity is responsible for configuring and managing their environment to achieve compliance with the local NCSC controls.

Control ID	Control Title	Minimum Requirement	Google Cloud Capabilities, Contractual Commitments & Implementation Links
CLD-1	Regulatory Authorization	Entities MUST ensure the Cloud Service Provider (CSP) is authorized to operate in the State of Kuwait in accordance with regulations issued by the relevant national authorities.	Google will comply with all laws, regulations, and binding regulatory guidance applicable to it in the provision of the services. Please refer to CITRA Authorized Companies for further details.

CLD-2	Provider Due Diligence	Prior to selection, Entities MUST evaluate the CSP's security posture. This requirement is satisfied by reviewing the CSP's valid, independent international security certifications (e.g., ISO 27001, SOC 2 Type II, CSA STAR Level 2).	Google undergoes regular independent third-party audits. Google commits to comply with key international standards including ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2, and SOC 3. Google Cloud also maintains the CSA STAR Level 2 attestation. Customers can download these reports from the Compliance Reports Manager.
CLD-3	Right to Audit (Third-Party Assurance)	Contracts MUST include a "Right to Audit." To protect the security of multi-tenant environments, this right is exercised by the Entity reviewing the CSP's independent Third-Party Audit Reports (e.g., SOC 2, C5) rather than conducting physical data center visits.	Customers can review Google's certifications and audit reports at any time. Customers can download these reports from the Compliance Reports Manager. When required under the applicable privacy law, Google Cloud grants a contractual "Right to Audit" under Section 7.5 (Reviews and Audits of Compliance) of the Cloud Data Processing Addendum (CDPA).

CLD-4	Incident Notification Clause	Contracts MUST include a commitment from the CSP to notify the Entity of a confirmed data incident without undue delay to allow for accurate investigation and reporting.	Google will notify you of data incidents promptly and without undue delay after becoming aware. This commitment is formalized in the Data Incidents section 7.2 of the Google Cloud Data Processing Addendum (CDPA).
CLD-5	Data Ownership & Exit	The contract MUST explicitly state that the Entity retains exclusive ownership of their data. The CSP MUST provide tools or standard APIs to allow the Entity to retrieve their data upon contract termination.	Customers retain all intellectual property rights in "Customer Data". Google Cloud acts strictly as a data processor. Customers can use standard self-service tools and APIs (e.g., GCS tools, BigQuery export) to retrieve data at any time, including termination, without lock-in or additional fees.
CLD-6	Service Level Agreements (SLAs)	Contracts MUST define Service Level Agreements (SLAs) for availability. The agreement SHOULD include financial remedies (service credits) for failure to meet these standards.	Google Cloud provides contractually backed, service-specific SLAs. In the event of an outage failing to meet availability targets, customers are contractually entitled to Service Credits applied to subsequent billing cycles. These are available at Google Cloud SLAs.

CLD-7	Shared Responsibility	Entities MUST document the cloud service model (IaaS, PaaS, or SaaS) and the resulting division of security responsibilities. The Entity retains accountability for Data Classification, Identity & Access Management (IAM), and Resource Configuration, regardless of the model.	It is important for regulated entities to have a clear understanding of the allocation of responsibility in the cloud. Google is responsible for implementing and maintaining the security measures to protect customer data on systems managed or controlled by Google (Section 7.1 CDPA). The Customer is responsible for the use of the services, securing account authentication credentials, systems, and devices, using additional security controls to ensure an appropriate level of security, and backing up or retaining copies of customer data (Section 7.3.1. CDPA). Please refer to Google Cloud Architecture Framework: Security, Privacy, and Compliance for further details.
CLD-8	Cloud Asset Inventory	Maintain a real-time inventory of cloud resources. Use programmatic resource tagging to identify the Data Classification (Public, Restricted, Sensitive) and Business Owner of each resource.	Google provides tools to help you manage your assets on our services. Cloud Asset Inventory allows you to view, monitor, and analyze all your Google Cloud assets across projects and services in real-time. Customers can use Resource Manager to hierarchically organize resources and apply Labels (key-value pairs) programmatically to identify data classification levels and business owners. Please refer to Cloud Asset Inventory Overview and Creating and Managing Labels for further details.

CLD-9	MFA for Cloud Consoles	Multi-Factor Authentication (MFA) MUST be enforced for all users with administrative access to the Cloud Management Console and root accounts.	Google provides a wide variety of MFA verification methods to help protect your user accounts and data. Customers can enforce MFA for all users, including administrators accessing the Google Cloud Console, using Cloud Identity settings. Policies can be configured to require MFA for specific organizational units or administrative roles. Please refer to Enforce 2-Step Verification (MFA) in Cloud Identity for further details.
CLD-10	Service Account Hygiene	Service Accounts (non-human identities) MUST NOT be used for interactive human login. Keys for service accounts SHOULD be rotated periodically based on risk, or managed via automated identity federation (e.g., OIDC) to prevent credential theft.	Google Cloud IAM Service Accounts are designed for non-human identities. Google Cloud enforces that service accounts cannot be used for interactive human login via web interfaces. To mitigate credential theft, Google Cloud recommends using Workload Identity Federation (which supports OIDC) to grant external workloads access to Google Cloud resources without needing to manage or rotate service account keys. Please refer to Workload Identity Federation and Best practices for managing service account keys for further details.

CLD-11	Encryption by Default	All data at rest in the cloud MUST be encrypted. Entities SHOULD utilize the CSP's default encryption (platform-managed keys) as a minimum standard. For Sensitive data, Entities MAY opt for Customer-Managed Encryption Keys (CMEK) on cloud, based on a risk assessment.	Google encrypts customer data stored at rest by default, with no additional action required from you. We also offer a continuum of encryption key management options. For Sensitive data, customers can choose to use Cloud KMS, which lets you manage cryptographic keys, including Customer-Managed Encryption Keys (CMEK).
CLD-12	Data Residency (Customer Content)	The Entity MUST configure cloud services and related contracts to store and process Customer Content (files, databases, application data) according to the National Data Classification Framework.	Google provides you with choices about where to store your data. Once you choose where to store your data, Google will not store it outside your chosen region(s). Customers can leverage Google Cloud's global regions to meet their specific data residency requirements under the National Data Classification Framework. Customers can also use Organization Policies to programmatically restrict resource locations as a technical enforcement mechanism. Please refer to Restricting Resource Locations with Organization Policies for further details.

CLD-13	Operational Metadata Exemption	Residency requirements apply to Customer Content. Operational Metadata (e.g., project IDs, billing logs, system status, IP addresses) can be processed globally. Entities must ensure that metadata identifiers remain non-sensitive.	Google Cloud processes Operational Metadata globally to provide a fast, reliable, robust, and resilient service, as well as for accurate billing and security monitoring. Customers are responsible for their resource naming conventions and must ensure that they do not include sensitive Customer Content in Operational Metadata (such as Project IDs, VM names, or labels).
CLD-14	Public Access Prevention	Cloud storage resources (e.g., object storage buckets) MUST be configured to block public access by default. Public exposure MUST be an explicit, documented exception approved by the data owner.	Google Cloud Storage provides a native feature called "Public Access Prevention" which allows customers to enforce a restriction that prevents public access to Cloud Storage buckets. Customers can apply this setting at the organization, folder, or project level using Organization Policies to ensure that public access is blocked by default. The Customer is solely responsible for configuring, documenting, and approving any explicit exceptions. Please refer to Enforcing Public Access Prevention on Cloud Storage for further details.

CLD-15	Cloud Audit Logging	Enable audit logging for cloud projects. Logs MUST capture "Admin Activity" (configuration changes) and "Data Access" (who accessed data) for sensitive workloads. Retain logs for a minimum of 12 months.	Cloud Audit Logs help your security teams maintain audit trails in Google Cloud. Cloud Audit Logs automatically record "Admin Activity" logs by default. Customers can easily enable "Data Access" logs to capture who accessed data for sensitive workloads. To meet the 12-month retention requirement, customers can use Cloud Logging sinks to route audit logs to a Cloud Storage bucket configured with the appropriate retention policies. Please refer to Cloud Audit Logs Overview and Routing and Storing Logs (Sinks) for further details.
CLD-16	Secure Connectivity	All traffic between the Entity and the cloud provider MUST be encrypted in transit using industry-standard protocols (e.g., TLS 1.2 or higher). Management interfaces MUST NOT be exposed directly to the public internet; use secure bastions, VPNs, or Identity-Aware Proxies.	Google encrypts all data in transit. Google Cloud APIs enforce TLS 1.2 or higher. To protect management interfaces, customers can utilize Google Cloud's Identity-Aware Proxy (IAP) to establish secure, zero-trust access without exposing interfaces to the public internet. Customers can also use Cloud VPN, Cloud Interconnect, and secure bastion hosts. Please refer to Identity-Aware Proxy (IAP) for further details.

Partnering on Your Compliance Journey

Google Cloud is more than a technology provider; we are your partner in navigating the complexities of regulatory compliance. We are dedicated to continuously enhancing our platform and services to help financial institutions in Kuwait meet evolving requirements and innovate securely.

We encourage you to explore Google Cloud's comprehensive compliance resource center to access whitepapers, compliance guides, and detailed documentation relevant to the financial sector and data governance, including the Google Cloud Trust Center, Security section, Geography and Regions documentation, Security Best Practices, and Privacy information. For guidance on how Google Cloud can support your journey to comply with NCSC regulations, please do not hesitate to contact your Google Cloud account team. We are here to help you build and operate secure, compliant, and transformative solutions in the cloud.