# ThreatModel for BigQuery

### Content

This publication includes:

- overall data flow diagram of Google Cloud BigQuery

- overview of the Mitre ATT&CK matrix for Google Cloud BigQuery

- prioritized list of all threat scenarios

- list of all the control activities and testing procedures

- risk-based prioritized list of control implementation

### License Agreement

This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/). This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, so long as attribution is given to the creator. The license allows for commercial use. If you remix, adapt, or build upon the material, you must license the modified material under identical terms.



### Source

The latest version of this work is hosted on [GitHub](https://github.com/trustoncloud/threatmodel-for-gcp-bigquery).

### Contact

If you have any questions, please contact [chatbot@trustoncloud.com](mailto:chatbot@trustoncloud.com).

| **BigQuery** Data Flow Diagram | Security Scorecard  | ***Security in the Cloud*** | | | --- | --- | | Number of Actions\* | 176 | | Identity management | Cloud IAM | | Number of IAM permissions\* | 123 | | Resource-based access | tables  rows  columns  connections  data exchanges  listings | | Logging coverage for APIs | 64.1%  (missing 52) | | Number of Logging Event Names\* | 126 | | VPC Service Controls | Yes | | Network Filtering | No | | Encryption-at-rest | Yes | | Encryption-in-transit | Yes |   \* See details in Appendixes |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

## Mitre ATT&CK matrix for BigQuery

| **Reconnaissance** | **Resource Development** | **Initial Access** | **Execution** | **Persistence** | **Privilege Escalation** | **Defense Evasion** | **Credential Access** | **Discovery** | **Lateral Movement** | **Collection** | **Command and Control** | **Exfiltration** | **Impact** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Unauthorized access to data by changing connection configurations [Bigquery.T2] | Importing malicious models in BigQuery [Bigquery.T24] |  | Restricting access to resources by modifying privileges [Bigquery.T10] |  |  | Discovery of BigQuery sharing resources [Bigquery.T31] |  |  |  | Exfiltration of data by exporting tables to other services [Bigquery.T6] | Destruction of data by deleting dataset or table [Bigquery.T1] |
|  |  |  |  |  | Unauthorized access to the table columns by adding or removing policy tags [Bigquery.T17] |  |  |  |  |  |  | Escalate privileges, loss of availability or integrity of data, or exfiltrate data via an unauthorized query on a dataset or table [Bigquery.T9] | Loss of integrity and availability by copying datasets and overwriting the destination table(s) [Bigquery.T3] |
|  |  |  |  |  | Misconfiguration of a dataset causing loss of integrity and availability, or privilege escalation by modification of the dataset's access array [Bigquery.T21] |  |  |  |  |  |  | Data exfiltration by updating the destination dataset in transfer and transfer credentials; or DoS by schedule manipulation [Bigquery.T13] | Loss of the integrity of the training model [Bigquery.T4] |
|  |  |  |  |  | Unauthorized access to listings by setting permissions [Bigquery.T28] |  |  |  |  |  |  | Data exfiltration by exporting query results [Bigquery.T15] | Loss of integrity and availability by appending or overwriting data, or by creating a table [Bigquery.T5] |
|  |  |  |  |  |  |  |  |  |  |  |  | BigQuery ML model exfiltration [Bigquery.T18] | Loss of integrity and availability by manipulating data using routines [Bigquery.T8] |
|  |  |  |  |  |  |  |  |  |  |  |  | Table exfiltration by cloning [Bigquery.T19] | Disruption of application functionality by modification of table and view configurations [Bigquery.T11] |
|  |  |  |  |  |  |  |  |  |  |  |  | Exfiltration of query results to an unauthorized destination table and bucket [Bigquery.T20] | Denial of Service/Denial of Wallet by removing/creating reservations [Bigquery.T12] |
|  |  |  |  |  |  |  |  |  |  |  |  | Unauthorized access to cached data from the last 24 hours [Bigquery.T26] | Loss of data during recovery by deleting a snapshot [Bigquery.T14] |
|  |  |  |  |  |  |  |  |  |  |  |  | Unauthorized access to contents of a listing [Bigquery.T30] | Permanent loss of a BigQuery ML model by modifying its expiration time [Bigquery.T22] |
|  |  |  |  |  |  |  |  |  |  |  |  | Email leakage via malicious listing [Bigquery.T33] | Misconfiguration of a table to cause loss of integrity and availability [Bigquery.T25] |
|  |  |  |  |  |  |  |  |  |  |  |  | Expose sensitive data via auto-enabled Gemini API [Bigquery.T35] | Loss of data integrity by restoring a snapshot [Bigquery.T27] |
|  |  |  |  |  |  |  |  |  |  |  |  |  | Denial of Service by revoking subscriptions [Bigquery.T29] |
|  |  |  |  |  |  |  |  |  |  |  |  |  | Denial of Service by deleting data exchanges, listings, or subscriptions [Bigquery.T32] |
|  |  |  |  |  |  |  |  |  |  |  |  |  | Denial of Service via unauthorized continuous query cancellation [Bigquery.T34] |
|  |  |  |  |  |  |  |  |  |  |  |  |  | Data corruption via unauthorized hard failover [Bigquery.T36] |

## Feature Classes

BigQuery has the following feature classes and subclasses (i.e. dependent on the usage of its class) that can be activated, restricted, or blocked using Google Cloud Identity and Access Management.

| **Feature** | **Relation** | **Description** |
| --- | --- | --- |
| Dataset and tables (FC1) | class, used by Share resources via BigQuery sharing | You can create a table inside a dataset. You can run SQL queries and jobs on datasets. Jobs are actions that BigQuery runs on your behalf to load data, export data, query data, or copy data. |
| Routines (stored procedures or User-Defined Functions) (FC2) | subclass of Dataset and tables | A routine is a reusable piece of code that can be executed within SQL queries. |
| BigQuery connections and BigQuery Omni (FC3) | subclass of Dataset and tables | To create a connection for federated queries when adding data from external data sources or exporting data to cross Cloud Storages. |
| BigQuery Data Transfer (FC4) | subclass of Dataset and tables | You can transfer external data from SaaS applications to Google BigQuery on a regular basis. |
| BigQuery reservation (FC5) | subclass of Dataset and tables | You can purchase dedicated query processing capacity. |
| BigQuery ML (FC6) | subclass of Dataset and tables | You can create and execute machine-learning models in BigQuery using standard SQL queries. |
| Table snapshot (FC7) | subclass of Dataset and tables | A BigQuery table snapshot preserves the contents of a table (called the base table) at a particular time. |
| Data policy (FC8) | subclass of Dataset and tables | You can provide different levels of visibility to different groups of users by using policy tags. |
| Share resources via BigQuery sharing (FC9) | subclass of Dataset and tables | BigQuery sharing is a data exchange platform built on top of BigQuery that enables efficient and secure sharing of data (e.g., BigQuery tables) across organizational boundaries. |
| Subscribe to access resources via BigQuery sharing (FC10) | class | You can subscribe to the listings. |

| Dataset and tables *(class, used by Share resources via BigQuery sharing, FC1)* *You can create a table inside a dataset. You can run SQL queries and jobs on datasets. Jobs are actions that BigQuery runs on your behalf to load data, export data, query data, or copy data.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Creates a new empty dataset. | bigquery.datasets.create |  Threat List  | **Name** | **CVSS** | | --- | --- | | Escalate privileges, loss of availability or integrity of data, or exfiltrate data via an unauthorized query on a dataset or table | [High (8.0)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) | | Loss of integrity and availability by copying datasets and overwriting the destination table(s) | [Medium (5.7)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H) | | Misconfiguration of a table to cause loss of integrity and availability | [Medium (5.7)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H) | | Misconfiguration of a dataset causing loss of integrity and availability, or privilege escalation by modification of the dataset's access array | [Medium (5.7)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H) | | Loss of integrity and availability by appending or overwriting data, or by creating a table | [Medium (5.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:L) | | Exfiltration of query results to an unauthorized destination table and bucket | [Medium (4.8)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:L/A:N) | | Disruption of application functionality by modification of table and view configurations | [Medium (4.8)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H) | | Table exfiltration by cloning | [Medium (4.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N) | | Exfiltration of data by exporting tables to other services | [Medium (4.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N) | | Restricting access to resources by modifying privileges | [Medium (4.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N) | | Destruction of data by deleting dataset or table | [Low (3.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L) | | Denial of Service via unauthorized continuous query cancellation | [Low (2.4)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L) | | Expose sensitive data via auto-enabled Gemini API | [Low (2.4)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N) | | Unauthorized access to cached data from the last 24 hours | [Low (2.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Escalate privileges, loss of availability or integrity of data, or exfiltrate data via an unauthorized query on a dataset or table

| | **Threat Id** | Bigquery.T9 | | --- | --- | | **Name** | Escalate privileges, loss of availability or integrity of data, or exfiltrate data via an unauthorized query on a dataset or table | | **Description** | SQL queries are run on the data stored inside tables. An attacker can run a simple SQL query (e.g., "SELECT \* FROM *TABLE\_NAME*") to get all the data from a specific table or to execute unauthorized queries for different attacks (e.g., replication to an unauthorized region). An attacker can also update or drop columns in a table, change the case sensitivity of datasets and their tables to escalate privileges while avoiding detection by a poorly designed access management system, set unauthorized default values for a column to corrupt or steal data, or update the metadata cache settings of object or BigLake tables to impact the query latency. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [High (8.0)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) | | **IAM Access** | {  "OR": [{  "AND": ["bigquery.jobs.create", "bigquery.tables.getData"]  }, "bigquery.datasets.update"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO8 - Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings**    C15 - Ensure no dataset is accessible to "AllUsers" or "AllAuthenticatedUsers", except if allowed.    C60 - Define the authorized configuration for each reservation (i.e., maxSlots, edition, ignoreIdleSlots, autoscale, secondaryLocation) and its assignments (i.e., assignee, jobType). | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel.    C6 - Maintain a list of authorized IAM entities allowed to access the tables, views, and table data in a specific dataset (note: columns can be made case-sensitive, and a default value can be set for columns).    C7 - Ensure only authorized IAM entities are allowed to access the tables, views, and table data in each dataset. | High | 3 | - | - |
| **CO5 - Restrict access to columns and protect sensitive data**    C9 - Define the criteria for the sensitivity of columns in each table and each view, and their requirements for data protection (e.g., using BigQuery column-level security, column-level data masking, custom masking routines, restriction analysis rules, list overlap analysis rules, aggregation threshold analysis rules, differential privacy clauses, or data clean rooms).    C10 - Ensure only authorized IAM entities are allowed to access sensitive columns of tables and views. | High | 2 | - | - |
| **CO24 - Enforce secure SDLC processes on routines and queries**    C122 - Enforce secure SDLC processes on queries (e.g., using source control, static analysis, dynamic analysis, and peer review). | High | 1 | - | - |
| **CO6 - Restrict access to rows with BigQuery row-level security**    C12 - Define the criteria for the sensitivity of rows in each table.    C13 - Ensure only authorized IAM entities are allowed to access sensitive rows of a table (e.g., using BigQuery row-level security). | High | 2 | - | - |
| **CO20 - Monitor abnormal performance of queries**    C56 - Monitor the abnormal behavior, such as unexpected increases in execution time or unusual resource utilization, of a query (e.g., by using the query execution graph or administrative jobs explorer). | Medium | - | - | 1 |
| **CO21 - Use authorized metadata caching**    C57 - Define the requirements for metadata cache mode and staleness (30 minutes to 7 days) for each external table.    C58 - Ensure the metadata cache mode and staleness of each external table are set according to its requirements. | Medium | 2 | - | - |
| **CO33 - Define and enforce BigQuery configuration baselines at the organization and project levels**    C123 - Maintain the list of authorized configuration settings (e.g., default\_batch\_query\_queue\_timeout\_ms, default\_interactive\_query\_queue\_timeout\_ms, default\_query\_job\_timeout\_ms, enable\_fine\_grained\_dataset\_acls\_option) for each organization or project.    C124 - Ensure only authorized configuration settings for each organization or project are configured. | Medium | 2 | - | - |

#### Loss of integrity and availability by copying datasets and overwriting the destination table(s)

| | **Threat Id** | Bigquery.T3 | | --- | --- | | **Name** | Loss of integrity and availability by copying datasets and overwriting the destination table(s) | | **Description** | Datasets can be copied to another existing dataset. During this process, the tables in the destination dataset can be overwritten. An attacker can overwrite the destination table, causing a loss of integrity and availability. | | **Goal** | Data manipulation | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (5.7)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H) | | **IAM Access** | {  "AND": ["bigquery.jobs.create", "bigquery.datasets.get", "bigquery.datasets.update", "bigquery.tables.create"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel.    C6 - Maintain a list of authorized IAM entities allowed to access the tables, views, and table data in a specific dataset (note: columns can be made case-sensitive, and a default value can be set for columns).    C7 - Ensure only authorized IAM entities are allowed to access the tables, views, and table data in each dataset. | High | 3 | - | - |
| **CO10 - Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings**    C22 - Maintain a list of authorized sources and destinations (e.g., Cloud Storage, BigQuery, Vertex AI (for LLM, via BigQuery connection only)) to be used with each dataset, table, model, connection, job, and listing.    C23 - Ensure each dataset, table, model, connection, job, and listing uses authorized sources and destinations.    C25 - Protect the sources and destinations used by each table, model, connection, job, and listing, using their respective services' ThreatModels. | High | 3 | - | - |

#### Misconfiguration of a table to cause loss of integrity and availability

| | **Threat Id** | Bigquery.T25 | | --- | --- | | **Name** | Misconfiguration of a table to cause loss of integrity and availability | | **Description** | A table is a primary storage structure used to hold structured data within datasets. Standard BigQuery tables store structured data directly within BigQuery, external datasets and tables reference data stored outside BigQuery, and views are logical tables built using SQL queries. An attacker can create or update a table with an unauthorized configuration to cause loss of integrity or availability (e.g., by creating or updating a materialized view with an unauthorized value for staleness to deliberately serve outdated and potentially misleading data to users or applications, which could lead to inaccurate analysis results and misinformed business decisions, by referencing an external source with corrupted data, by creating a table with an unauthorized value for expiration, or by using an unauthorized key for encryption). | | **Goal** | Data manipulation | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (5.7)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H) | | **IAM Access** | {  "OR": ["bigquery.tables.create", "bigquery.tables.update"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO8 - Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings**    C17 - Define the authorized configuration (i.e., defaultTableExpirationMs, defaultPartitionExpirationMs, defaultEncryptionConfiguration, linkedDatasetSource, externalDatasetReference, defaultCollation, defaultRoundingMode, maxTimeTravelHours, storageBillingModel, and defaultEncryptionConfiguration) for each BigQuery dataset.    C18 - Ensure the configuration of each BigQuery dataset is authorized.    C81 - Define the authorized configuration (i.e., schema, clustering, expirationTime, view, materializedView, externalDataConfiguration, encryptionConfiguration, defaultCollation, defaultRoundingMode, and tableConstraints) for each BigQuery table.    C82 - Ensure the configuration of each BigQuery table is authorized. | Very High | 4 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |

#### Misconfiguration of a dataset causing loss of integrity and availability, or privilege escalation by modification of the dataset's access array

| | **Threat Id** | Bigquery.T21 | | --- | --- | | **Name** | Misconfiguration of a dataset causing loss of integrity and availability, or privilege escalation by modification of the dataset's access array | | **Description** | A dataset is a top-level container used to organize and control access to tables and views. Certain default configurations and options can be set at the organization, project, or dataset level, which indirectly affect the tables within that dataset. An attacker can create or update a dataset with unauthorized values for these configurations to cause loss of integrity and availability (e.g., setting an unauthorized value for defaultTableExpirationMs to delete a table automatically when its expirationTime is reached) or create or modify an access array for a dataset to escalate privileges. | | **Goal** | Data manipulation | | **MITRE ATT&CK®** | [TA0004](https://attack.mitre.org/tactics/TA0004) | | **CVSS** | [Medium (5.7)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H) | | **IAM Access** | {  "OR": ["bigquery.datasets.create", {  "AND": [{  "OPTIONAL": "bigquery.datasets.setIamPolicy"  }, "bigquery.datasets.update"]  }]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel.    C6 - Maintain a list of authorized IAM entities allowed to access the tables, views, and table data in a specific dataset (note: columns can be made case-sensitive, and a default value can be set for columns).    C7 - Ensure only authorized IAM entities are allowed to access the tables, views, and table data in each dataset.    C84 - Prevent the unauthorized access/creation/modification/deletion of BigQuery resources (e.g., datasets, tables) (e.g., by using an IAM policy with an allow/deny statement on "bigquery.tables.\*" and/or "bigquery.datasets.\*" with the tags and the authorized value for the conditions "resource.type" = "authorized type", "resource.name" = "authorized name"). | Very High | 3 | 1 | - |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO8 - Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings**    C17 - Define the authorized configuration (i.e., defaultTableExpirationMs, defaultPartitionExpirationMs, defaultEncryptionConfiguration, linkedDatasetSource, externalDatasetReference, defaultCollation, defaultRoundingMode, maxTimeTravelHours, storageBillingModel, and defaultEncryptionConfiguration) for each BigQuery dataset.    C18 - Ensure the configuration of each BigQuery dataset is authorized.    C133 - Prevent the creation/update of a dataset without an authorized configuration (e.g., using a custom constraint resourceType:[bigquery.googleapis.com/Dataset](https://docs.cloud.google.com/bigquery/docs/custom-constraints#supported_resources), resource(s): resource.defaultCollation != an authorized collation, resource.defaultRoundingMode != an authorized rounding mode, resource.maxTimeTravelHours != an authorized time travel window, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | Very High | 2 | 1 | - |
| **CO10 - Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings**    C22 - Maintain a list of authorized sources and destinations (e.g., Cloud Storage, BigQuery, Vertex AI (for LLM, via BigQuery connection only)) to be used with each dataset, table, model, connection, job, and listing.    C135 - Prevent the creation of a dataset without an authorized source (e.g., using a custom constraint resourceType:[bigquery.googleapis.com/Dataset](https://docs.cloud.google.com/bigquery/docs/custom-constraints#supported_resources), resource(s): resource.linkedDatasetSource.sourceDataset.datasetId != an authorized linked data source, resource.externalDatasetReference != an authorized external dataset reference, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | High | 1 | 1 | - |
| **CO12 - Set the expiration time of BigQuery tables as per the requirements**    C32 - Define the requirements for the expiration time of each BigQuery table.    C136 - Prevent the creation or update of a dataset without an authorized expiration time (e.g., using a custom constraint resourceType:[bigquery.googleapis.com/Dataset](https://docs.cloud.google.com/bigquery/docs/custom-constraints#supported_resources), resource(s): resource.defaultTableExpirationMs != an authorized expiration time, resource.defaultPartitionExpirationMs != an authorized partition expiration time, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | High | 1 | 1 | - |
| **CO32 - Enforce authorized access entities only, change management, and secure decommissioning on datasets**    C116 - Maintain the list of authorized access entities (i.e., role, userByEmail, groupByEmail, domain, specialGroup, iamMember, view, routine, or dataset) for each dataset.    C117 - Ensure only authorized access entities of each dataset are configured. | High | 2 | - | - |
| **CO7 - Encrypt resources (e.g., datasets, models, data transfers) with customer-managed encryption keys and protect the keys**    C26 - Maintain a list of authorized CMEKs to be used with each BigQuery resource (e.g., dataset, DLP function, model, data transfer), ideally dedicated (e.g., using Autokey on bigquery.googleapis.com/Dataset), and of the default CMEK at the project or organization level, and define the requirement to rotate key versions for tables.    C134 - Prevent the creation of a dataset without an authorized key (e.g., using a custom constraint resourceType:[bigquery.googleapis.com/Dataset](https://docs.cloud.google.com/bigquery/docs/custom-constraints#supported_resources), resource(s): resource.defaultEncryptionConfiguration.kmsKeyName != an authorized encryption key, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | High | 1 | 1 | - |
| **CO3 - Ensure backup, failover, and recovery capabilities for BigQuery resources (e.g., snapshots and exports for datasets and tables, failover procedures for reservations)**    C3 - Define the requirements for the backup of each BigQuery dataset, table, and model.    C4 - Ensure each BigQuery dataset, table, and model is backed up (e.g., by creating snapshots or exports) according to the requirements and is restorable. | Medium | 2 | - | - |

#### Loss of integrity and availability by appending or overwriting data, or by creating a table

| | **Threat Id** | Bigquery.T5 | | --- | --- | | **Name** | Loss of integrity and availability by appending or overwriting data, or by creating a table | | **Description** | Data is stored inside a BigQuery table. An attacker can create a table, overwrite table data using a load or query operation, or append additional data to an existing table by performing a load-append operation or by appending query results to the table, causing a loss of data integrity and availability. | | **Goal** | Data manipulation | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (5.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:L) | | **IAM Access** | {  "OR": ["bigquery.tables.create", "bigquery.tables.updateData", "bigquery.jobs.create"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel.    C6 - Maintain a list of authorized IAM entities allowed to access the tables, views, and table data in a specific dataset (note: columns can be made case-sensitive, and a default value can be set for columns).    C7 - Ensure only authorized IAM entities are allowed to access the tables, views, and table data in each dataset.    C84 - Prevent the unauthorized access/creation/modification/deletion of BigQuery resources (e.g., datasets, tables) (e.g., by using an IAM policy with an allow/deny statement on "bigquery.tables.\*" and/or "bigquery.datasets.\*" with the tags and the authorized value for the conditions "resource.type" = "authorized type", "resource.name" = "authorized name"). | Very High | 3 | 1 | - |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO8 - Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings**    C81 - Define the authorized configuration (i.e., schema, clustering, expirationTime, view, materializedView, externalDataConfiguration, encryptionConfiguration, defaultCollation, defaultRoundingMode, and tableConstraints) for each BigQuery table.    C82 - Ensure the configuration of each BigQuery table is authorized. | Very High | 2 | - | - |
| **CO16 - Monitor data protection, data ingestion, and data quality**    C42 - Monitor the abnormal number of concurrent connections and throughput for the BigQuery table (e.g., by using the Monitoring metric CONSUMER QUOTA - QUOTA LIMIT). | Very Low | - | - | 1 |

#### Exfiltration of query results to an unauthorized destination table and bucket

| | **Threat Id** | Bigquery.T20 | | --- | --- | | **Name** | Exfiltration of query results to an unauthorized destination table and bucket | | **Description** | An asynchronous job can be created, which can include various types of jobs such as query jobs, load jobs, copy jobs, and extract jobs. An attacker can execute an unauthorized query, provide an unauthorized destination table or bucket to store query results, overwrite the destination table, update the schema for the destination table, encrypt data using the DLP function with an unauthorized key, or change the encryption of the destination table. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Medium (4.8)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:L/A:N) | | **IAM Access** | {  "AND": ["bigquery.jobs.create", {  "OPTIONAL": "bigquery.tables.getData"  }]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO8 - Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings**    C75 - Define the authorized configuration (e.g., createDisposition, writeDisposition, schemaUpdateOptions) for each asynchronous query job.    C76 - Ensure the configuration of each asynchronous query job is authorized. | Very High | 2 | - | - |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO10 - Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings**    C22 - Maintain a list of authorized sources and destinations (e.g., Cloud Storage, BigQuery, Vertex AI (for LLM, via BigQuery connection only)) to be used with each dataset, table, model, connection, job, and listing.    C23 - Ensure each dataset, table, model, connection, job, and listing uses authorized sources and destinations. | High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO7 - Encrypt resources (e.g., datasets, models, data transfers) with customer-managed encryption keys and protect the keys**    C26 - Maintain a list of authorized CMEKs to be used with each BigQuery resource (e.g., dataset, DLP function, model, data transfer), ideally dedicated (e.g., using Autokey on bigquery.googleapis.com/Dataset), and of the default CMEK at the project or organization level, and define the requirement to rotate key versions for tables.    C27 - Ensure only authorized CMEKs and their versions are used with the BigQuery resource.    C28 - Protect the CMEKs used by each BigQuery resource using the Cloud KMS ThreatModel (including enforcing CMEK protection using organization policy constraints/gcp.restrictCmekCryptoKeyProjects and constraints/gcp.restrictNonCmekServices as per Cloudkms.C32 and Cloudkms.C34).    C85 - Define the requirements for generating, storing, accessing, distributing, rotating, backing up, and destroying encryption keys for applications (e.g., by using a dedicated secret management tool such as HashiCorp Vault or GCP Secret Manager) as per the security standards.    C86 - Ensure the keys for applications are generated, stored, accessed, distributed, rotated, backed up, and destroyed as per the security standards. | High | 5 | - | - |
| **CO16 - Monitor data protection, data ingestion, and data quality**    C87 - Establish, document, and train on procedures for responding to key compromise events, including key leaks and unapproved access. Implement a key revocation process to invalidate compromised keys and replace them with new, secure keys. | Low | 1 | - | - |

#### Disruption of application functionality by modification of table and view configurations

| | **Threat Id** | Bigquery.T11 | | --- | --- | | **Name** | Disruption of application functionality by modification of table and view configurations | | **Description** | Specific properties are associated with tables and views during their creation. An attacker can modify these properties (e.g., schema, expiration time, encryption key), causing downstream applications' disruption or permanent data loss. | | **Goal** | Disruption of Service | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (4.8)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H) | | **IAM Access** | {  "UNIQUE": "bigquery.tables.update"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO8 - Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings**    C17 - Define the authorized configuration (i.e., defaultTableExpirationMs, defaultPartitionExpirationMs, defaultEncryptionConfiguration, linkedDatasetSource, externalDatasetReference, defaultCollation, defaultRoundingMode, maxTimeTravelHours, storageBillingModel, and defaultEncryptionConfiguration) for each BigQuery dataset.    C18 - Ensure the configuration of each BigQuery dataset is authorized. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel.    C6 - Maintain a list of authorized IAM entities allowed to access the tables, views, and table data in a specific dataset (note: columns can be made case-sensitive, and a default value can be set for columns).    C7 - Ensure only authorized IAM entities are allowed to access the tables, views, and table data in each dataset. | High | 3 | - | - |
| **CO12 - Set the expiration time of BigQuery tables as per the requirements**    C32 - Define the requirements for the expiration time of each BigQuery table.    C33 - Ensure the expiration time of each BigQuery table is set according to the requirements. | High | 2 | - | - |
| **CO7 - Encrypt resources (e.g., datasets, models, data transfers) with customer-managed encryption keys and protect the keys**    C26 - Maintain a list of authorized CMEKs to be used with each BigQuery resource (e.g., dataset, DLP function, model, data transfer), ideally dedicated (e.g., using Autokey on bigquery.googleapis.com/Dataset), and of the default CMEK at the project or organization level, and define the requirement to rotate key versions for tables.    C27 - Ensure only authorized CMEKs and their versions are used with the BigQuery resource.    C28 - Protect the CMEKs used by each BigQuery resource using the Cloud KMS ThreatModel (including enforcing CMEK protection using organization policy constraints/gcp.restrictCmekCryptoKeyProjects and constraints/gcp.restrictNonCmekServices as per Cloudkms.C32 and Cloudkms.C34).    C36 - Ensure [AEAD encryption functions](https://docs.cloud.google.com/bigquery/docs/column-key-encrypt) are used to encrypt data at the column level. | High | 4 | - | - |

#### Table exfiltration by cloning

| | **Threat Id** | Bigquery.T19 | | --- | --- | | **Name** | Table exfiltration by cloning | | **Description** | A table clone is a writable copy of another table. It can be created in another project within the same region. An attacker can clone a table to an unauthorized project to exfiltrate data. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Medium (4.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N) | | **IAM Access** | {  "UNIQUE": "bigquery.jobs.create"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO19 - Enforce authorized configurations on jobs**    C53 - Define the authorized configuration for each job.    C54 - Ensure each job uses an authorized configuration. | Medium | 2 | - | - |
| **CO18 - Limit the amount of cloned data**    C50 - Define the requirements for setting the time travel of each BigQuery dataset.    C51 - Ensure the time travel of each BigQuery dataset is set according to its requirements. | Low | 2 | - | - |

#### Exfiltration of data by exporting tables to other services

| | **Threat Id** | Bigquery.T6 | | --- | --- | | **Name** | Exfiltration of data by exporting tables to other services | | **Description** | Data can be sent to other services for storing or processing. An attacker can export data to either their destination table or a service like Cloud Storage, Data Studio, or DLP. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Medium (4.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N) | | **IAM Access** | {  "AND": [{  "OPTIONAL": {  "AND": ["storage.objects.create", "storage.objects.delete"]  }  }, "bigquery.tables.export", "bigquery.jobs.create", "bigquery.tables.getData"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel.    C6 - Maintain a list of authorized IAM entities allowed to access the tables, views, and table data in a specific dataset (note: columns can be made case-sensitive, and a default value can be set for columns).    C7 - Ensure only authorized IAM entities are allowed to access the tables, views, and table data in each dataset. | High | 3 | - | - |
| **CO10 - Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings**    C22 - Maintain a list of authorized sources and destinations (e.g., Cloud Storage, BigQuery, Vertex AI (for LLM, via BigQuery connection only)) to be used with each dataset, table, model, connection, job, and listing.    C23 - Ensure each dataset, table, model, connection, job, and listing uses authorized sources and destinations.    C25 - Protect the sources and destinations used by each table, model, connection, job, and listing, using their respective services' ThreatModels. | High | 3 | - | - |
| **CO5 - Restrict access to columns and protect sensitive data**    C9 - Define the criteria for the sensitivity of columns in each table and each view, and their requirements for data protection (e.g., using BigQuery column-level security, column-level data masking, custom masking routines, restriction analysis rules, list overlap analysis rules, aggregation threshold analysis rules, differential privacy clauses, or data clean rooms).    C10 - Ensure only authorized IAM entities are allowed to access sensitive columns of tables and views. | High | 2 | - | - |
| **CO6 - Restrict access to rows with BigQuery row-level security**    C12 - Define the criteria for the sensitivity of rows in each table.    C13 - Ensure only authorized IAM entities are allowed to access sensitive rows of a table (e.g., using BigQuery row-level security). | High | 2 | - | - |
| **CO9 - De-identify sensitive data using Cloud DLP**    C20 - Ensure sensitive data is identified and redacted (e.g., using Cloud DLP). | Medium | 1 | - | - |

#### Restricting access to resources by modifying privileges

| | **Threat Id** | Bigquery.T10 | | --- | --- | | **Name** | Restricting access to resources by modifying privileges | | **Description** | IAM permissions can be used to allow users to perform actions on BigQuery resources (i.e., datasets, tables, connections, reservations, and assignments). An attacker can limit legitimate users' access to resources or allow unauthorized users to access resources by modifying the permissions. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0004](https://attack.mitre.org/tactics/TA0004) | | **CVSS** | [Medium (4.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N) | | **IAM Access** | {  "OR": ["bigquery.datasets.setIamPolicy", "bigquery.rowAccessPolicies.setIamPolicy", "bigquery.tables.setIamPolicy", "bigquery.connections.setIamPolicy", "bigquery.rowAccessPolicies.update", "bigqueryreservation.reservations.setIamPolicy"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |

#### Destruction of data by deleting dataset or table

| | **Threat Id** | Bigquery.T1 | | --- | --- | | **Name** | Destruction of data by deleting dataset or table | | **Description** | A dataset is a container that holds tables and other datasets, and a table is a collection of rows and columns within a dataset, where the actual data is stored and queried. All tables within the dataset, before deletion, must be deleted either manually or by setting the deleteContents parameter to true. An attacker can delete the table or a dataset, causing a permanent loss of data. | | **Goal** | Disruption of Service | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Low (3.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L) | | **IAM Access** | {  "AND": ["bigquery.tables.delete", {  "OPTIONAL": "bigquery.datasets.delete"  }]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel.    C84 - Prevent the unauthorized access/creation/modification/deletion of BigQuery resources (e.g., datasets, tables) (e.g., by using an IAM policy with an allow/deny statement on "bigquery.tables.\*" and/or "bigquery.datasets.\*" with the tags and the authorized value for the conditions "resource.type" = "authorized type", "resource.name" = "authorized name"). | Very High | 1 | 1 | - |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO8 - Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings**    C81 - Define the authorized configuration (i.e., schema, clustering, expirationTime, view, materializedView, externalDataConfiguration, encryptionConfiguration, defaultCollation, defaultRoundingMode, and tableConstraints) for each BigQuery table.    C82 - Ensure the configuration of each BigQuery table is authorized. | Very High | 2 | - | - |
| **CO3 - Ensure backup, failover, and recovery capabilities for BigQuery resources (e.g., snapshots and exports for datasets and tables, failover procedures for reservations)**    C3 - Define the requirements for the backup of each BigQuery dataset, table, and model.    C4 - Ensure each BigQuery dataset, table, and model is backed up (e.g., by creating snapshots or exports) according to the requirements and is restorable. | Medium | 2 | - | - |

#### Denial of Service via unauthorized continuous query cancellation

| | **Threat Id** | Bigquery.T34 | | --- | --- | | **Name** | Denial of Service via unauthorized continuous query cancellation | | **Description** | Continuous queries in BigQuery can be long-lived jobs that perform real-time analytics, ML inference, or replication into downstream systems. An attacker can disrupt these pipelines by continuously canceling active queries, causing loss of analytics, halting data replication, and triggering operational downtime for dependent applications. | | **Goal** | Disruption of Service | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Low (2.4)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L) | | **IAM Access** | {  "UNIQUE": "bigquery.jobs.update"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |

#### Expose sensitive data via auto-enabled Gemini API

| | **Threat Id** | Bigquery.T35 | | --- | --- | | **Name** | Expose sensitive data via auto-enabled Gemini API | | **Description** | The Gemini for Google Cloud API is enabled by default in BigQuery projects linked to accounts based in supported locations unless explicitly opted out. An attacker can exploit Gemini integrations to prompt, extract, or process sensitive data outside BigQuery via AI features without clear user awareness or guardrails. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Low (2.4)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N) | | **IAM Access** | {  "AND": ["bigquery.jobs.create", "bigquery.tables.getData", "cloudaicompanion.entitlements.get"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO34 - Restrict and manage Gemini in BigQuery projects**    C126 - Ensure the Cloud AI Companion API is enabled/disabled for the BigQuery project following the Service Usage ThreatModel and is protected using Cloud AI Companion ThreatModel.    C127 - Maintain the list of authorized BigQuery projects allowed to use Gemini.    C128 - Ensure only authorized BigQuery projects are allowed to use Gemini. | High | 3 | - | - |

#### Unauthorized access to cached data from the last 24 hours

| | **Threat Id** | Bigquery.T26 | | --- | --- | | **Name** | Unauthorized access to cached data from the last 24 hours | | **Description** | Users can read the contents of tables within BigQuery, enabling them to query and retrieve data stored in specific tables. Results from queries against table snapshots can also be returned from the [cache](https://docs.cloud.google.com/bigquery/docs/cached-results#security), even if the caller loses access to the data within the last 24 hours. An attacker can retrieve data from BigQuery tables or access the query results from the cache without making any new queries. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Low (2.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N) | | **IAM Access** | {  "AND": ["bigquery.tables.getData", {  "OPTIONAL": "datacatalog.categories.fineGrainedGet"  }]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO5 - Restrict access to columns and protect sensitive data**    C9 - Define the criteria for the sensitivity of columns in each table and each view, and their requirements for data protection (e.g., using BigQuery column-level security, column-level data masking, custom masking routines, restriction analysis rules, list overlap analysis rules, aggregation threshold analysis rules, differential privacy clauses, or data clean rooms).    C10 - Ensure only authorized IAM entities are allowed to access sensitive columns of tables and views. | High | 2 | - | - |
| **CO19 - Enforce authorized configurations on jobs**    C53 - Define the authorized configuration for each job.    C54 - Ensure each job uses an authorized configuration. | Medium | 2 | - | - |

| Routines (stored procedures or User-Defined Functions) *(subclass of Dataset and tables, FC2)* *A stored procedure is a set of statements that can be invoked by other queries or stored procedures. A User-Defined Function (UDF) lets you create a function by using an SQL expression or JavaScript code. A UDF accepts columns of input, performs actions on the input, and returns the results of those actions as values.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Creates a new routine in the dataset. | bigquery.routines.create |  Threat List  | **Name** | **CVSS** | | --- | --- | | Loss of integrity and availability by manipulating data using routines | [Medium (5.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:L) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Loss of integrity and availability by manipulating data using routines

| | **Threat Id** | Bigquery.T8 | | --- | --- | | **Name** | Loss of integrity and availability by manipulating data using routines | | **Description** | Routines (stored procedures and UDFs) allow the creation of functions using an SQL expression or JavaScript code. They accept columns of input, perform actions on the input, and return the result of those actions as a value. An attacker can write routines to perform actions like updating, deleting, and adding data to the tables. An attacker can also execute UDFs (User-Defined Functions) from unauthorized Cloud Storage for such purposes. | | **Goal** | Data manipulation | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (5.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:L) | | **IAM Access** | {  "AND": ["bigquery.routines.create", "bigquery.jobs.create"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO8 - Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings**    C15 - Ensure no dataset is accessible to "AllUsers" or "AllAuthenticatedUsers", except if allowed.    C17 - Define the authorized configuration (i.e., defaultTableExpirationMs, defaultPartitionExpirationMs, defaultEncryptionConfiguration, linkedDatasetSource, externalDatasetReference, defaultCollation, defaultRoundingMode, maxTimeTravelHours, storageBillingModel, and defaultEncryptionConfiguration) for each BigQuery dataset.    C18 - Ensure the configuration of each BigQuery dataset is authorized. | Very High | 3 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel.    C6 - Maintain a list of authorized IAM entities allowed to access the tables, views, and table data in a specific dataset (note: columns can be made case-sensitive, and a default value can be set for columns).    C7 - Ensure only authorized IAM entities are allowed to access the tables, views, and table data in each dataset. | High | 3 | - | - |
| **CO23 - Use authorized User-Defined Functions**    C70 - Maintain a list of authorized Cloud Storage buckets to be used with query jobs for User-Defined Functions (UDFs).    C71 - Ensure each query uses an authorized Cloud Storage bucket for a UDF.    C73 - Protect the Cloud Storage buckets used for storing UDFs using Cloud Storage ThreatModel. | High | 3 | - | - |
| **CO24 - Enforce secure SDLC processes on routines and queries**    C74 - Enforce secure SDLC processes on routines (e.g., using source control, static analysis, dynamic analysis, peer review). | High | 1 | - | - |
| **CO5 - Restrict access to columns and protect sensitive data**    C9 - Define the criteria for the sensitivity of columns in each table and each view, and their requirements for data protection (e.g., using BigQuery column-level security, column-level data masking, custom masking routines, restriction analysis rules, list overlap analysis rules, aggregation threshold analysis rules, differential privacy clauses, or data clean rooms).    C10 - Ensure only authorized IAM entities are allowed to access sensitive columns of tables and views. | High | 2 | - | - |
| **CO6 - Restrict access to rows with BigQuery row-level security**    C12 - Define the criteria for the sensitivity of rows in each table.    C13 - Ensure only authorized IAM entities are allowed to access sensitive rows of a table (e.g., using BigQuery row-level security). | High | 2 | - | - |

| BigQuery connections and BigQuery Omni *(subclass of Dataset and tables, FC3)* *To create a connection for federated queries when adding data from external data sources or exporting data to cross Cloud Storages.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Creates a new connection. | bigquery.connections.create |  Threat List  | **Name** | **CVSS** | | --- | --- | | Unauthorized access to data by changing connection configurations | [Medium (5.7)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:N) | | Data exfiltration by exporting query results | [Medium (4.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Unauthorized access to data by changing connection configurations

| | **Threat Id** | Bigquery.T2 | | --- | --- | | **Name** | Unauthorized access to data by changing connection configurations | | **Description** | BigQuery federations enable BigQuery to query data residing in Cloud SQL or other places in real-time, without copying or moving data. For each federation, a connection is created. An attacker can use an existing connection by viewing the connection list or sharing it with another user to get unauthorized access to tables residing in other sources. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0001](https://attack.mitre.org/tactics/TA0001) | | **CVSS** | [Medium (5.7)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:N) | | **IAM Access** | {  "OR": ["bigquery.connections.update", "bigquery.connections.get", "bigquery.connections.list", "bigquery.connections.use", "bigquery.connections.setIamPolicy"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel.    C6 - Maintain a list of authorized IAM entities allowed to access the tables, views, and table data in a specific dataset (note: columns can be made case-sensitive, and a default value can be set for columns).    C7 - Ensure only authorized IAM entities are allowed to access the tables, views, and table data in each dataset. | High | 3 | - | - |
| **CO10 - Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings**    C22 - Maintain a list of authorized sources and destinations (e.g., Cloud Storage, BigQuery, Vertex AI (for LLM, via BigQuery connection only)) to be used with each dataset, table, model, connection, job, and listing.    C23 - Ensure each dataset, table, model, connection, job, and listing uses authorized sources and destinations.    C25 - Protect the sources and destinations used by each table, model, connection, job, and listing, using their respective services' ThreatModels. | High | 3 | - | - |
| **CO5 - Restrict access to columns and protect sensitive data**    C9 - Define the criteria for the sensitivity of columns in each table and each view, and their requirements for data protection (e.g., using BigQuery column-level security, column-level data masking, custom masking routines, restriction analysis rules, list overlap analysis rules, aggregation threshold analysis rules, differential privacy clauses, or data clean rooms).    C10 - Ensure only authorized IAM entities are allowed to access sensitive columns of tables and views.    C44 - Define the criteria to use authorized data policies for each column in each table.    C45 - Ensure only authorized IAM entities are allowed to access sensitive columns of a table by using data policies. | High | 4 | - | - |
| **CO6 - Restrict access to rows with BigQuery row-level security**    C12 - Define the criteria for the sensitivity of rows in each table.    C13 - Ensure only authorized IAM entities are allowed to access sensitive rows of a table (e.g., using BigQuery row-level security). | High | 2 | - | - |

#### Data exfiltration by exporting query results

| | **Threat Id** | Bigquery.T15 | | --- | --- | | **Name** | Data exfiltration by exporting query results | | **Description** | BigQuery Omni uses BigQuery connections to export query results to GCP services (e.g., Spanner, BigTable, and Cloud Storage), Amazon S3, or Azure Storage. An attacker can create a connection to export query results to their GCP services, Amazon S3, or Azure Storage to exfiltrate data. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Medium (4.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N) | | **IAM Access** | {  "AND": ["bigquery.connections.create", "bigquery.jobs.create", "bigquery.tables.getData", "bigquery.tables.export", "bigquery.connections.use"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO14 - Limit use of BigQuery Omni**    C38 - Define the requirements for using BigQuery Omni (AWS and/or Azure).    C39 - Ensure the use of BigQuery Omni as per the requirements (e.g., using organizational constraints [constraints/bigquery.disableBQOmniAWS](https://docs.cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints) and [constraints/bigquery.disableBQOmniAzure](https://docs.cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints)). | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO10 - Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings**    C22 - Maintain a list of authorized sources and destinations (e.g., Cloud Storage, BigQuery, Vertex AI (for LLM, via BigQuery connection only)) to be used with each dataset, table, model, connection, job, and listing.    C23 - Ensure each dataset, table, model, connection, job, and listing uses authorized sources and destinations.    C25 - Protect the sources and destinations used by each table, model, connection, job, and listing, using their respective services' ThreatModels. | High | 3 | - | - |

| BigQuery Data Transfer *(subclass of Dataset and tables, FC4)* *You can transfer external data from SaaS applications to Google BigQuery on a regular basis.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Creates a new data transfer configuration. | bigquery.transfers.update |  Threat List  | **Name** | **CVSS** | | --- | --- | | Data exfiltration by updating the destination dataset in transfer and transfer credentials; or DoS by schedule manipulation | [Medium (5.7)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:L) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Data exfiltration by updating the destination dataset in transfer and transfer credentials; or DoS by schedule manipulation

| | **Threat Id** | Bigquery.T13 | | --- | --- | | **Name** | Data exfiltration by updating the destination dataset in transfer and transfer credentials; or DoS by schedule manipulation | | **Description** | The BigQuery Data Transfer Service automates data movement into BigQuery on a scheduled, managed basis using the credentials of the provided service account or the user who created or updated it. An attacker can create or update the destination dataset or transfer credentials or transfer job configuration to point to their own dataset, giving them full control over the transfer for exfiltration, create transfers of data from unauthorized sources to cause data poisoning, or modify ingestions (via schedule changes, disabling a config, altering refresh windows, creating transfers with an unauthorized encryption key), leading to Denial of Service. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Medium (5.7)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:L) | | **IAM Access** | {  "AND": ["bigquery.transfers.update", "bigquery.datasets.get", "bigquery.datasets.update", {  "OPTIONAL": {  "AND": ["bigquery.datasets.setIamPolicy", "bigquery.datasets.getIamPolicy"]  }  }]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO22 - Secure and use the authorized sources and their respective authorized configurations with BigQuery Data Transfer**    C66 - Maintain a list of authorized sources (e.g., Cloud Storage, Amazon S3, Oracle, Salesforce) and their respective authorized configurations (i.e., destination dataset, schedule, config status, encryption key, parameters) to be used with each transfer.    C67 - Ensure each transfer uses an authorized source and its authorized configuration.    C69 - Protect the sources used with each transfer, using the respective service's ThreatModel.    C119 - Prevent the creation/update of a transfer without an authorized source and/or destination (e.g., using a custom constraint resourceType:[bigquerydatatransfer.googleapis.com/TransferConfig](https://docs.cloud.google.com/bigquery/docs/transfer-custom-constraints#supported_resources), resource(s): resource.dataSourceId != an authorized data source, resource.destinationDatasetId != an authorized dataset, methodTypes="UPDATE" and "CREATE", and actionType="DENY").    C120 - Prevent the create/update of a transfer without an authorized ingestion (i.e., schedule, refresh window, and status of transfer configuration) (e.g., using a custom constraint resourceType:[bigquerydatatransfer.googleapis.com/TransferConfig](https://docs.cloud.google.com/bigquery/docs/transfer-custom-constraints#supported_resources), resource(s): resource.dataRefreshWindowDays != authorized data refresh window, resource.disabled != authorized config status, resource.emailPreferences.enableFailureEmail != authorized failure email status, resource.encryptionConfiguration.kmsKeyName != authorized KMS key, resource.schedule != authorized schedule, resource.scheduleOptions.disableAutoScheduling != authorized autoscheduling status, resource.scheduleOptions.endTime != authorized end time, resource.scheduleOptions.startTime != authorized start time, resource.scheduleOptionsV2.timeBasedSchedule.endTime != authorized end time, resource.scheduleOptionsV2.timeBasedSchedule.schedule != authorized schedule, resource.scheduleOptionsV2.timeBasedSchedule.startTime != authorized start time, resource.scheduleOptionsV2.eventDrivenSchedule.pubsubSubscription != authorized Pub/Sub subscription, resource.notificationPubsubTopic != authorized Pub/Sub topic, methodTypes="UPDATE" and "CREATE", and actionType="DENY").    C137 - Protect the network attachments used with private database sources, using the Compute Engine ThreatModel. | High | 4 | 2 | - |
| **CO15 - Enable logs for BigQuery Data Transfer**    C41 - Ensure Cloud Audit Logs for BigQuery Data Transfer are enabled ([ref](https://docs.cloud.google.com/bigquery-transfer/docs/audit-logging)).    C88 - Monitor the creation/modification of unauthorized data transfers (e.g., by using Cloud Logging events "google.cloud.bigquery.datatransfer.v1.DataTransferService.CreateTransferConfig" and "google.cloud.bigquery.datatransfer.v1.DataTransferService.UpdateTransferConfig" and their fields request.serviceAccountName, request.transferConfig.dataSourceId, request.transferConfig.destinationDatasetId, request.transferConfig.emailPreferences, request.transferConfig.notificationPubsubTopic, and request.transferConfig.schedule). | Medium | 1 | - | 1 |
| **CO33 - Define and enforce BigQuery configuration baselines at the organization and project levels**    C123 - Maintain the list of authorized configuration settings (e.g., default\_batch\_query\_queue\_timeout\_ms, default\_interactive\_query\_queue\_timeout\_ms, default\_query\_job\_timeout\_ms, enable\_fine\_grained\_dataset\_acls\_option) for each organization or project.    C124 - Ensure only authorized configuration settings for each organization or project are configured. | Medium | 2 | - | - |

| BigQuery reservation *(subclass of Dataset and tables, FC5)* *BI Engine allows you to analyze data stored in BigQuery with sub-second query response time and high concurrency, using BI reservations.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Creates a new reservation resource. | bigquery.reservations.create |  Threat List  | **Name** | **CVSS** | | --- | --- | | Denial of Service/Denial of Wallet by removing/creating reservations | [Medium (4.8)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H) | | Data corruption via unauthorized hard failover | [Low (2.4)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Denial of Service/Denial of Wallet by removing/creating reservations

| | **Threat Id** | Bigquery.T12 | | --- | --- | | **Name** | Denial of Service/Denial of Wallet by removing/creating reservations | | **Description** | A slot is a dedicated vCPU that runs queries. Each slot is allocated to a reservation. An attacker can remove a reservation, failing any jobs that are currently executing with slots from that reservation, which may decrease the performance for future jobs, create a reservation with unauthorized configurations, modify an existing reservation to achieve the same objective, or incur additional costs by changing the assignee. | | **Goal** | Disruption of Service | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (4.8)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H) | | **IAM Access** | {  "OR": [{  "AND": ["bigquery.reservations.delete", "bigquery.reservationAssignments.delete"]  }, {  "AND": [{  "OR": ["bigquery.reservationAssignments.create", "bigquery.reservationAssignments.update"]  }, {  "OR": ["bigquery.reservations.create", "bigquery.reservations.update"]  }]  }]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel.    C84 - Prevent the unauthorized access/creation/modification/deletion of BigQuery resources (e.g., datasets, tables) (e.g., by using an IAM policy with an allow/deny statement on "bigquery.tables.\*" and/or "bigquery.datasets.\*" with the tags and the authorized value for the conditions "resource.type" = "authorized type", "resource.name" = "authorized name"). | Very High | 1 | 1 | - |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO8 - Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings**    C60 - Define the authorized configuration for each reservation (i.e., maxSlots, edition, ignoreIdleSlots, autoscale, secondaryLocation) and its assignments (i.e., assignee, jobType).    C61 - Ensure each reservation and its assignments use an authorized configuration.    C63 - Monitor the creation/modification of unauthorized reservations (e.g., by using Cloud Logging event "google.cloud.bigquery.reservation.v1.ReservationService.CreateReservation" and "google.cloud.bigquery.reservation.v1.ReservationService.UpdateReservation", and their fields request.reservation.autoscale.maxSlots and request.reservation.edition).    C64 - Monitor the creation/modification of unauthorized assignments (e.g., by using Cloud Logging event "google.cloud.bigquery.reservation.v1.ReservationService.CreateAssignment" and its fields request.assignment.assignee, request.assignment.jobType, and request.parent, and event "google.cloud.bigquery.reservation.v1.ReservationService.UpdateAssignment" and its fields request.assignment.assignee and request.assignment.jobType). | Very High | 2 | - | 2 |
| **CO13 - Monitor BigQuery capacity and utilization**    C35 - Monitor slot consumption (e.g., using slot recommender), job concurrency, job execution time, job errors, and bytes processed across the entire organization (e.g., using BigQuery Admin Resource Charts).    C43 - Monitor slot capacity (e.g., using the slot estimator) to estimate the correct number of slots for the BigQuery workload. | Medium | - | - | 2 |

#### Data corruption via unauthorized hard failover

| | **Threat Id** | Bigquery.T36 | | --- | --- | | **Name** | Data corruption via unauthorized hard failover | | **Description** | Users can promote a BigQuery reservation's secondary region to primary, with options for soft or hard failover. An attacker can initiate a hard failover without waiting for full data replication, resulting in some data corruption. | | **Goal** | Data manipulation | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Low (2.4)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N) | | **IAM Access** | {  "UNIQUE": "bigquery.reservations.update"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO14 - Limit use of BigQuery Omni**    C38 - Define the requirements for using BigQuery Omni (AWS and/or Azure).    C39 - Ensure the use of BigQuery Omni as per the requirements (e.g., using organizational constraints [constraints/bigquery.disableBQOmniAWS](https://docs.cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints) and [constraints/bigquery.disableBQOmniAzure](https://docs.cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints)). | Very High | 2 | - | - |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO3 - Ensure backup, failover, and recovery capabilities for BigQuery resources (e.g., snapshots and exports for datasets and tables, failover procedures for reservations)**    C130 - Define the failover process (e.g., use soft failover mode by default, document the justification for any hard failover, require approval for exceptions, record the chosen failover mode in the change process, validate replication status) for reservations.    C131 - Ensure a reservation is failed over according to the process.    C132 - Monitor the failover mode of a reservation (e.g., by using Cloud Logging event "google.cloud.bigquery.reservation.v1.ReservationService.FailoverReservation" and its field request.failoverMode). | High | 2 | - | 1 |

| BigQuery ML *(subclass of Dataset and tables, FC6)* *You can create and execute machine-learning models in BigQuery using standard SQL queries.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Create new models. | bigquery.models.create |  Threat List  | **Name** | **CVSS** | | --- | --- | | BigQuery ML model exfiltration | [Medium (4.8)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:L/A:N) | | Importing malicious models in BigQuery | [Medium (4.7)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:L) | | Loss of the integrity of the training model | [Medium (4.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N) | | Permanent loss of a BigQuery ML model by modifying its expiration time | [Medium (4.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### BigQuery ML model exfiltration

| | **Threat Id** | Bigquery.T18 | | --- | --- | | **Name** | BigQuery ML model exfiltration | | **Description** | BigQuery ML models can be integrated with the Vertex AI Model Registry for management purposes and exported to Cloud Storage. An attacker can register an existing model with their Vertex AI Model Registry or export it to unauthorized Cloud Storage to exfiltrate the model. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Medium (4.8)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:L/A:N) | | **IAM Access** | {  "AND": ["bigquery.jobs.create", {  "OR": ["bigquery.models.updateData", "bigquery.models.export"]  }]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO10 - Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings**    C22 - Maintain a list of authorized sources and destinations (e.g., Cloud Storage, BigQuery, Vertex AI (for LLM, via BigQuery connection only)) to be used with each dataset, table, model, connection, job, and listing.    C23 - Ensure each dataset, table, model, connection, job, and listing uses authorized sources and destinations. | High | 2 | - | - |
| **CO17 - Register BigQuery models as per the requirements**    C47 - Define the requirements to register the BigQuery models with the Vertex AI Model Registry for each BigQuery model.    C48 - Ensure each BigQuery model is registered with the Vertex AI Model Registry according to its requirements. | Medium | 2 | - | - |

#### Importing malicious models in BigQuery

| | **Threat Id** | Bigquery.T24 | | --- | --- | | **Name** | Importing malicious models in BigQuery | | **Description** | Models can be imported from Cloud Storage buckets into BigQuery. An attacker can import a malicious or unauthorized model into BigQuery to perform harmful actions within BigQuery, affecting the integrity of the system, causing disruptions, potentially accessing and manipulating sensitive data within BigQuery, or misusing resources, such as excessive consumption of computing resources. | | **Goal** | Disruption of Service | | **MITRE ATT&CK®** | [TA0002](https://attack.mitre.org/tactics/TA0002) | | **CVSS** | [Medium (4.7)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:L) | | **IAM Access** | {  "AND": ["bigquery.jobs.create", "storage.objects.get", "bigquery.models.create"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO10 - Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings**    C22 - Maintain a list of authorized sources and destinations (e.g., Cloud Storage, BigQuery, Vertex AI (for LLM, via BigQuery connection only)) to be used with each dataset, table, model, connection, job, and listing.    C23 - Ensure each dataset, table, model, connection, job, and listing uses authorized sources and destinations. | High | 2 | - | - |

#### Loss of the integrity of the training model

| | **Threat Id** | Bigquery.T4 | | --- | --- | | **Name** | Loss of the integrity of the training model | | **Description** | ML models are trained on data, and the accuracy of a model depends on the quantity and quality of the training data. The training data is stored in the form of tables or views. An attacker can decrease the quality of a model by adding bogus data to tables and views or by removing data from them, thereby decreasing the effectiveness of the resulting model and harming business decisions based on predictions from this model. | | **Goal** | Data manipulation | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (4.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:N) | | **IAM Access** | {  "AND": ["bigquery.jobs.create", {  "OR": ["bigquery.models.updateData", "bigquery.models.updateMetadata"]  }]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO26 - Use fingerprinting for ML models to ensure their integrity**    C89 - Define the requirements for generating, embedding, storing, accessing, updating, revoking, and destroying fingerprints for ML models as per the security requirements.    C90 - Ensure the fingerprints for ML models are generated, embedded, stored, accessed, updated, revoked, and destroyed as per the security requirements. | High | 2 | - | - |
| **CO16 - Monitor data protection, data ingestion, and data quality**    C42 - Monitor the abnormal number of concurrent connections and throughput for the BigQuery table (e.g., by using the Monitoring metric CONSUMER QUOTA - QUOTA LIMIT).    C65 - Monitor the quality of data used with the ML models (e.g., by [data profiling](https://docs.cloud.google.com/bigquery/docs/data-profile-scan)). | Low | - | - | 2 |

#### Permanent loss of a BigQuery ML model by modifying its expiration time

| | **Threat Id** | Bigquery.T22 | | --- | --- | | **Name** | Permanent loss of a BigQuery ML model by modifying its expiration time | | **Description** | A model's expiration time in BigQuery determines when it will be automatically deleted, serving as its "time to live" (TTL), and can also be adjusted after the model has been created. An attacker can update the expiration time of a model to cause its permanent loss. | | **Goal** | Disruption of Service | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (4.1)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H) | | **IAM Access** | {  "UNIQUE": "bigquery.models.updateMetadata"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO25 - Set an authorized expiration time for each ML model**    C78 - Define the authorized expiration time for each ML model.    C79 - Ensure the expiration time for each ML model is authorized. | Medium | 2 | - | - |
| **CO3 - Ensure backup, failover, and recovery capabilities for BigQuery resources (e.g., snapshots and exports for datasets and tables, failover procedures for reservations)**    C3 - Define the requirements for the backup of each BigQuery dataset, table, and model.    C4 - Ensure each BigQuery dataset, table, and model is backed up (e.g., by creating snapshots or exports) according to the requirements and is restorable. | Medium | 2 | - | - |

| Table snapshot *(subclass of Dataset and tables, FC7)* *A BigQuery table snapshot preserves the contents of a table (called the base table) at a particular time. You can save a snapshot of a current table or create a snapshot of a table as it was at any time in the past seven days.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Create new table snapshots. | bigquery.tables.createSnapshot |  Threat List  | **Name** | **CVSS** | | --- | --- | | Loss of data integrity by restoring a snapshot | [Medium (5.7)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H) | | Loss of data during recovery by deleting a snapshot | [Medium (4.3)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:N) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Loss of data integrity by restoring a snapshot

| | **Threat Id** | Bigquery.T27 | | --- | --- | | **Name** | Loss of data integrity by restoring a snapshot | | **Description** | Snapshots are created to preserve the contents of a table at a specific time. These can be used to restore data to an existing table or a new table. An attacker can overwrite the contents of an existing table by restoring a snapshot to it. | | **Goal** | Data manipulation | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (5.7)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H) | | **IAM Access** | {  "AND": ["bigquery.jobs.create", "bigquery.tables.restoreSnapshot", "bigquery.tables.getData", "bigquery.tables.updateData", "bigquery.tables.update", {  "OPTIONAL": "bigquery.tables.create"  }]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO3 - Ensure backup, failover, and recovery capabilities for BigQuery resources (e.g., snapshots and exports for datasets and tables, failover procedures for reservations)**    C3 - Define the requirements for the backup of each BigQuery dataset, table, and model.    C4 - Ensure each BigQuery dataset, table, and model is backed up (e.g., by creating snapshots or exports) according to the requirements and is restorable. | Medium | 2 | - | - |

#### Loss of data during recovery by deleting a snapshot

| | **Threat Id** | Bigquery.T14 | | --- | --- | | **Name** | Loss of data during recovery by deleting a snapshot | | **Description** | Snapshots can be used to restore previous data. An attacker (or someone by negligence) can delete snapshots to block data recovery. | | **Goal** | Data manipulation | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Medium (4.3)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:U/C:N/I:H/A:N) | | **IAM Access** | {  "UNIQUE": "bigquery.tables.deleteSnapshot"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO3 - Ensure backup, failover, and recovery capabilities for BigQuery resources (e.g., snapshots and exports for datasets and tables, failover procedures for reservations)**    C3 - Define the requirements for the backup of each BigQuery dataset, table, and model.    C4 - Ensure each BigQuery dataset, table, and model is backed up (e.g., by creating snapshots or exports) according to the requirements and is restorable. | Medium | 2 | - | - |

| Data policy *(subclass of Dataset and tables, FC8)* *Policy tags are tags with access control policies that can be applied to subresources.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Creates a new data policy under a project with the given dataPolicyId (used as the display name), policy tag, and data policy type. | bigquery.dataPolicies.create |  Threat List  | **Name** | **CVSS** | | --- | --- | | Unauthorized access to the table columns by adding or removing policy tags | [Medium (6.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Unauthorized access to the table columns by adding or removing policy tags

| | **Threat Id** | Bigquery.T17 | | --- | --- | | **Name** | Unauthorized access to the table columns by adding or removing policy tags | | **Description** | Policy tags are attached to a column in a BigQuery table to control the visibility of sensitive data to different groups of users. An attacker can create or update a data policy or its data masking rules and associate it with a column by attaching the policy tags associated with the column policy to the column in order to escalate privileges or leak data. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0004](https://attack.mitre.org/tactics/TA0004) | | **CVSS** | [Medium (6.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:N) | | **IAM Access** | {  "AND": [{  "OPTIONAL": "bigquery.dataPolicies.setIamPolicy"  }, {  "OR": ["bigquery.dataPolicies.create", "bigquery.dataPolicies.update"]  }, "datacatalog.taxonomies.get", "bigquery.tables.setCategory", "bigquery.tables.create"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO5 - Restrict access to columns and protect sensitive data**    C44 - Define the criteria to use authorized data policies for each column in each table.    C45 - Ensure only authorized IAM entities are allowed to access sensitive columns of a table by using data policies. | Medium | 2 | - | - |

| Share resources via BigQuery sharing *(subclass of Dataset and tables, FC9)* *BigQuery sharing is a data exchange platform built on top of BigQuery that enables efficient and secure sharing of data (e.g., BigQuery tables) across organizational boundaries. An exchange is a collection of data and analytics assets designed for sharing.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Creates a new data exchange. | analyticshub.dataExchanges.create | | Creates a new listing. | analyticshub.listings.create |  Threat List  | **Name** | **CVSS** | | --- | --- | | Unauthorized access to contents of a listing | [Medium (4.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N) | | Unauthorized access to listings by setting permissions | [Medium (4.0)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:N/I:H/A:N) | | Discovery of BigQuery sharing resources | [Low (3.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N) | | Denial of Service by revoking subscriptions | [Low (3.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L) | | Denial of Service by deleting data exchanges, listings, or subscriptions | [Low (2.4)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Unauthorized access to contents of a listing

| | **Threat Id** | Bigquery.T30 | | --- | --- | | **Name** | Unauthorized access to contents of a listing | | **Description** | A listing contains BigQuery resources (e.g., tables, models, views) or a Pub/Sub topic that is published within a data exchange. An attacker can create a public listing to provide access to its content or launch an attack against subscribers by phishing (e.g., providing their own email ID or URL) in primaryContact, requestAccess, dataProvider, or publisher. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Medium (4.2)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N) | | **IAM Access** | {  "AND": [{  "OR": ["analyticshub.listings.create", "analyticshub.listings.update"]  }, {  "OR": ["bigquery.datasets.get", "pubsub.topics.get"]  }]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO10 - Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings**    C22 - Maintain a list of authorized sources and destinations (e.g., Cloud Storage, BigQuery, Vertex AI (for LLM, via BigQuery connection only)) to be used with each dataset, table, model, connection, job, and listing. | High | 1 | - | - |
| **CO28 - Enforce access to sensitive data via data clean rooms**    C92 - Define the requirements to configure a data exchange as a data clean room (e.g., sharing sensitive data with 3rd parties).    C93 - Ensure required data exchanges are configured as data clean rooms (i.e., sharingEnvironmentConfig.dcrExchangeConfig). | High | 2 | - | - |
| **CO5 - Restrict access to columns and protect sensitive data**    C9 - Define the criteria for the sensitivity of columns in each table and each view, and their requirements for data protection (e.g., using BigQuery column-level security, column-level data masking, custom masking routines, restriction analysis rules, list overlap analysis rules, aggregation threshold analysis rules, differential privacy clauses, or data clean rooms).    C10 - Ensure only authorized IAM entities are allowed to access sensitive columns of tables and views. | High | 2 | - | - |
| **CO6 - Restrict access to rows with BigQuery row-level security**    C12 - Define the criteria for the sensitivity of rows in each table.    C13 - Ensure only authorized IAM entities are allowed to access sensitive rows of a table (e.g., using BigQuery row-level security). | High | 2 | - | - |
| **CO27 - Ensure sensitive data is not added in the listing fields**    C110 - Maintain a list of authorized emails or URLs (i.e., primaryContact, requestAccess, dataProvider, or publisher) to be used by listings and data exchanges.    C111 - Ensure listings and data exchanges use authorized emails. | Medium | 2 | - | - |
| **CO31 - Restrict the export of data by enabling restricted export**    C113 - Define the requirements for enabling restricted export for listings.    C114 - Ensure the restricted export for listings is enabled according to the requirements. | Medium | 2 | - | - |
| **CO8 - Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings**    C98 - Define the authorized configuration (i.e., displayName, description, documentation, icon, discoveryType, RestrictedExportConfig, logLinkedDatasetQueryUserEmail = true) for each listing and identify the requirements for deploying a public listing.    C99 - Ensure the configuration of each listing is authorized, and discoveryType is public only if required.    C106 - Protect the Pub/Sub topic used by a listing, using the Pub/Sub ThreatModel. | Medium | 3 | - | - |

#### Unauthorized access to listings by setting permissions

| | **Threat Id** | Bigquery.T28 | | --- | --- | | **Name** | Unauthorized access to listings by setting permissions | | **Description** | A data exchange or a listing can be subscribed to. An attacker can provide unauthorized subscribers with access to a listing's content by setting permissions for listings at the project, data exchange, or listing level. | | **Goal** | Data manipulation | | **MITRE ATT&CK®** | [TA0004](https://attack.mitre.org/tactics/TA0004) | | **CVSS** | [Medium (4.0)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:R/S:U/C:N/I:H/A:N) | | **IAM Access** | {  "OR": ["analyticshub.dataExchanges.setIamPolicy", "analyticshub.listings.setIamPolicy"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO10 - Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings**    C22 - Maintain a list of authorized sources and destinations (e.g., Cloud Storage, BigQuery, Vertex AI (for LLM, via BigQuery connection only)) to be used with each dataset, table, model, connection, job, and listing. | High | 1 | - | - |
| **CO28 - Enforce access to sensitive data via data clean rooms**    C92 - Define the requirements to configure a data exchange as a data clean room (e.g., sharing sensitive data with 3rd parties).    C93 - Ensure required data exchanges are configured as data clean rooms (i.e., sharingEnvironmentConfig.dcrExchangeConfig). | High | 2 | - | - |
| **CO29 - Restrict access to listings and data exchanges to authorized subscribers only**    C103 - Maintain the list of authorized subscriptions for each listing and data exchange.    C104 - Ensure only authorized subscriptions for listings and data exchanges are configured. | High | 2 | - | - |
| **CO5 - Restrict access to columns and protect sensitive data**    C9 - Define the criteria for the sensitivity of columns in each table and each view, and their requirements for data protection (e.g., using BigQuery column-level security, column-level data masking, custom masking routines, restriction analysis rules, list overlap analysis rules, aggregation threshold analysis rules, differential privacy clauses, or data clean rooms).    C10 - Ensure only authorized IAM entities are allowed to access sensitive columns of tables and views. | High | 2 | - | - |
| **CO6 - Restrict access to rows with BigQuery row-level security**    C12 - Define the criteria for the sensitivity of rows in each table.    C13 - Ensure only authorized IAM entities are allowed to access sensitive rows of a table (e.g., using BigQuery row-level security). | High | 2 | - | - |
| **CO8 - Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings**    C95 - Define the authorized configuration (i.e., displayName, description, documentation, icon, discoveryType, logLinkedDatasetQueryUserEmail = true) for each data exchange and identify the requirements for deploying the public data exchange.    C96 - Ensure the configuration of each data exchange is authorized, and discoveryType is public only if required.    C98 - Define the authorized configuration (i.e., displayName, description, documentation, icon, discoveryType, RestrictedExportConfig, logLinkedDatasetQueryUserEmail = true) for each listing and identify the requirements for deploying a public listing.    C99 - Ensure the configuration of each listing is authorized, and discoveryType is public only if required. | Medium | 4 | - | - |

#### Discovery of BigQuery sharing resources

| | **Threat Id** | Bigquery.T31 | | --- | --- | | **Name** | Discovery of BigQuery sharing resources | | **Description** | Email IDs are configured for the provider, publisher, and subscriber of a data exchange and listing. An attacker can gather these and launch attacks against them. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0007](https://attack.mitre.org/tactics/TA0007) | | **CVSS** | [Low (3.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N) | | **IAM Access** | {  "OR": ["analyticshub.listings.list", "analyticshub.dataExchanges.list", "analyticshub.listings.viewSubscriptions", "analyticshub.listings.get", "analyticshub.dataExchanges.get", "analyticshub.subscriptions.get", "analyticshub.subscriptions.list"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO27 - Ensure sensitive data is not added in the listing fields**    C101 - Ensure no sensitive data is included in the fields of the listings (i.e., displayName, description, documentation, icon). | Medium | 1 | - | - |
| **CO8 - Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings**    C95 - Define the authorized configuration (i.e., displayName, description, documentation, icon, discoveryType, logLinkedDatasetQueryUserEmail = true) for each data exchange and identify the requirements for deploying the public data exchange.    C96 - Ensure the configuration of each data exchange is authorized, and discoveryType is public only if required.    C98 - Define the authorized configuration (i.e., displayName, description, documentation, icon, discoveryType, RestrictedExportConfig, logLinkedDatasetQueryUserEmail = true) for each listing and identify the requirements for deploying a public listing.    C99 - Ensure the configuration of each listing is authorized, and discoveryType is public only if required. | Medium | 4 | - | - |

#### Denial of Service by revoking subscriptions

| | **Threat Id** | Bigquery.T29 | | --- | --- | | **Name** | Denial of Service by revoking subscriptions | | **Description** | A subscription is created upon subscribing to a listing. An attacker can revoke a subscription for a legitimate subscriber, causing Denial of Service to the subscriber. | | **Goal** | Disruption of Service | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Low (3.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:L) | | **IAM Access** | {  "UNIQUE": "analyticshub.listings.update"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO10 - Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings**    C22 - Maintain a list of authorized sources and destinations (e.g., Cloud Storage, BigQuery, Vertex AI (for LLM, via BigQuery connection only)) to be used with each dataset, table, model, connection, job, and listing.    C23 - Ensure each dataset, table, model, connection, job, and listing uses authorized sources and destinations.    C25 - Protect the sources and destinations used by each table, model, connection, job, and listing, using their respective services' ThreatModels. | High | 3 | - | - |
| **CO29 - Restrict access to listings and data exchanges to authorized subscribers only**    C103 - Maintain the list of authorized subscriptions for each listing and data exchange.    C104 - Ensure only authorized subscriptions for listings and data exchanges are configured. | High | 2 | - | - |

#### Denial of Service by deleting data exchanges, listings, or subscriptions

| | **Threat Id** | Bigquery.T32 | | --- | --- | | **Name** | Denial of Service by deleting data exchanges, listings, or subscriptions | | **Description** | A data exchange, its individual listings, and their subscriptions can be deleted. Data exchanges and listings with active Pub/Sub subscriptions can't be deleted. An attacker can delete any of these resources to cause Denial of Service for their subscribers. | | **Goal** | Disruption of Service | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **CVSS** | [Low (2.4)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L) | | **IAM Access** | {  "OR": ["analyticshub.dataExchanges.delete", "analyticshub.listings.delete", "analyticshub.subscriptions.delete"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO2 - Enforce network-level restrictions leveraging VPC origin and VPC Service Controls**    C2 - Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel.    C121 - Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Very High | 2 | - | - |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO10 - Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings**    C22 - Maintain a list of authorized sources and destinations (e.g., Cloud Storage, BigQuery, Vertex AI (for LLM, via BigQuery connection only)) to be used with each dataset, table, model, connection, job, and listing. | High | 1 | - | - |
| **CO29 - Restrict access to listings and data exchanges to authorized subscribers only**    C103 - Maintain the list of authorized subscriptions for each listing and data exchange.    C104 - Ensure only authorized subscriptions for listings and data exchanges are configured. | High | 2 | - | - |

| Subscribe to access resources via BigQuery sharing *(class, FC10)* *You can subscribe to the listings.* Data Flow Diagram (DFD) | Actions and IAM Permissions to deny the feature  | **Action** | **IAM Permission** | | --- | --- | | Subscribes to a listing. Currently, with BigQuery sharing, you can create listings that reference only BigQuery datasets. Upon subscription to a listing for a BigQuery dataset, BigQuery sharing creates a linked dataset in the subscriber's project. | analyticshub.listings.subscribe | | Creates a subscription to a data clean room. | analyticshub.dataExchanges.subscribe |  Threat List  | **Name** | **CVSS** | | --- | --- | | Email leakage via malicious listing | [Low (2.0)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Email leakage via malicious listing

| | **Threat Id** | Bigquery.T33 | | --- | --- | | **Name** | Email leakage via malicious listing | | **Description** | When a subscriber subscribes to a listing, a linked source is created in the subscriber's project, which acts as a reference or pointer to the source in the provider's project. An attacker can subscribe to a malicious public listing, impersonating a legitimate provider to share their email IDs and launch further attacks. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [Low (2.0)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N) | | **IAM Access** | {  "OR": ["analyticshub.dataExchanges.subscribe", "analyticshub.listings.subscribe"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **CO1 - Limit access to the IAM actions required to execute attacks**    C1 - Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **CO30 - Restrict and manage subscriptions to authorized listings and data exchanges only**    C107 - Maintain the list of listings and/or data exchanges authorized to be subscribed to, and by whom.    C108 - Ensure only authorized entities you control are subscribed to the authorized listings and data exchanges. | High | 2 | - | - |

# Control Implementation

## Limit access to the IAM actions required to execute attacks [Bigquery.CO1]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C1]  Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | Request the list of authorized IAM members that have the permissions required to launch attacks, its review process, and its review records. | High | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3  Bigquery.FC4  Bigquery.FC5  Bigquery.FC6  Bigquery.FC7  Bigquery.FC8  Bigquery.FC9  Bigquery.FC10 | Bigquery.T1 (Very High)  Bigquery.T2 (Very High)  Bigquery.T3 (Very High)  Bigquery.T4 (Very High)  Bigquery.T5 (Very High)  Bigquery.T6 (Very High)  Bigquery.T8 (Very High)  Bigquery.T9 (Very High)  Bigquery.T10 (Very High)  Bigquery.T11 (Very High)  Bigquery.T12 (Very High)  Bigquery.T13 (Very High)  Bigquery.T14 (Very High)  Bigquery.T15 (Very High)  Bigquery.T17 (Very High)  Bigquery.T18 (Very High)  Bigquery.T19 (Very High)  Bigquery.T20 (Very High)  Bigquery.T21 (Very High)  Bigquery.T22 (Very High)  Bigquery.T24 (Very High)  Bigquery.T25 (Very High)  Bigquery.T26 (Very High)  Bigquery.T27 (Very High)  Bigquery.T28 (Very High)  Bigquery.T29 (Very High)  Bigquery.T30 (Very High)  Bigquery.T31 (Very High)  Bigquery.T32 (Very High)  Bigquery.T33 (Very High)  Bigquery.T34 (Very High)  Bigquery.T35 (Very High)  Bigquery.T36 (Very High) | High |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C6]  Maintain a list of authorized IAM entities allowed to access the tables, views, and table data in a specific dataset (note: columns can be made case-sensitive, and a default value can be set for columns). | Request the list of authorized IAM entities allowed to access the tables, views, and table data in a specific dataset, its review process, and its review records. | Very Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3 | Bigquery.T2 (Very Low)  Bigquery.T3 (Very Low)  Bigquery.T5 (Very Low)  Bigquery.T6 (Very Low)  Bigquery.T8 (Very Low)  Bigquery.T9 (Very Low)  Bigquery.T11 (Very Low)  Bigquery.T21 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C7, depends on Bigquery.C6, assured by Bigquery.C8]  Ensure only authorized IAM entities are allowed to access the tables, views, and table data in each dataset. | Request 1) the mechanism ensuring only authorized IAM entities are allowed to access the tables, views, and table data in a specific dataset, 2) its records of execution for all new IAM entities, and 3) the plan to move any older IAM entities. | Medium | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3 | Bigquery.T2 (High)  Bigquery.T3 (High)  Bigquery.T5 (High)  Bigquery.T6 (High)  Bigquery.T8 (High)  Bigquery.T9 (High)  Bigquery.T11 (High)  Bigquery.T21 (Medium) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C8]  Verify only authorized IAM entities are allowed to access the tables, views, and table data in each dataset. | Configure an unauthorized IAM entity to have access to 1) a table or 2) a view; it should be detected. | Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3 | - | High |
| Preventative (COSO)  Protect (NIST CSF) | [Bigquery.C84, depends on Bigquery.C81,Bigquery.C75,Bigquery.C60,Bigquery.C17]  Prevent the unauthorized access/creation/modification/deletion of BigQuery resources (e.g., datasets, tables) (e.g., by using an IAM policy with an allow/deny statement on "bigquery.tables.\*" and/or "bigquery.datasets.\*" with the tags and the authorized value for the conditions "resource.type" = "authorized type", "resource.name" = "authorized name"). | Create/update/delete an unauthorized BigQuery resource; it should be denied. | Low | Bigquery.FC1  Bigquery.FC5 | Bigquery.T1 (High)  Bigquery.T5 (High)  Bigquery.T12 (High)  Bigquery.T21 (High) | High |

## Enforce network-level restrictions leveraging VPC origin and VPC Service Controls [Bigquery.CO2]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C2]  Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel. | Request how the Compute ThreatModel is applied for enforcing VPC origin. | Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC4  Bigquery.FC5  Bigquery.FC6  Bigquery.FC7  Bigquery.FC8  Bigquery.FC9 | Bigquery.T1 (High)  Bigquery.T3 (High)  Bigquery.T4 (High)  Bigquery.T5 (High)  Bigquery.T6 (High)  Bigquery.T8 (High)  Bigquery.T9 (High)  Bigquery.T10 (High)  Bigquery.T11 (High)  Bigquery.T12 (High)  Bigquery.T13 (High)  Bigquery.T14 (High)  Bigquery.T17 (High)  Bigquery.T18 (High)  Bigquery.T19 (High)  Bigquery.T20 (High)  Bigquery.T21 (High)  Bigquery.T22 (High)  Bigquery.T24 (High)  Bigquery.T26 (High)  Bigquery.T27 (High)  Bigquery.T28 (High)  Bigquery.T29 (High)  Bigquery.T30 (High)  Bigquery.T31 (High)  Bigquery.T32 (High)  Bigquery.T34 (High)  Bigquery.T36 (High) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C121]  Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Request how the Access Context Manager ThreatModel is applied for enforcing VPC Service Controls. | Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC4  Bigquery.FC5  Bigquery.FC6  Bigquery.FC7  Bigquery.FC8  Bigquery.FC9 | Bigquery.T1 (High)  Bigquery.T3 (High)  Bigquery.T4 (High)  Bigquery.T5 (High)  Bigquery.T6 (High)  Bigquery.T8 (High)  Bigquery.T9 (High)  Bigquery.T10 (High)  Bigquery.T11 (High)  Bigquery.T12 (High)  Bigquery.T13 (High)  Bigquery.T14 (High)  Bigquery.T17 (High)  Bigquery.T18 (High)  Bigquery.T19 (High)  Bigquery.T20 (High)  Bigquery.T21 (High)  Bigquery.T22 (High)  Bigquery.T24 (High)  Bigquery.T26 (High)  Bigquery.T27 (High)  Bigquery.T28 (High)  Bigquery.T29 (High)  Bigquery.T30 (High)  Bigquery.T31 (High)  Bigquery.T32 (High)  Bigquery.T34 (High)  Bigquery.T36 (High) | Very High |

## Ensure backup, failover, and recovery capabilities for BigQuery resources (e.g., snapshots and exports for datasets and tables, failover procedures for reservations) [Bigquery.CO3]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C3]  Define the requirements for the backup of each BigQuery dataset, table, and model. | Request the backup requirements for each BigQuery dataset, table, and model. | Low | Bigquery.FC1  Bigquery.FC6  Bigquery.FC7 | Bigquery.T1 (Very Low)  Bigquery.T14 (Very Low)  Bigquery.T21 (Very Low)  Bigquery.T22 (Very Low)  Bigquery.T27 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C4, depends on Bigquery.C3, assured by Bigquery.C5]  Ensure each BigQuery dataset, table, and model is backed up (e.g., by creating snapshots or exports) according to the requirements and is restorable. | Request the mechanism ensuring BigQuery datasets, tables, and models are backed up (e.g., by creating snapshots or exports) according to their requirements, the evidence of their execution, and their regular testing of restoration. | High | Bigquery.FC1  Bigquery.FC6  Bigquery.FC7 | Bigquery.T1 (High)  Bigquery.T14 (High)  Bigquery.T21 (High)  Bigquery.T22 (High)  Bigquery.T27 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C5]  Verify all BigQuery datasets, tables, and models are backed up according to the requirements. | Change the backup mechanism to be outside the requirements; it should be detected. | High | Bigquery.FC1  Bigquery.FC6  Bigquery.FC7 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C130]  Define the failover process (e.g., use soft failover mode by default, document the justification for any hard failover, require approval for exceptions, record the chosen failover mode in the change process, validate replication status) for reservations. | Request the failover process for reservations, its review process, and its review records. | Low | Bigquery.FC5 | Bigquery.T36 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C131, depends on Bigquery.C130]  Ensure a reservation is failed over according to the process. | Request the mechanism ensuring that the reservation is failed over according to the process. | Medium | Bigquery.FC5 | Bigquery.T36 (High) | Low |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C132, depends on Bigquery.C130]  Monitor the failover mode of a reservation (e.g., by using Cloud Logging event "google.cloud.bigquery.reservation.v1.ReservationService.FailoverReservation" and its field request.failoverMode). | Fail over a reservation in hard mode; it should be detected. | Medium | Bigquery.FC5 | Bigquery.T36 (Medium) | Very Low |

## Restrict access to columns and protect sensitive data [Bigquery.CO5]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C9]  Define the criteria for the sensitivity of columns in each table and each view, and their requirements for data protection (e.g., using BigQuery column-level security, column-level data masking, custom masking routines, restriction analysis rules, list overlap analysis rules, aggregation threshold analysis rules, differential privacy clauses, or data clean rooms). | Request the criteria for the sensitivity of columns in a table and each view and their requirements for data protection. | Very Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3  Bigquery.FC9 | Bigquery.T2 (Very Low)  Bigquery.T6 (Very Low)  Bigquery.T8 (Very Low)  Bigquery.T9 (Very Low)  Bigquery.T26 (Very Low)  Bigquery.T28 (Very Low)  Bigquery.T30 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C10, depends on Bigquery.C9, assured by Bigquery.C11]  Ensure only authorized IAM entities are allowed to access sensitive columns of tables and views. | Request 1) the mechanism ensuring only authorized IAM entities are allowed to access sensitive columns of tables and views, 2) its records of execution for all new IAM entities, and 3) the plan to move any older IAM entities. | Medium | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3  Bigquery.FC9 | Bigquery.T2 (High)  Bigquery.T6 (High)  Bigquery.T8 (Medium)  Bigquery.T9 (Medium)  Bigquery.T26 (Medium)  Bigquery.T28 (Medium)  Bigquery.T30 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C11]  Verify only authorized IAM entities are allowed to access sensitive columns of each table and each view. | Configure an unauthorized IAM entity with access to a sensitive column; it should be detected. | Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3  Bigquery.FC9 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C44]  Define the criteria to use authorized data policies for each column in each table. | Request the criteria for using data policies for each column in each table. | Very Low | Bigquery.FC3  Bigquery.FC8 | Bigquery.T2 (Very Low)  Bigquery.T17 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C45, depends on Bigquery.C44, assured by Bigquery.C46]  Ensure only authorized IAM entities are allowed to access sensitive columns of a table by using data policies. | Request 1) the mechanism ensuring only authorized IAM entities are allowed to access sensitive columns of a table with data policies, 2) its records of execution for all new IAM entities, and 3) the plan to move any older IAM entities. | Medium | Bigquery.FC3  Bigquery.FC8 | Bigquery.T2 (Medium)  Bigquery.T17 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C46]  Verify only authorized IAM entities are allowed to access sensitive columns of a table by using data policies. | Configure an unauthorized IAM entity with access to a sensitive column in a data policy; it should be detected. | Low | Bigquery.FC3  Bigquery.FC8 | - | Medium |

## Restrict access to rows with BigQuery row-level security [Bigquery.CO6]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C12]  Define the criteria for the sensitivity of rows in each table. | Request the criteria for the sensitivity of rows in a table. | Very Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3  Bigquery.FC9 | Bigquery.T2 (Very Low)  Bigquery.T6 (Very Low)  Bigquery.T8 (Very Low)  Bigquery.T9 (Very Low)  Bigquery.T28 (Very Low)  Bigquery.T30 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C13, depends on Bigquery.C12, assured by Bigquery.C14]  Ensure only authorized IAM entities are allowed to access sensitive rows of a table (e.g., using BigQuery row-level security). | Request 1) the mechanism ensuring only authorized IAM entities are allowed to access sensitive rows of a table, 2) its records of execution for all new IAM entities, and 3) the plan to move any older IAM entities. | Medium | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3  Bigquery.FC9 | Bigquery.T2 (Medium)  Bigquery.T6 (High)  Bigquery.T8 (Medium)  Bigquery.T9 (High)  Bigquery.T28 (Medium)  Bigquery.T30 (Medium) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C14]  Verify only authorized IAM entities are allowed to access sensitive rows of a table. | Configure an unauthorized IAM entity with access to a sensitive row; it should be detected. | Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3  Bigquery.FC9 | - | High |

## Encrypt resources (e.g., datasets, models, data transfers) with customer-managed encryption keys and protect the keys [Bigquery.CO7]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C26]  Maintain a list of authorized CMEKs to be used with each BigQuery resource (e.g., dataset, DLP function, model, data transfer), ideally dedicated (e.g., using Autokey on bigquery.googleapis.com/Dataset), and of the default CMEK at the project or organization level, and define the requirement to rotate key versions for tables. | Request the list of authorized CMEKs and their versions to be used by the BigQuery resource and the default CMEK per project or at the organization level, and the requirement to rotate key versions for tables, their review process, and their review records. | Very Low | Bigquery.FC1 | Bigquery.T11 (Very Low)  Bigquery.T20 (Very Low)  Bigquery.T21 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C27, depends on Bigquery.C26, assured by Bigquery.C29]  Ensure only authorized CMEKs and their versions are used with the BigQuery resource. | Request 1) the mechanism ensuring only authorized CMEKs are configured, 2) its records of execution for all new BigQuery resources, and 3) the plan to move any older BigQuery resources. | Medium | Bigquery.FC1 | Bigquery.T11 (Medium)  Bigquery.T20 (Medium) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C28, depends on Bigquery.C26]  Protect the CMEKs used by each BigQuery resource using the Cloud KMS ThreatModel (including enforcing CMEK protection using organization policy constraints/gcp.restrictCmekCryptoKeyProjects and constraints/gcp.restrictNonCmekServices as per Cloudkms.C32 and Cloudkms.C34). | Request how the Cloud KMS ThreatModel is applied to BigQuery resources. | High | Bigquery.FC1 | Bigquery.T11 (Medium)  Bigquery.T20 (Medium) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C29]  Verify each BigQuery resource is encrypted using an authorized CMEK and its version. | Use an unauthorized 1) CMEK or a 2) version with a BigQuery resource; it should be detected. | Low | Bigquery.FC1 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C36, depends on Bigquery.C26, assured by Bigquery.C37]  Ensure [AEAD encryption functions](https://docs.cloud.google.com/bigquery/docs/column-key-encrypt) are used to encrypt data at the column level. | Request the mechanism ensuring AEAD encryption functions are used to encrypt data at the column level. | Medium | Bigquery.FC1 | Bigquery.T11 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C37]  Verify AEAD encryption functions are used to encrypt data at the column level. | Do not encrypt the data at the column level; it should be detected. | Low | Bigquery.FC1 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C85, depends on Bigquery.C26]  Define the requirements for generating, storing, accessing, distributing, rotating, backing up, and destroying encryption keys for applications (e.g., by using a dedicated secret management tool such as HashiCorp Vault or GCP Secret Manager) as per the security standards. | Request the requirements for generating, storing, accessing, distributing, using, rotating, backing up, and destroying keys for applications, their review process, and its review records. | Medium | Bigquery.FC1 | Bigquery.T20 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C86, depends on Bigquery.C85,Bigquery.C26]  Ensure the keys for applications are generated, stored, accessed, distributed, rotated, backed up, and destroyed as per the security standards. | Request 1) the mechanism ensuring the keys for applications are generated, stored, accessed, distributed, rotated, backed up, and destroyed as per the security standards, 2) its records of execution for all new keys, and 3) the plan to move any older keys. | Medium | Bigquery.FC1 | Bigquery.T20 (High) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Bigquery.C134, depends on Bigquery.C26]  Prevent the creation of a dataset without an authorized key (e.g., using a custom constraint resourceType:[bigquery.googleapis.com/Dataset](https://docs.cloud.google.com/bigquery/docs/custom-constraints#supported_resources), resource(s): resource.defaultEncryptionConfiguration.kmsKeyName != an authorized encryption key, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | Create a dataset with unauthorized key; it should be denied. | Medium | Bigquery.FC1 | Bigquery.T21 (High) | Medium |

## Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings [Bigquery.CO8]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C15, assured by Bigquery.C16]  Ensure no dataset is accessible to "AllUsers" or "AllAuthenticatedUsers", except if allowed. | Request 1) the mechanism ensuring no dataset is accessible to "AllUsers" or "AllAuthenticatedUsers", 2) its records of execution for all datasets, and 3) the plan to move any older datasets. | Low | Bigquery.FC1  Bigquery.FC2 | Bigquery.T8 (High)  Bigquery.T9 (High) | Very High |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C16]  Verify no dataset is accessible to "AllUsers" or "AllAuthenticatedUsers" (e.g., using the Security Command Center finding [PUBLIC\_DATASET](https://docs.cloud.google.com/security-command-center/docs/concepts-vulnerabilities-findings#dataset-findings)). | Modify a dataset to allow access to 1) "AllUsers", or 2) "AllAuthenticatedUsers"; it should be detected. | Very Low | Bigquery.FC1  Bigquery.FC2 | - | Very High |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C17]  Define the authorized configuration (i.e., defaultTableExpirationMs, defaultPartitionExpirationMs, defaultEncryptionConfiguration, linkedDatasetSource, externalDatasetReference, defaultCollation, defaultRoundingMode, maxTimeTravelHours, storageBillingModel, and defaultEncryptionConfiguration) for each BigQuery dataset. | Request the authorized configuration for each BigQuery dataset, its review process, and its review records. | Low | Bigquery.FC1  Bigquery.FC2 | Bigquery.T8 (Very Low)  Bigquery.T11 (Very Low)  Bigquery.T21 (Very Low)  Bigquery.T25 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C18, depends on Bigquery.C17, assured by Bigquery.C19]  Ensure the configuration of each BigQuery dataset is authorized. | Request the mechanism ensuring the configuration of each BigQuery dataset is authorized, and the evidence of its execution. | High | Bigquery.FC1  Bigquery.FC2 | Bigquery.T8 (High)  Bigquery.T11 (High)  Bigquery.T21 (High)  Bigquery.T25 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C19]  Verify all BigQuery datasets have authorized configurations. | Create a dataset with an unauthorized configuration; it should be detected. | High | Bigquery.FC1  Bigquery.FC2 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C60]  Define the authorized configuration for each reservation (i.e., maxSlots, edition, ignoreIdleSlots, autoscale, secondaryLocation) and its assignments (i.e., assignee, jobType). | Request the authorized configuration for each reservation and its assignments. | Low | Bigquery.FC1  Bigquery.FC5 | Bigquery.T9 (Very Low)  Bigquery.T12 (Very Low) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C61, depends on Bigquery.C60, assured by Bigquery.C62]  Ensure each reservation and its assignments use an authorized configuration. | Request the mechanism ensuring the reservation and its assignments use an authorized configuration, and the evidence of its execution. | High | Bigquery.FC5 | Bigquery.T12 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C62]  Verify all reservations and their assignments use an authorized configuration. | Use an unauthorized configuration with 1) a reservation, or 2) an assignment; it should be detected. | High | Bigquery.FC5 | - | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C63, depends on Bigquery.C60]  Monitor the creation/modification of unauthorized reservations (e.g., by using Cloud Logging event "google.cloud.bigquery.reservation.v1.ReservationService.CreateReservation" and "google.cloud.bigquery.reservation.v1.ReservationService.UpdateReservation", and their fields request.reservation.autoscale.maxSlots and request.reservation.edition). | Create/update the reservation with unauthorized values; it should be detected. | Medium | Bigquery.FC5 | Bigquery.T12 (Medium) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C64, depends on Bigquery.C60]  Monitor the creation/modification of unauthorized assignments (e.g., by using Cloud Logging event "google.cloud.bigquery.reservation.v1.ReservationService.CreateAssignment" and its fields request.assignment.assignee, request.assignment.jobType, and request.parent, and event "google.cloud.bigquery.reservation.v1.ReservationService.UpdateAssignment" and its fields request.assignment.assignee and request.assignment.jobType). | Create/update the assignment with unauthorized values; it should be detected. | Medium | Bigquery.FC5 | Bigquery.T12 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C75]  Define the authorized configuration (e.g., createDisposition, writeDisposition, schemaUpdateOptions) for each asynchronous query job. | Request the authorized configuration for each asynchronous query job, its review process, and its review records. | Low | Bigquery.FC1 | Bigquery.T20 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C76, depends on Bigquery.C75, assured by Bigquery.C77]  Ensure the configuration of each asynchronous query job is authorized. | Request the mechanism ensuring the configuration of each asynchronous query job is authorized, and the evidence of its execution. | High | Bigquery.FC1 | Bigquery.T20 (Medium) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C77]  Verify all asynchronous query jobs have authorized configurations. | Create an asynchronous query job with unauthorized configurations; it should be detected. | High | Bigquery.FC1 | - | Low |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C81]  Define the authorized configuration (i.e., schema, clustering, expirationTime, view, materializedView, externalDataConfiguration, encryptionConfiguration, defaultCollation, defaultRoundingMode, and tableConstraints) for each BigQuery table. | Request the authorized configuration for each BigQuery table, its review process, and its review records. | Medium | Bigquery.FC1 | Bigquery.T1 (Very Low)  Bigquery.T5 (Very Low)  Bigquery.T25 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C82, depends on Bigquery.C81, assured by Bigquery.C83]  Ensure the configuration of each BigQuery table is authorized. | Request the mechanism ensuring the configuration of each BigQuery table is authorized, and the evidence of its execution. | High | Bigquery.FC1 | Bigquery.T1 (Low)  Bigquery.T5 (Medium)  Bigquery.T25 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C83]  Verify all BigQuery tables have authorized configurations. | Create a table with an unauthorized configuration; it should be detected. | High | Bigquery.FC1 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C95]  Define the authorized configuration (i.e., displayName, description, documentation, icon, discoveryType, logLinkedDatasetQueryUserEmail = true) for each data exchange and identify the requirements for deploying the public data exchange. | Request the authorized configuration for each data exchange and the criteria for its discovery type, its review process, and its review records. | Low | Bigquery.FC9 | Bigquery.T28 (Very Low)  Bigquery.T31 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C96, depends on Bigquery.C95, assured by Bigquery.C97]  Ensure the configuration of each data exchange is authorized, and discoveryType is public only if required. | Request 1) the mechanism ensuring authorized configurations are used, 2) its records of execution for all new data exchanges, and 3) the plan to move any older data exchanges. | High | Bigquery.FC9 | Bigquery.T28 (Medium)  Bigquery.T31 (Medium) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C97]  Verify all data exchanges have authorized configurations. | Create a data exchange with an unauthorized configuration; it should be detected. | High | Bigquery.FC9 | - | Low |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C98]  Define the authorized configuration (i.e., displayName, description, documentation, icon, discoveryType, RestrictedExportConfig, logLinkedDatasetQueryUserEmail = true) for each listing and identify the requirements for deploying a public listing. | Request the authorized configuration for each listing and requirement for its discovery type, its review process, and its review records. | Low | Bigquery.FC9 | Bigquery.T28 (Very Low)  Bigquery.T30 (Very Low)  Bigquery.T31 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C99, depends on Bigquery.C98, assured by Bigquery.C100]  Ensure the configuration of each listing is authorized, and discoveryType is public only if required. | Request 1) the mechanism ensuring that authorized configurations are used, 2) its records of execution for all new listings, and 3) the plan to move any older listings. | High | Bigquery.FC9 | Bigquery.T28 (Medium)  Bigquery.T30 (Medium)  Bigquery.T31 (Medium) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C100]  Verify all listings have authorized configurations. | Create a listing with an unauthorized configuration; it should be detected. | High | Bigquery.FC9 | - | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C106, depends on Bigquery.C98]  Protect the Pub/Sub topic used by a listing, using the Pub/Sub ThreatModel. | Request how the Pub/Sub ThreatModel is applied to topics used by a listing. | High | Bigquery.FC9 | Bigquery.T30 (High) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Bigquery.C133, depends on Bigquery.C17]  Prevent the creation/update of a dataset without an authorized configuration (e.g., using a custom constraint resourceType:[bigquery.googleapis.com/Dataset](https://docs.cloud.google.com/bigquery/docs/custom-constraints#supported_resources), resource(s): resource.defaultCollation != an authorized collation, resource.defaultRoundingMode != an authorized rounding mode, resource.maxTimeTravelHours != an authorized time travel window, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | Create or update a dataset with unauthorized configuration; it should be denied. | Medium | Bigquery.FC1 | Bigquery.T21 (High) | Medium |

## De-identify sensitive data using Cloud DLP [Bigquery.CO9]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C20, assured by Bigquery.C21]  Ensure sensitive data is identified and redacted (e.g., using Cloud DLP). | Request the mechanism to identify and redact sensitive data. | High | Bigquery.FC1 | Bigquery.T6 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C21]  Verify sensitive data is identified and redacted (e.g., using Cloud DLP). | Add non-redacted sensitive data; it should be detected. | High | Bigquery.FC1 | - | Medium |

## Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings [Bigquery.CO10]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C22]  Maintain a list of authorized sources and destinations (e.g., Cloud Storage, BigQuery, Vertex AI (for LLM, via BigQuery connection only)) to be used with each dataset, table, model, connection, job, and listing. | Request the list of all authorized sources and destinations to be used with each dataset, table, model, connection, job, and listing, its review process, and its review records. | High | Bigquery.FC1  Bigquery.FC3  Bigquery.FC6  Bigquery.FC9 | Bigquery.T2 (Very Low)  Bigquery.T3 (Very Low)  Bigquery.T6 (Very Low)  Bigquery.T15 (Very Low)  Bigquery.T18 (Very Low)  Bigquery.T20 (Very Low)  Bigquery.T21 (Very Low)  Bigquery.T24 (Very Low)  Bigquery.T28 (Very Low)  Bigquery.T29 (Very Low)  Bigquery.T30 (Very Low)  Bigquery.T32 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C23, depends on Bigquery.C22, assured by Bigquery.C24]  Ensure each dataset, table, model, connection, job, and listing uses authorized sources and destinations. | Request 1) the mechanism ensuring only authorized sources and destinations are configured, 2) its records of execution for all new sources and destinations, and 3) the plan to move any older sources and destinations. | Medium | Bigquery.FC1  Bigquery.FC3  Bigquery.FC6  Bigquery.FC9 | Bigquery.T2 (High)  Bigquery.T3 (High)  Bigquery.T6 (High)  Bigquery.T15 (High)  Bigquery.T18 (High)  Bigquery.T20 (High)  Bigquery.T24 (High)  Bigquery.T29 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C24]  Verify each dataset, table, model, connection, job, and listing uses authorized sources and destinations. | For a BigQuery dataset, table, model, connection, job, or listing, use an unauthorized 1) source or 2) destination; it should be detected. | Medium | Bigquery.FC1  Bigquery.FC3  Bigquery.FC6  Bigquery.FC9 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C25, depends on Bigquery.C22]  Protect the sources and destinations used by each table, model, connection, job, and listing, using their respective services' ThreatModels. | Request how the respective source and destination ThreatModels are applied to BigQuery. | High | Bigquery.FC1  Bigquery.FC3  Bigquery.FC9 | Bigquery.T2 (High)  Bigquery.T3 (High)  Bigquery.T6 (High)  Bigquery.T15 (High)  Bigquery.T29 (Medium) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Bigquery.C135, depends on Bigquery.C22]  Prevent the creation of a dataset without an authorized source (e.g., using a custom constraint resourceType:[bigquery.googleapis.com/Dataset](https://docs.cloud.google.com/bigquery/docs/custom-constraints#supported_resources), resource(s): resource.linkedDatasetSource.sourceDataset.datasetId != an authorized linked data source, resource.externalDatasetReference != an authorized external dataset reference, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | Create a dataset with an unauthorized source; it should be denied. | Medium | Bigquery.FC1 | Bigquery.T21 (High) | Medium |

## Set the expiration time of BigQuery tables as per the requirements [Bigquery.CO12]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C32]  Define the requirements for the expiration time of each BigQuery table. | Request the requirements for the expiration time of each BigQuery table. | Low | Bigquery.FC1 | Bigquery.T11 (Very Low)  Bigquery.T21 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C33, depends on Bigquery.C32, assured by Bigquery.C34]  Ensure the expiration time of each BigQuery table is set according to the requirements. | Request the mechanism ensuring the expiration time of each BigQuery table is set according to its requirements. | Medium | Bigquery.FC1 | Bigquery.T11 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C34]  Verify the expiration time of each BigQuery table is set to its requirements. | Set the expiration time of a BigQuery table to be outside its requirements; it should be detected. | High | Bigquery.FC1 | - | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Bigquery.C136, depends on Bigquery.C32]  Prevent the creation or update of a dataset without an authorized expiration time (e.g., using a custom constraint resourceType:[bigquery.googleapis.com/Dataset](https://docs.cloud.google.com/bigquery/docs/custom-constraints#supported_resources), resource(s): resource.defaultTableExpirationMs != an authorized expiration time, resource.defaultPartitionExpirationMs != an authorized partition expiration time, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | Create or update a dataset with an unauthorized expiration time; it should be denied. | Medium | Bigquery.FC1 | Bigquery.T21 (High) | Medium |

## Monitor BigQuery capacity and utilization [Bigquery.CO13]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C35]  Monitor slot consumption (e.g., using slot recommender), job concurrency, job execution time, job errors, and bytes processed across the entire organization (e.g., using BigQuery Admin Resource Charts). | Create a job and use slots in an abnormal way; it should be detected. | Low | Bigquery.FC5 | Bigquery.T12 (Medium) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C43]  Monitor slot capacity (e.g., using the slot estimator) to estimate the correct number of slots for the BigQuery workload. | Increase or decrease slot capacity widely; it should be detected. | Low | Bigquery.FC5 | Bigquery.T12 (Low) | Low |

## Limit use of BigQuery Omni [Bigquery.CO14]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C38]  Define the requirements for using BigQuery Omni (AWS and/or Azure). | Request the requirements for the use of BigQuery Omni. | Low | Bigquery.FC3  Bigquery.FC5 | Bigquery.T15 (Very Low)  Bigquery.T36 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C39, depends on Bigquery.C38, assured by Bigquery.C40]  Ensure the use of BigQuery Omni as per the requirements (e.g., using organizational constraints [constraints/bigquery.disableBQOmniAWS](https://docs.cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints) and [constraints/bigquery.disableBQOmniAzure](https://docs.cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints)). | Request the implementation to ensure the use of BigQuery Omni as per the requirements and its records of execution. | Medium | Bigquery.FC3  Bigquery.FC5 | Bigquery.T15 (Very High)  Bigquery.T36 (Very Low) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C40]  Verify the use of BigQuery Omni as per the requirements. | Use BigQuery Omni outside the requirements; it should be detected. | Low | Bigquery.FC3  Bigquery.FC5 | - | High |

## Enable logs for BigQuery Data Transfer [Bigquery.CO15]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C41]  Ensure Cloud Audit Logs for BigQuery Data Transfer are enabled ([ref](https://docs.cloud.google.com/bigquery-transfer/docs/audit-logging)). | Request the implementation for enabling the Cloud Audit Logs for BigQuery Data Transfer and its records for execution. | Medium | Bigquery.FC4 | Bigquery.T13 (Low) | Low |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C88, depends on Bigquery.C66]  Monitor the creation/modification of unauthorized data transfers (e.g., by using Cloud Logging events "google.cloud.bigquery.datatransfer.v1.DataTransferService.CreateTransferConfig" and "google.cloud.bigquery.datatransfer.v1.DataTransferService.UpdateTransferConfig" and their fields request.serviceAccountName, request.transferConfig.dataSourceId, request.transferConfig.destinationDatasetId, request.transferConfig.emailPreferences, request.transferConfig.notificationPubsubTopic, and request.transferConfig.schedule). | Create/update an unauthorized data transfer; it should be detected. | Medium | Bigquery.FC4 | Bigquery.T13 (Medium) | Medium |

## Monitor data protection, data ingestion, and data quality [Bigquery.CO16]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C42]  Monitor the abnormal number of concurrent connections and throughput for the BigQuery table (e.g., by using the Monitoring metric CONSUMER QUOTA - QUOTA LIMIT). | Create 1) an abnormal number of concurrent connections and 2) abnormal throughput for a BigQuery table; it should be detected. | Low | Bigquery.FC1  Bigquery.FC6 | Bigquery.T4 (Low)  Bigquery.T5 (Very Low) | Low |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C65]  Monitor the quality of data used with the ML models (e.g., by [data profiling](https://docs.cloud.google.com/bigquery/docs/data-profile-scan)). | Ingest bogus data in a table; it should be detected. | Low | Bigquery.FC6 | Bigquery.T4 (Low) | Low |
| Directive (COSO)  Respond (NIST CSF) | [Bigquery.C87]  Establish, document, and train on procedures for responding to key compromise events, including key leaks and unapproved access. Implement a key revocation process to invalidate compromised keys and replace them with new, secure keys. | Request the plan for key compromised events, and the records and results of the last Incident Response simulation. | High | Bigquery.FC1 | Bigquery.T20 (Medium) | Low |

## Register BigQuery models as per the requirements [Bigquery.CO17]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C47]  Define the requirements to register the BigQuery models with the Vertex AI Model Registry for each BigQuery model. | Request the registration requirements for each BigQuery model. | Low | Bigquery.FC6 | Bigquery.T18 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C48, depends on Bigquery.C47, assured by Bigquery.C49]  Ensure each BigQuery model is registered with the Vertex AI Model Registry according to its requirements. | Request the mechanism ensuring the BigQuery model is registered according to its requirements, and its records of execution. | High | Bigquery.FC6 | Bigquery.T18 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C49]  Verify all BigQuery models are registered with the Vertex AI Model Registry according to their requirements. | Register a model with a Vertex AI Model Registry outside the requirements; it should be detected. | High | Bigquery.FC6 | - | Medium |

## Limit the amount of cloned data [Bigquery.CO18]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C50]  Define the requirements for setting the time travel of each BigQuery dataset. | Request the requirements for setting time travel for each BigQuery dataset. | Low | Bigquery.FC1 | Bigquery.T19 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C51, depends on Bigquery.C50, assured by Bigquery.C52]  Ensure the time travel of each BigQuery dataset is set according to its requirements. | Request the mechanism ensuring the time travel of each BigQuery dataset is set according to its requirements. | Medium | Bigquery.FC1 | Bigquery.T19 (Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C52]  Verify the time travel of each BigQuery dataset is set to its requirements. | Set the time travel of a BigQuery dataset to an unauthorized value; it should be detected. | High | Bigquery.FC1 | - | Low |

## Enforce authorized configurations on jobs [Bigquery.CO19]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C53]  Define the authorized configuration for each job. | Request the authorized configuration for each job, its review process, and its review records. | Low | Bigquery.FC1 | Bigquery.T19 (Very Low)  Bigquery.T26 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C54, depends on Bigquery.C53, assured by Bigquery.C55]  Ensure each job uses an authorized configuration. | Request the mechanism ensuring the job uses an authorized configuration and its records of execution. | High | Bigquery.FC1 | Bigquery.T19 (High)  Bigquery.T26 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C55]  Verify all jobs use an authorized configuration. | Use an unauthorized configuration with a job; it should be detected. | High | Bigquery.FC1 | - | Medium |

## Monitor abnormal performance of queries [Bigquery.CO20]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C56]  Monitor the abnormal behavior, such as unexpected increases in execution time or unusual resource utilization, of a query (e.g., by using the query execution graph or administrative jobs explorer). | Run a query with abnormal behavior; it should be detected. | Low | Bigquery.FC1 | Bigquery.T9 (Medium) | Medium |

## Use authorized metadata caching [Bigquery.CO21]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C57]  Define the requirements for metadata cache mode and staleness (30 minutes to 7 days) for each external table. | Request the requirements for enabling metadata cache and setting its staleness (30 minutes to 7 days) for each external table. | Low | Bigquery.FC1 | Bigquery.T9 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C58, depends on Bigquery.C57, assured by Bigquery.C59]  Ensure the metadata cache mode and staleness of each external table are set according to its requirements. | Request the mechanism ensuring the metadata cache mode and staleness of each external table are set according to its requirements. | Medium | Bigquery.FC1 | Bigquery.T9 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C59]  Verify the metadata cache mode and staleness of each external table are set to their requirements. | Set the metadata cache mode and staleness of an external table outside the requirements; it should be detected. | Medium | Bigquery.FC1 | - | Medium |

## Secure and use the authorized sources and their respective authorized configurations with BigQuery Data Transfer [Bigquery.CO22]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C66]  Maintain a list of authorized sources (e.g., Cloud Storage, Amazon S3, Oracle, Salesforce) and their respective authorized configurations (i.e., destination dataset, schedule, config status, encryption key, parameters) to be used with each transfer. | Request the list of all authorized sources and their respective authorized configurations to be used with each transfer, its review process, and its review records. | Low | Bigquery.FC4 | Bigquery.T13 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C67, depends on Bigquery.C66, assured by Bigquery.C68]  Ensure each transfer uses an authorized source and its authorized configuration. | Request 1) the mechanism ensuring only an authorized source and its authorized configuration are configured, 2) its records of execution for all new sources, and 3) the plan to move any older sources. | Medium | Bigquery.FC4 | Bigquery.T13 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C68]  Verify each transfer uses an authorized source and its authorized configuration. | For a transfer, 1) use an unauthorized source, 2) remove an authorized source, or 3) use an unauthorized configuration for a source; it should be detected. | Medium | Bigquery.FC4 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C69, depends on Bigquery.C66]  Protect the sources used with each transfer, using the respective service's ThreatModel. | Request how the respective service ThreatModel is applied to protect each BigQuery Data Transfer source. | High | Bigquery.FC4 | Bigquery.T13 (Medium) | Low |
| Preventative (COSO)  Protect (NIST CSF) | [Bigquery.C119, depends on Bigquery.C66]  Prevent the creation/update of a transfer without an authorized source and/or destination (e.g., using a custom constraint resourceType:[bigquerydatatransfer.googleapis.com/TransferConfig](https://docs.cloud.google.com/bigquery/docs/transfer-custom-constraints#supported_resources), resource(s): resource.dataSourceId != an authorized data source, resource.destinationDatasetId != an authorized dataset, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | Create a transfer with an unauthorized 1) data source or create/update with an unauthorized 2) destination dataset; it should be denied. | Medium | Bigquery.FC4 | Bigquery.T13 (Medium) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Bigquery.C120, depends on Bigquery.C66]  Prevent the create/update of a transfer without an authorized ingestion (i.e., schedule, refresh window, and status of transfer configuration) (e.g., using a custom constraint resourceType:[bigquerydatatransfer.googleapis.com/TransferConfig](https://docs.cloud.google.com/bigquery/docs/transfer-custom-constraints#supported_resources), resource(s): resource.dataRefreshWindowDays != authorized data refresh window, resource.disabled != authorized config status, resource.emailPreferences.enableFailureEmail != authorized failure email status, resource.encryptionConfiguration.kmsKeyName != authorized KMS key, resource.schedule != authorized schedule, resource.scheduleOptions.disableAutoScheduling != authorized autoscheduling status, resource.scheduleOptions.endTime != authorized end time, resource.scheduleOptions.startTime != authorized start time, resource.scheduleOptionsV2.timeBasedSchedule.endTime != authorized end time, resource.scheduleOptionsV2.timeBasedSchedule.schedule != authorized schedule, resource.scheduleOptionsV2.timeBasedSchedule.startTime != authorized start time, resource.scheduleOptionsV2.eventDrivenSchedule.pubsubSubscription != authorized Pub/Sub subscription, resource.notificationPubsubTopic != authorized Pub/Sub topic, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | Create a transfer with an unauthorized key or create/update a transfer with an unauthorized schedule; it should be denied. | Medium | Bigquery.FC4 | Bigquery.T13 (Medium) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C137, depends on Bigquery.C66]  Protect the network attachments used with private database sources, using the Compute Engine ThreatModel. | Request how the Compute Engine ThreatModel is applied to protect network attachments used with private database sources. | High | Bigquery.FC4 | Bigquery.T13 (Medium) | Low |

## Use authorized User-Defined Functions [Bigquery.CO23]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C70]  Maintain a list of authorized Cloud Storage buckets to be used with query jobs for User-Defined Functions (UDFs). | Request the list of Cloud Storage buckets used with query jobs for User-Defined Functions (UDFs). | High | Bigquery.FC2 | Bigquery.T8 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C71, depends on Bigquery.C70, assured by Bigquery.C72]  Ensure each query uses an authorized Cloud Storage bucket for a UDF. | Request 1) the mechanism ensuring queries use an authorized Cloud Storage bucket for UDFs, 2) its records of execution for all new UDFs, and 3) the plan to move any older UDFs. | Medium | Bigquery.FC2 | Bigquery.T8 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C72]  Verify each query uses an authorized Cloud Storage bucket for its UDF. | For a UDF, use an unauthorized bucket; it should be detected. | Medium | Bigquery.FC2 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C73, depends on Bigquery.C70]  Protect the Cloud Storage buckets used for storing UDFs using Cloud Storage ThreatModel. | Request how the Cloud Storage ThreatModel is applied to buckets used for storing UDFs. | High | Bigquery.FC2 | Bigquery.T8 (Medium) | Low |

## Enforce secure SDLC processes on routines and queries [Bigquery.CO24]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C74]  Enforce secure SDLC processes on routines (e.g., using source control, static analysis, dynamic analysis, peer review). | Request the process and records of enforcing the SDLC process on routines to ensure the review of their code. | Medium | Bigquery.FC2 | Bigquery.T8 (High) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C122]  Enforce secure SDLC processes on queries (e.g., using source control, static analysis, dynamic analysis, and peer review). | Request 1) the processes and records of enforcing a secure SDLC on queries, 2) the records of execution for all new queries, and 3) the plan to move any older queries. | Medium | Bigquery.FC1 | Bigquery.T9 (High) | High |

## Set an authorized expiration time for each ML model [Bigquery.CO25]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C78]  Define the authorized expiration time for each ML model. | Request the authorized expiration time for each ML model. | Low | Bigquery.FC6 | Bigquery.T22 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C79, depends on Bigquery.C78, assured by Bigquery.C80]  Ensure the expiration time for each ML model is authorized. | Request the mechanism ensuring the expiration time for each ML model is authorized, and the evidence of its execution. | High | Bigquery.FC6 | Bigquery.T22 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C80]  Verify all ML models have an authorized expiration time. | Create an ML model with an unauthorized expiration time; it should be detected. | High | Bigquery.FC6 | - | Medium |

## Use fingerprinting for ML models to ensure their integrity [Bigquery.CO26]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C89]  Define the requirements for generating, embedding, storing, accessing, updating, revoking, and destroying fingerprints for ML models as per the security requirements. | Request the requirements for generating, embedding, storing, accessing, updating, revoking, and destroying fingerprints for ML models, their review process, and its review records. | Medium | Bigquery.FC6 | Bigquery.T4 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C90, depends on Bigquery.C89, assured by Bigquery.C91]  Ensure the fingerprints for ML models are generated, embedded, stored, accessed, updated, revoked, and destroyed as per the security requirements. | Request 1) the mechanism ensuring the fingerprints for ML models are generated, embedded, stored, accessed, updated, revoked, and destroyed as per the security requirements, 2) their records of execution for all new keys, and 3) the plan to move any older keys. | Medium | Bigquery.FC6 | Bigquery.T4 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C91]  Verify the fingerprints for ML models are generated, embedded, stored, accessed, updated, revoked, and destroyed as per the security requirements. | 1) Generate, 2) embed, 3) store, 4) access, 5) update, 6) revoke, or 7) destroy a fingerprint outside the security requirements; it should be detected. | High | Bigquery.FC6 | - | Medium |

## Ensure sensitive data is not added in the listing fields [Bigquery.CO27]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C101, assured by Bigquery.C102]  Ensure no sensitive data is included in the fields of the listings (i.e., displayName, description, documentation, icon). | Request the mechanism ensuring sensitive data is not included in the fields of listings, and the evidence of its execution. | Medium | Bigquery.FC9 | Bigquery.T31 (Medium) | Very Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C102]  Verify no sensitive data is included in the fields of listings. | Add sensitive data to a field of a listing; it should be detected. | High | Bigquery.FC9 | - | Very Low |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C110, depends on Bigquery.C22]  Maintain a list of authorized emails or URLs (i.e., primaryContact, requestAccess, dataProvider, or publisher) to be used by listings and data exchanges. | Request the list of all authorized emails to be used by listings and data exchanges, its review process, and its review records. | High | Bigquery.FC9 | Bigquery.T30 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C111, depends on Bigquery.C110, assured by Bigquery.C112]  Ensure listings and data exchanges use authorized emails. | Request 1) the mechanism ensuring only authorized emails are configured, 2) its records of execution for all new emails, and 3) the plan to move any older emails. | Medium | Bigquery.FC9 | Bigquery.T30 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C112]  Verify listings and data exchanges use authorized emails. | For a listing or data exchange, use an unauthorized email; it should be detected. | Medium | Bigquery.FC9 | - | Medium |

## Enforce access to sensitive data via data clean rooms [Bigquery.CO28]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C92]  Define the requirements to configure a data exchange as a data clean room (e.g., sharing sensitive data with 3rd parties). | Request the requirements to configure a data exchange as a data clean room, its review process, and its review records. | Low | Bigquery.FC9 | Bigquery.T28 (Very Low)  Bigquery.T30 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C93, depends on Bigquery.C92, assured by Bigquery.C94]  Ensure required data exchanges are configured as data clean rooms (i.e., sharingEnvironmentConfig.dcrExchangeConfig). | Request 1) the mechanism ensuring required data exchanges are configured as data clean rooms, 2) its records of execution for all new data exchanges, and 3) the plan to move any older data exchanges. | Medium | Bigquery.FC9 | Bigquery.T28 (High)  Bigquery.T30 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C94]  Verify all required data exchanges are configured as data clean rooms. | Configure a data exchange required to be a data clean room as a non-data clean room; it should be detected. | Low | Bigquery.FC9 | - | Medium |

## Restrict access to listings and data exchanges to authorized subscribers only [Bigquery.CO29]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C103, depends on Bigquery.C22]  Maintain the list of authorized subscriptions for each listing and data exchange. | Request the list of authorized subscriptions for each listing and/or data exchange, its review process, and its review records. | Low | Bigquery.FC9 | Bigquery.T28 (Very Low)  Bigquery.T29 (Very Low)  Bigquery.T32 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C104, depends on Bigquery.C103, assured by Bigquery.C105]  Ensure only authorized subscriptions for listings and data exchanges are configured. | Request 1) the mechanism ensuring only authorized subscriptions for listings and data exchanges are configured, 2) its records of execution for all new listings and/or data exchanges, and 3) the plan to move any older listings and/or data exchanges. | Medium | Bigquery.FC9 | Bigquery.T28 (High)  Bigquery.T29 (High)  Bigquery.T32 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C105]  Verify listings and data exchanges have only authorized subscriptions. | 1) Add an unauthorized subscription, or 2) remove the authorized subscription from a listing and/or data exchange; it should be detected. | Medium | Bigquery.FC9 | - | Medium |

## Restrict and manage subscriptions to authorized listings and data exchanges only [Bigquery.CO30]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C107]  Maintain the list of listings and/or data exchanges authorized to be subscribed to, and by whom. | Request the list of listings and data exchanges authorized to be subscribed to and by whom, their review process, and their review records. | Low | Bigquery.FC10 | Bigquery.T33 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C108, depends on Bigquery.C107, assured by Bigquery.C109]  Ensure only authorized entities you control are subscribed to the authorized listings and data exchanges. | Request 1) the mechanism ensuring only authorized entities you control are subscribed to authorized listings and data exchanges, 2) its records of execution for all new subscriptions on listings or data exchanges, and 3) the plan to move any older subscriptions on listings or data exchanges. | Medium | Bigquery.FC10 | Bigquery.T33 (High) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C109]  Verify only authorized entities you control are subscribed to authorized listings and data exchanges. | 1) Subscribe to an unauthorized listing and/or data exchange with an entity you control, or 2) subscribe with an unauthorized entity you control to a listing or exchange authorized for other entities you control; it should be detected. | Medium | Bigquery.FC10 | - | Low |

## Restrict the export of data by enabling restricted export [Bigquery.CO31]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C113, depends on Bigquery.C22]  Define the requirements for enabling restricted export for listings. | Request the requirements for enabling restricted export for listings, their review process, and their review records. | Low | Bigquery.FC9 | Bigquery.T30 (Very Low) | Very Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C114, depends on Bigquery.C92, assured by Bigquery.C115]  Ensure the restricted export for listings is enabled according to the requirements. | Request 1) the mechanism ensuring only restricted export is configured, 2) its records of execution for all new listings, and 3) the plan to move any older listings. | Medium | Bigquery.FC9 | Bigquery.T30 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C115]  Verify the restricted export for listings is enabled according to the requirements. | Enable the restricted export for listings outside the requirements; it should be detected. | High | Bigquery.FC9 | - | Medium |

## Enforce authorized access entities only, change management, and secure decommissioning on datasets [Bigquery.CO32]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C116]  Maintain the list of authorized access entities (i.e., role, userByEmail, groupByEmail, domain, specialGroup, iamMember, view, routine, or dataset) for each dataset. | Request the list of authorized access entities of each dataset, its review process, and its review records. | Low | Bigquery.FC1 | Bigquery.T21 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C117, depends on Bigquery.C116, assured by Bigquery.C118]  Ensure only authorized access entities of each dataset are configured. | Request 1) the mechanism ensuring only authorized access entities of each dataset are configured, 2) its records of execution for all new datasets, and 3) the plan to move any older datasets. | Medium | Bigquery.FC1 | Bigquery.T21 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C118]  Verify all datasets use their authorized access entity. | 1) Allow an unauthorized access entity on a dataset, or 2) remove an authorized access entity on a dataset; it should be detected. | Medium | Bigquery.FC1 | - | Medium |

## Define and enforce BigQuery configuration baselines at the organization and project levels [Bigquery.CO33]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C123]  Maintain the list of authorized configuration settings (e.g., default\_batch\_query\_queue\_timeout\_ms, default\_interactive\_query\_queue\_timeout\_ms, default\_query\_job\_timeout\_ms, enable\_fine\_grained\_dataset\_acls\_option) for each organization or project. | Request the list of authorized configuration settings for each organization or project, its review process, and its review records. | Low | Bigquery.FC1  Bigquery.FC4 | Bigquery.T9 (Very Low)  Bigquery.T13 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C124, depends on Bigquery.C123, assured by Bigquery.C125]  Ensure only authorized configuration settings for each organization or project are configured. | Request 1) the mechanism ensuring only authorized configuration settings for each organization or project are configured, 2) its records of execution for all new organizations or projects, and 3) the plan to move any older organizations or projects. | Medium | Bigquery.FC1  Bigquery.FC4 | Bigquery.T9 (Medium)  Bigquery.T13 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C125]  Verify all organizations or projects use their authorized configuration settings. | 1) Deploy unauthorized configuration settings on an organization or project, or 2) remove authorized configuration settings on an organization or project; it should be detected. | Medium | Bigquery.FC1  Bigquery.FC4 | - | Medium |

## Restrict and manage Gemini in BigQuery projects [Bigquery.CO34]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C126, depends on Bigquery.C127]  Ensure the Cloud AI Companion API is enabled/disabled for the BigQuery project following the Service Usage ThreatModel and is protected using Cloud AI Companion ThreatModel. | Request how the Service Usage ThreatModel and Cloud AI Companion ThreatModel are applied to the Cloud AI Companion API in the BigQuery project. | Medium | Bigquery.FC1 | Bigquery.T35 (High) | Low |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C127]  Maintain the list of authorized BigQuery projects allowed to use Gemini. | Request the list of authorized BigQuery projects allowed to use Gemini, its review process, and its review records. | Low | Bigquery.FC1 | Bigquery.T35 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C128, depends on Bigquery.C127, assured by Bigquery.C129]  Ensure only authorized BigQuery projects are allowed to use Gemini. | Request 1) the mechanism ensuring only authorized BigQuery projects are allowed to use Gemini, 2) its records of execution for all new BigQuery projects, and 3) the plan to move any older BigQuery projects. | Medium | Bigquery.FC1 | Bigquery.T35 (Medium) | Very Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C129]  Verify all authorized BigQuery projects are allowed to use Gemini. | 1) Enable Gemini in an unauthorized BigQuery project, or 2) disable Gemini from an authorized BigQuery project; it should be detected. | Medium | Bigquery.FC1 | - | Very Low |

# Compliance Mapping

## PCI DSS v4

| **PCI DSS v4** | **Control Objectives** | **Controls** | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **Very High** | **High** | **Medium** | **Low** | **Very Low** |
| 1.1 | [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls | Bigquery.C2  Bigquery.C121 | - | - | - | - |
| 1.2 | [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls  [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO24] Enforce secure SDLC processes on routines and queries  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO32] Enforce authorized access entities only, change management, and secure decommissioning on datasets  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels  [Bigquery.CO34] Restrict and manage Gemini in BigQuery projects | Bigquery.C2  Bigquery.C121  Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40  Bigquery.C122 | Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C74  Bigquery.C114  Bigquery.C115  Bigquery.C116  Bigquery.C117  Bigquery.C118  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C73  Bigquery.C126  Bigquery.C127 | Bigquery.C113  Bigquery.C128  Bigquery.C129 |
| 1.2.1 | [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls | Bigquery.C2  Bigquery.C121 | - | - | - | - |
| 1.2.3  1.2.4  1.2.5 | [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls  [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO24] Enforce secure SDLC processes on routines and queries  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO32] Enforce authorized access entities only, change management, and secure decommissioning on datasets  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels  [Bigquery.CO34] Restrict and manage Gemini in BigQuery projects | Bigquery.C2  Bigquery.C121  Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40  Bigquery.C122 | Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C74  Bigquery.C114  Bigquery.C115  Bigquery.C116  Bigquery.C117  Bigquery.C118  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C73  Bigquery.C126  Bigquery.C127 | Bigquery.C113  Bigquery.C128  Bigquery.C129 |
| 1.2.6 | [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls | Bigquery.C2  Bigquery.C121 | - | - | - | - |
| 1.2.7 | [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls  [Bigquery.CO7] Encrypt resources (e.g., datasets, models, data transfers) with customer-managed encryption keys and protect the keys  [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO10] Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO17] Register BigQuery models as per the requirements  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO24] Enforce secure SDLC processes on routines and queries  [Bigquery.CO27] Ensure sensitive data is not added in the listing fields  [Bigquery.CO29] Restrict access to listings and data exchanges to authorized subscribers only  [Bigquery.CO30] Restrict and manage subscriptions to authorized listings and data exchanges only  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO32] Enforce authorized access entities only, change management, and secure decommissioning on datasets  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels  [Bigquery.CO34] Restrict and manage Gemini in BigQuery projects | Bigquery.C2  Bigquery.C121  Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40  Bigquery.C122 | Bigquery.C26  Bigquery.C27  Bigquery.C29  Bigquery.C36  Bigquery.C37  Bigquery.C85  Bigquery.C86  Bigquery.C134  Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C22  Bigquery.C23  Bigquery.C24  Bigquery.C25  Bigquery.C135  Bigquery.C47  Bigquery.C48  Bigquery.C49  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C74  Bigquery.C110  Bigquery.C111  Bigquery.C112  Bigquery.C103  Bigquery.C104  Bigquery.C105  Bigquery.C114  Bigquery.C115  Bigquery.C116  Bigquery.C117  Bigquery.C118  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C28  Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C73  Bigquery.C107  Bigquery.C108  Bigquery.C109  Bigquery.C126  Bigquery.C127 | Bigquery.C101  Bigquery.C102  Bigquery.C113  Bigquery.C128  Bigquery.C129 |
| 1.2.8 | [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls | Bigquery.C2  Bigquery.C121 | - | - | - | - |
| 1.2.10 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls  [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO10] Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO17] Register BigQuery models as per the requirements  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels | Bigquery.C2  Bigquery.C121  Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40 | Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C22  Bigquery.C23  Bigquery.C24  Bigquery.C25  Bigquery.C135  Bigquery.C47  Bigquery.C48  Bigquery.C49  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C73 | - |
| 1.3 | [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls | Bigquery.C2  Bigquery.C121 | - | - | - | - |
| 1.3.1  1.3.2  1.3.3  1.4  1.4.1  1.4.2  1.4.3  1.4.5 | [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO24] Enforce secure SDLC processes on routines and queries  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO32] Enforce authorized access entities only, change management, and secure decommissioning on datasets  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels  [Bigquery.CO34] Restrict and manage Gemini in BigQuery projects | Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40  Bigquery.C122 | Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C74  Bigquery.C114  Bigquery.C115  Bigquery.C116  Bigquery.C117  Bigquery.C118  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C73  Bigquery.C126  Bigquery.C127 | Bigquery.C113  Bigquery.C128  Bigquery.C129 |
| 1.5  1.5.1  2.2.1 | [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls | Bigquery.C2  Bigquery.C121 | - | - | - | - |
| 2.3 | [Bigquery.CO7] Encrypt resources (e.g., datasets, models, data transfers) with customer-managed encryption keys and protect the keys | - | - | Bigquery.C26  Bigquery.C27  Bigquery.C29  Bigquery.C36  Bigquery.C37  Bigquery.C85  Bigquery.C86  Bigquery.C134 | Bigquery.C28 | - |
| 2.3.2  3.3.2 | [Bigquery.CO18] Limit the amount of cloned data  [Bigquery.CO28] Enforce access to sensitive data via data clean rooms | - | - | Bigquery.C92  Bigquery.C93  Bigquery.C94 | Bigquery.C50  Bigquery.C51  Bigquery.C52 | - |
| 3.4.1 | [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security  [Bigquery.CO9] De-identify sensitive data using Cloud DLP  [Bigquery.CO10] Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings  [Bigquery.CO27] Ensure sensitive data is not added in the listing fields  [Bigquery.CO28] Enforce access to sensitive data via data clean rooms | - | Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46  Bigquery.C20  Bigquery.C21  Bigquery.C22  Bigquery.C23  Bigquery.C24  Bigquery.C25  Bigquery.C135  Bigquery.C110  Bigquery.C111  Bigquery.C112  Bigquery.C92  Bigquery.C93  Bigquery.C94 | - | Bigquery.C101  Bigquery.C102 |
| 3.5.1 | [Bigquery.CO7] Encrypt resources (e.g., datasets, models, data transfers) with customer-managed encryption keys and protect the keys | - | - | Bigquery.C26  Bigquery.C27  Bigquery.C29  Bigquery.C36  Bigquery.C37  Bigquery.C85  Bigquery.C86  Bigquery.C134 | Bigquery.C28 | - |
| 3.5.1.1  3.5.1.2  3.5.1.3  3.6.1  3.6.1.1  3.6.1.2  3.6.1.3  3.6.1.4  3.7.1  3.7.2  3.7.3  3.7.4  3.7.5  3.7.6  3.7.7  3.7.9  4.2.1.1 | [Bigquery.CO24] Enforce secure SDLC processes on routines and queries | - | Bigquery.C122 | Bigquery.C74 | - | - |
| 6.2  6.2.1  6.2.2  6.2.3  6.2.4  6.5.5 | [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO24] Enforce secure SDLC processes on routines and queries  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO32] Enforce authorized access entities only, change management, and secure decommissioning on datasets  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels  [Bigquery.CO34] Restrict and manage Gemini in BigQuery projects | Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40  Bigquery.C122 | Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C74  Bigquery.C114  Bigquery.C115  Bigquery.C116  Bigquery.C117  Bigquery.C118  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C73  Bigquery.C126  Bigquery.C127 | Bigquery.C113  Bigquery.C128  Bigquery.C129 |
| 6.5.6 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security  [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO10] Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO17] Register BigQuery models as per the requirements  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels | Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14  Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46  Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C22  Bigquery.C23  Bigquery.C24  Bigquery.C25  Bigquery.C135  Bigquery.C47  Bigquery.C48  Bigquery.C49  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C73 | - |
| 7.1  7.2 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls  [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security  [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO10] Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO17] Register BigQuery models as per the requirements  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO29] Restrict access to listings and data exchanges to authorized subscribers only  [Bigquery.CO30] Restrict and manage subscriptions to authorized listings and data exchanges only  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels | Bigquery.C2  Bigquery.C121  Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14  Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46  Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C22  Bigquery.C23  Bigquery.C24  Bigquery.C25  Bigquery.C135  Bigquery.C47  Bigquery.C48  Bigquery.C49  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C103  Bigquery.C104  Bigquery.C105  Bigquery.C114  Bigquery.C115  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C73  Bigquery.C107  Bigquery.C108  Bigquery.C109 | Bigquery.C113 |
| 7.2.1  7.2.2 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO10] Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO17] Register BigQuery models as per the requirements  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels | Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40 | Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C22  Bigquery.C23  Bigquery.C24  Bigquery.C25  Bigquery.C135  Bigquery.C47  Bigquery.C48  Bigquery.C49  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C73 | - |
| 7.2.3 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO17] Register BigQuery models as per the requirements | - | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84 | Bigquery.C47  Bigquery.C48  Bigquery.C49 | - | - |
| 7.2.4 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls  [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security  [Bigquery.CO10] Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings  [Bigquery.CO17] Register BigQuery models as per the requirements  [Bigquery.CO29] Restrict access to listings and data exchanges to authorized subscribers only  [Bigquery.CO30] Restrict and manage subscriptions to authorized listings and data exchanges only  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels | Bigquery.C2  Bigquery.C121 | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46  Bigquery.C22  Bigquery.C23  Bigquery.C24  Bigquery.C25  Bigquery.C135  Bigquery.C47  Bigquery.C48  Bigquery.C49  Bigquery.C103  Bigquery.C104  Bigquery.C105  Bigquery.C114  Bigquery.C115  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C107  Bigquery.C108  Bigquery.C109 | Bigquery.C113 |
| 7.2.5 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls  [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security  [Bigquery.CO10] Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings  [Bigquery.CO15] Enable logs for BigQuery Data Transfer  [Bigquery.CO16] Monitor data protection, data ingestion, and data quality  [Bigquery.CO29] Restrict access to listings and data exchanges to authorized subscribers only  [Bigquery.CO30] Restrict and manage subscriptions to authorized listings and data exchanges only  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels | Bigquery.C2  Bigquery.C121 | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46  Bigquery.C22  Bigquery.C23  Bigquery.C24  Bigquery.C25  Bigquery.C135  Bigquery.C88  Bigquery.C103  Bigquery.C104  Bigquery.C105  Bigquery.C114  Bigquery.C115  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C41  Bigquery.C42  Bigquery.C65  Bigquery.C87  Bigquery.C107  Bigquery.C108  Bigquery.C109 | Bigquery.C113 |
| 7.2.6 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security  [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO10] Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO17] Register BigQuery models as per the requirements  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels | Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14  Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46  Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C22  Bigquery.C23  Bigquery.C24  Bigquery.C25  Bigquery.C135  Bigquery.C47  Bigquery.C48  Bigquery.C49  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C73 | - |
| 7.3  7.3.1  7.3.2  7.3.3 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security | - | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46 | - | - |
| 8.1  8.2 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security  [Bigquery.CO17] Register BigQuery models as per the requirements | - | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46  Bigquery.C47  Bigquery.C48  Bigquery.C49 | - | - |
| 8.2.2 | [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security | - | Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46 | - | - |
| 8.2.3 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security  [Bigquery.CO17] Register BigQuery models as per the requirements | - | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46  Bigquery.C47  Bigquery.C48  Bigquery.C49 | - | - |
| 8.2.4  8.2.6 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security | - | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46 | - | - |
| 8.3 | [Bigquery.CO7] Encrypt resources (e.g., datasets, models, data transfers) with customer-managed encryption keys and protect the keys  [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO24] Enforce secure SDLC processes on routines and queries  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO32] Enforce authorized access entities only, change management, and secure decommissioning on datasets  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels  [Bigquery.CO34] Restrict and manage Gemini in BigQuery projects | Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40  Bigquery.C122 | Bigquery.C26  Bigquery.C27  Bigquery.C29  Bigquery.C36  Bigquery.C37  Bigquery.C85  Bigquery.C86  Bigquery.C134  Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C74  Bigquery.C114  Bigquery.C115  Bigquery.C116  Bigquery.C117  Bigquery.C118  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C28  Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C73  Bigquery.C126  Bigquery.C127 | Bigquery.C113  Bigquery.C128  Bigquery.C129 |
| 8.3.2 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security | - | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46 | - | - |
| 8.3.3 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks | - | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84 | - | - | - |
| 8.3.8 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security | - | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46 | - | - |
| 8.3.9 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security  [Bigquery.CO17] Register BigQuery models as per the requirements | - | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46  Bigquery.C47  Bigquery.C48  Bigquery.C49 | - | - |
| 8.3.10 | [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO24] Enforce secure SDLC processes on routines and queries  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO32] Enforce authorized access entities only, change management, and secure decommissioning on datasets  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels  [Bigquery.CO34] Restrict and manage Gemini in BigQuery projects | Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40  Bigquery.C122 | Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C74  Bigquery.C114  Bigquery.C115  Bigquery.C116  Bigquery.C117  Bigquery.C118  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C73  Bigquery.C126  Bigquery.C127 | Bigquery.C113  Bigquery.C128  Bigquery.C129 |
| 8.5 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security | - | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46 | - | - |
| 8.5.1 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls  [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security  [Bigquery.CO10] Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings  [Bigquery.CO17] Register BigQuery models as per the requirements  [Bigquery.CO29] Restrict access to listings and data exchanges to authorized subscribers only  [Bigquery.CO30] Restrict and manage subscriptions to authorized listings and data exchanges only  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels | Bigquery.C2  Bigquery.C121 | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46  Bigquery.C22  Bigquery.C23  Bigquery.C24  Bigquery.C25  Bigquery.C135  Bigquery.C47  Bigquery.C48  Bigquery.C49  Bigquery.C103  Bigquery.C104  Bigquery.C105  Bigquery.C114  Bigquery.C115  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C107  Bigquery.C108  Bigquery.C109 | Bigquery.C113 |
| 8.6  8.6.1 | [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security  [Bigquery.CO9] De-identify sensitive data using Cloud DLP  [Bigquery.CO10] Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings  [Bigquery.CO27] Ensure sensitive data is not added in the listing fields  [Bigquery.CO28] Enforce access to sensitive data via data clean rooms | - | Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46  Bigquery.C20  Bigquery.C21  Bigquery.C22  Bigquery.C23  Bigquery.C24  Bigquery.C25  Bigquery.C135  Bigquery.C110  Bigquery.C111  Bigquery.C112  Bigquery.C92  Bigquery.C93  Bigquery.C94 | - | Bigquery.C101  Bigquery.C102 |
| 9.4  9.4.1 | [Bigquery.CO3] Ensure backup, failover, and recovery capabilities for BigQuery resources (e.g., snapshots and exports for datasets and tables, failover procedures for reservations) | - | - | Bigquery.C3  Bigquery.C4  Bigquery.C5 | Bigquery.C130  Bigquery.C131 | Bigquery.C132 |
| 9.4.1.1  9.4.1.2 | [Bigquery.CO5] Restrict access to columns and protect sensitive data  [Bigquery.CO6] Restrict access to rows with BigQuery row-level security  [Bigquery.CO18] Limit the amount of cloned data  [Bigquery.CO27] Ensure sensitive data is not added in the listing fields | - | Bigquery.C9  Bigquery.C12  Bigquery.C13  Bigquery.C14 | Bigquery.C10  Bigquery.C11  Bigquery.C44  Bigquery.C45  Bigquery.C46  Bigquery.C110  Bigquery.C111  Bigquery.C112 | Bigquery.C50  Bigquery.C51  Bigquery.C52 | Bigquery.C101  Bigquery.C102 |
| 9.4.2 | [Bigquery.CO12] Set the expiration time of BigQuery tables as per the requirements  [Bigquery.CO25] Set an authorized expiration time for each ML model | - | - | Bigquery.C32  Bigquery.C33  Bigquery.C34  Bigquery.C136  Bigquery.C78  Bigquery.C79  Bigquery.C80 | - | - |
| 9.4.7 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO15] Enable logs for BigQuery Data Transfer  [Bigquery.CO16] Monitor data protection, data ingestion, and data quality  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO24] Enforce secure SDLC processes on routines and queries  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO32] Enforce authorized access entities only, change management, and secure decommissioning on datasets  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels  [Bigquery.CO34] Restrict and manage Gemini in BigQuery projects | Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40  Bigquery.C122 | Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C88  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C74  Bigquery.C114  Bigquery.C115  Bigquery.C116  Bigquery.C117  Bigquery.C118  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C41  Bigquery.C42  Bigquery.C65  Bigquery.C87  Bigquery.C73  Bigquery.C126  Bigquery.C127 | Bigquery.C113  Bigquery.C128  Bigquery.C129 |
| 10.2  10.2.1  10.2.1.1 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO10] Secure the authorized sources and destinations used for datasets, tables, models, connections, jobs, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO15] Enable logs for BigQuery Data Transfer  [Bigquery.CO16] Monitor data protection, data ingestion, and data quality  [Bigquery.CO17] Register BigQuery models as per the requirements  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO24] Enforce secure SDLC processes on routines and queries  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO32] Enforce authorized access entities only, change management, and secure decommissioning on datasets  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels  [Bigquery.CO34] Restrict and manage Gemini in BigQuery projects | Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40  Bigquery.C122 | Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C22  Bigquery.C23  Bigquery.C24  Bigquery.C25  Bigquery.C135  Bigquery.C88  Bigquery.C47  Bigquery.C48  Bigquery.C49  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C74  Bigquery.C114  Bigquery.C115  Bigquery.C116  Bigquery.C117  Bigquery.C118  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C41  Bigquery.C42  Bigquery.C65  Bigquery.C87  Bigquery.C73  Bigquery.C126  Bigquery.C127 | Bigquery.C113  Bigquery.C128  Bigquery.C129 |
| 10.2.1.2 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO15] Enable logs for BigQuery Data Transfer  [Bigquery.CO16] Monitor data protection, data ingestion, and data quality  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO24] Enforce secure SDLC processes on routines and queries  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO32] Enforce authorized access entities only, change management, and secure decommissioning on datasets  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels  [Bigquery.CO34] Restrict and manage Gemini in BigQuery projects | Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40  Bigquery.C122 | Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C88  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C74  Bigquery.C114  Bigquery.C115  Bigquery.C116  Bigquery.C117  Bigquery.C118  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C41  Bigquery.C42  Bigquery.C65  Bigquery.C87  Bigquery.C73  Bigquery.C126  Bigquery.C127 | Bigquery.C113  Bigquery.C128  Bigquery.C129 |
| 10.2.1.3  10.2.1.4  10.2.1.5  10.2.1.6  10.2.1.7  10.2.2 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO15] Enable logs for BigQuery Data Transfer | - | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84 | Bigquery.C88 | Bigquery.C41 | - |
| 10.3.3  10.4  10.4.1  10.4.1.1 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO15] Enable logs for BigQuery Data Transfer  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO24] Enforce secure SDLC processes on routines and queries  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO32] Enforce authorized access entities only, change management, and secure decommissioning on datasets  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels  [Bigquery.CO34] Restrict and manage Gemini in BigQuery projects | Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84  Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40  Bigquery.C122 | Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C88  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C74  Bigquery.C114  Bigquery.C115  Bigquery.C116  Bigquery.C117  Bigquery.C118  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C41  Bigquery.C73  Bigquery.C126  Bigquery.C127 | Bigquery.C113  Bigquery.C128  Bigquery.C129 |
| 10.6  10.6.1  10.6.2  10.6.3 | [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO24] Enforce secure SDLC processes on routines and queries  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO32] Enforce authorized access entities only, change management, and secure decommissioning on datasets  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels  [Bigquery.CO34] Restrict and manage Gemini in BigQuery projects | Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40  Bigquery.C122 | Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C74  Bigquery.C114  Bigquery.C115  Bigquery.C116  Bigquery.C117  Bigquery.C118  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C73  Bigquery.C126  Bigquery.C127 | Bigquery.C113  Bigquery.C128  Bigquery.C129 |
| 10.7  10.7.1  10.7.2  10.7.3 | [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls  [Bigquery.CO8] Enforce authorized configurations on BigQuery datasets, tables, reservations, assignments, asynchronous query jobs, BigQuery sharing's data exchanges, and listings  [Bigquery.CO14] Limit use of BigQuery Omni  [Bigquery.CO19] Enforce authorized configurations on jobs  [Bigquery.CO21] Use authorized metadata caching  [Bigquery.CO23] Use authorized User-Defined Functions  [Bigquery.CO24] Enforce secure SDLC processes on routines and queries  [Bigquery.CO31] Restrict the export of data by enabling restricted export  [Bigquery.CO32] Enforce authorized access entities only, change management, and secure decommissioning on datasets  [Bigquery.CO33] Define and enforce BigQuery configuration baselines at the organization and project levels  [Bigquery.CO34] Restrict and manage Gemini in BigQuery projects | Bigquery.C2  Bigquery.C121  Bigquery.C15  Bigquery.C16  Bigquery.C60 | Bigquery.C17  Bigquery.C75  Bigquery.C81  Bigquery.C38  Bigquery.C39  Bigquery.C40  Bigquery.C122 | Bigquery.C18  Bigquery.C19  Bigquery.C61  Bigquery.C62  Bigquery.C63  Bigquery.C64  Bigquery.C82  Bigquery.C83  Bigquery.C98  Bigquery.C106  Bigquery.C133  Bigquery.C53  Bigquery.C54  Bigquery.C55  Bigquery.C57  Bigquery.C58  Bigquery.C59  Bigquery.C70  Bigquery.C71  Bigquery.C72  Bigquery.C74  Bigquery.C114  Bigquery.C115  Bigquery.C116  Bigquery.C117  Bigquery.C118  Bigquery.C123  Bigquery.C124  Bigquery.C125 | Bigquery.C76  Bigquery.C77  Bigquery.C95  Bigquery.C96  Bigquery.C97  Bigquery.C99  Bigquery.C100  Bigquery.C73  Bigquery.C126  Bigquery.C127 | Bigquery.C113  Bigquery.C128  Bigquery.C129 |
| 11.2 | [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls | Bigquery.C2  Bigquery.C121 | - | - | - | - |
| 11.2.1  11.2.2  11.4.5  11.4.6  11.5.1 | [Bigquery.CO15] Enable logs for BigQuery Data Transfer  [Bigquery.CO16] Monitor data protection, data ingestion, and data quality  [Bigquery.CO20] Monitor abnormal performance of queries | - | - | Bigquery.C88  Bigquery.C56 | Bigquery.C41  Bigquery.C42  Bigquery.C65  Bigquery.C87 | - |
| 11.5.1.1 | [Bigquery.CO7] Encrypt resources (e.g., datasets, models, data transfers) with customer-managed encryption keys and protect the keys | - | - | Bigquery.C26  Bigquery.C27  Bigquery.C29  Bigquery.C36  Bigquery.C37  Bigquery.C85  Bigquery.C86  Bigquery.C134 | Bigquery.C28 | - |
| 12.3.3 | [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls | Bigquery.C2  Bigquery.C121 | - | - | - | - |
| 12.5.2 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO15] Enable logs for BigQuery Data Transfer | - | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84 | Bigquery.C88 | Bigquery.C41 | - |
| 12.10.5 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO16] Monitor data protection, data ingestion, and data quality  [Bigquery.CO20] Monitor abnormal performance of queries | - | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84 | Bigquery.C56 | Bigquery.C42  Bigquery.C65  Bigquery.C87 | - |
| 15.1 | [Bigquery.CO2] Enforce network-level restrictions leveraging VPC origin and VPC Service Controls | Bigquery.C2  Bigquery.C121 | - | - | - | - |
| A1.1.4  A3.2.1  A3.2.4 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks  [Bigquery.CO16] Monitor data protection, data ingestion, and data quality  [Bigquery.CO20] Monitor abnormal performance of queries | - | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84 | Bigquery.C56 | Bigquery.C42  Bigquery.C65  Bigquery.C87 | - |
| A3.2.6.1 | [Bigquery.CO1] Limit access to the IAM actions required to execute attacks | - | Bigquery.C1  Bigquery.C6  Bigquery.C7  Bigquery.C8  Bigquery.C84 | - | - | - |

*The Control Objectives are mapped to the* [*Secure Controls Framework*](https://www.securecontrolsframework.com/secure-controls-framework) *(SCF), provided under Attribution-NoDerivatives 4.0 International (CC BY-ND 4.0). Compliance mappings are not designed to fully ensure compliance with a specific governance or compliance standard. You are responsible for making your own assessment of whether your use of the Services meets applicable legal and regulatory requirements.*

*You can change the displayed Compliance mappings by contacting* [*chatbot@trustoncloud.com*](mailto:chatbot@trustoncloud.com)*.*

# Appendixes

## Appendix 1 - Prioritized list for control implementation

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C2]  Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy) following the Compute ThreatModel. | Request how the Compute ThreatModel is applied for enforcing VPC origin. | Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC4  Bigquery.FC5  Bigquery.FC6  Bigquery.FC7  Bigquery.FC8  Bigquery.FC9 | Bigquery.T1 (High)  Bigquery.T3 (High)  Bigquery.T4 (High)  Bigquery.T5 (High)  Bigquery.T6 (High)  Bigquery.T8 (High)  Bigquery.T9 (High)  Bigquery.T10 (High)  Bigquery.T11 (High)  Bigquery.T12 (High)  Bigquery.T13 (High)  Bigquery.T14 (High)  Bigquery.T17 (High)  Bigquery.T18 (High)  Bigquery.T19 (High)  Bigquery.T20 (High)  Bigquery.T21 (High)  Bigquery.T22 (High)  Bigquery.T24 (High)  Bigquery.T26 (High)  Bigquery.T27 (High)  Bigquery.T28 (High)  Bigquery.T29 (High)  Bigquery.T30 (High)  Bigquery.T31 (High)  Bigquery.T32 (High)  Bigquery.T34 (High)  Bigquery.T36 (High) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C121]  Enforce VPC Service Controls considering the environment's sensitivity (e.g., Prod vs. Non-Prod) using the Access Context Manager ThreatModel. | Request how the Access Context Manager ThreatModel is applied for enforcing VPC Service Controls. | Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC4  Bigquery.FC5  Bigquery.FC6  Bigquery.FC7  Bigquery.FC8  Bigquery.FC9 | Bigquery.T1 (High)  Bigquery.T3 (High)  Bigquery.T4 (High)  Bigquery.T5 (High)  Bigquery.T6 (High)  Bigquery.T8 (High)  Bigquery.T9 (High)  Bigquery.T10 (High)  Bigquery.T11 (High)  Bigquery.T12 (High)  Bigquery.T13 (High)  Bigquery.T14 (High)  Bigquery.T17 (High)  Bigquery.T18 (High)  Bigquery.T19 (High)  Bigquery.T20 (High)  Bigquery.T21 (High)  Bigquery.T22 (High)  Bigquery.T24 (High)  Bigquery.T26 (High)  Bigquery.T27 (High)  Bigquery.T28 (High)  Bigquery.T29 (High)  Bigquery.T30 (High)  Bigquery.T31 (High)  Bigquery.T32 (High)  Bigquery.T34 (High)  Bigquery.T36 (High) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C15, assured by Bigquery.C16]  Ensure no dataset is accessible to "AllUsers" or "AllAuthenticatedUsers", except if allowed. | Request 1) the mechanism ensuring no dataset is accessible to "AllUsers" or "AllAuthenticatedUsers", 2) its records of execution for all datasets, and 3) the plan to move any older datasets. | Low | Bigquery.FC1  Bigquery.FC2 | Bigquery.T8 (High)  Bigquery.T9 (High) | Very High |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C16]  Verify no dataset is accessible to "AllUsers" or "AllAuthenticatedUsers" (e.g., using the Security Command Center finding [PUBLIC\_DATASET](https://docs.cloud.google.com/security-command-center/docs/concepts-vulnerabilities-findings#dataset-findings)). | Modify a dataset to allow access to 1) "AllUsers", or 2) "AllAuthenticatedUsers"; it should be detected. | Very Low | Bigquery.FC1  Bigquery.FC2 | - | Very High |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C60]  Define the authorized configuration for each reservation (i.e., maxSlots, edition, ignoreIdleSlots, autoscale, secondaryLocation) and its assignments (i.e., assignee, jobType). | Request the authorized configuration for each reservation and its assignments. | Low | Bigquery.FC1  Bigquery.FC5 | Bigquery.T9 (Very Low)  Bigquery.T12 (Very Low) | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C1]  Limit the access to the IAM actions required to perform attacks, following the IAM Operating Model and using the IAM ThreatModel. | Request the list of authorized IAM members that have the permissions required to launch attacks, its review process, and its review records. | High | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3  Bigquery.FC4  Bigquery.FC5  Bigquery.FC6  Bigquery.FC7  Bigquery.FC8  Bigquery.FC9  Bigquery.FC10 | Bigquery.T1 (Very High)  Bigquery.T2 (Very High)  Bigquery.T3 (Very High)  Bigquery.T4 (Very High)  Bigquery.T5 (Very High)  Bigquery.T6 (Very High)  Bigquery.T8 (Very High)  Bigquery.T9 (Very High)  Bigquery.T10 (Very High)  Bigquery.T11 (Very High)  Bigquery.T12 (Very High)  Bigquery.T13 (Very High)  Bigquery.T14 (Very High)  Bigquery.T15 (Very High)  Bigquery.T17 (Very High)  Bigquery.T18 (Very High)  Bigquery.T19 (Very High)  Bigquery.T20 (Very High)  Bigquery.T21 (Very High)  Bigquery.T22 (Very High)  Bigquery.T24 (Very High)  Bigquery.T25 (Very High)  Bigquery.T26 (Very High)  Bigquery.T27 (Very High)  Bigquery.T28 (Very High)  Bigquery.T29 (Very High)  Bigquery.T30 (Very High)  Bigquery.T31 (Very High)  Bigquery.T32 (Very High)  Bigquery.T33 (Very High)  Bigquery.T34 (Very High)  Bigquery.T35 (Very High)  Bigquery.T36 (Very High) | High |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C6]  Maintain a list of authorized IAM entities allowed to access the tables, views, and table data in a specific dataset (note: columns can be made case-sensitive, and a default value can be set for columns). | Request the list of authorized IAM entities allowed to access the tables, views, and table data in a specific dataset, its review process, and its review records. | Very Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3 | Bigquery.T2 (Very Low)  Bigquery.T3 (Very Low)  Bigquery.T5 (Very Low)  Bigquery.T6 (Very Low)  Bigquery.T8 (Very Low)  Bigquery.T9 (Very Low)  Bigquery.T11 (Very Low)  Bigquery.T21 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C7, depends on Bigquery.C6, assured by Bigquery.C8]  Ensure only authorized IAM entities are allowed to access the tables, views, and table data in each dataset. | Request 1) the mechanism ensuring only authorized IAM entities are allowed to access the tables, views, and table data in a specific dataset, 2) its records of execution for all new IAM entities, and 3) the plan to move any older IAM entities. | Medium | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3 | Bigquery.T2 (High)  Bigquery.T3 (High)  Bigquery.T5 (High)  Bigquery.T6 (High)  Bigquery.T8 (High)  Bigquery.T9 (High)  Bigquery.T11 (High)  Bigquery.T21 (Medium) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C8]  Verify only authorized IAM entities are allowed to access the tables, views, and table data in each dataset. | Configure an unauthorized IAM entity to have access to 1) a table or 2) a view; it should be detected. | Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3 | - | High |
| Preventative (COSO)  Protect (NIST CSF) | [Bigquery.C84, depends on Bigquery.C81,Bigquery.C75,Bigquery.C60,Bigquery.C17]  Prevent the unauthorized access/creation/modification/deletion of BigQuery resources (e.g., datasets, tables) (e.g., by using an IAM policy with an allow/deny statement on "bigquery.tables.\*" and/or "bigquery.datasets.\*" with the tags and the authorized value for the conditions "resource.type" = "authorized type", "resource.name" = "authorized name"). | Create/update/delete an unauthorized BigQuery resource; it should be denied. | Low | Bigquery.FC1  Bigquery.FC5 | Bigquery.T1 (High)  Bigquery.T5 (High)  Bigquery.T12 (High)  Bigquery.T21 (High) | High |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C9]  Define the criteria for the sensitivity of columns in each table and each view, and their requirements for data protection (e.g., using BigQuery column-level security, column-level data masking, custom masking routines, restriction analysis rules, list overlap analysis rules, aggregation threshold analysis rules, differential privacy clauses, or data clean rooms). | Request the criteria for the sensitivity of columns in a table and each view and their requirements for data protection. | Very Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3  Bigquery.FC9 | Bigquery.T2 (Very Low)  Bigquery.T6 (Very Low)  Bigquery.T8 (Very Low)  Bigquery.T9 (Very Low)  Bigquery.T26 (Very Low)  Bigquery.T28 (Very Low)  Bigquery.T30 (Very Low) | High |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C12]  Define the criteria for the sensitivity of rows in each table. | Request the criteria for the sensitivity of rows in a table. | Very Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3  Bigquery.FC9 | Bigquery.T2 (Very Low)  Bigquery.T6 (Very Low)  Bigquery.T8 (Very Low)  Bigquery.T9 (Very Low)  Bigquery.T28 (Very Low)  Bigquery.T30 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C13, depends on Bigquery.C12, assured by Bigquery.C14]  Ensure only authorized IAM entities are allowed to access sensitive rows of a table (e.g., using BigQuery row-level security). | Request 1) the mechanism ensuring only authorized IAM entities are allowed to access sensitive rows of a table, 2) its records of execution for all new IAM entities, and 3) the plan to move any older IAM entities. | Medium | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3  Bigquery.FC9 | Bigquery.T2 (Medium)  Bigquery.T6 (High)  Bigquery.T8 (Medium)  Bigquery.T9 (High)  Bigquery.T28 (Medium)  Bigquery.T30 (Medium) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C14]  Verify only authorized IAM entities are allowed to access sensitive rows of a table. | Configure an unauthorized IAM entity with access to a sensitive row; it should be detected. | Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3  Bigquery.FC9 | - | High |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C17]  Define the authorized configuration (i.e., defaultTableExpirationMs, defaultPartitionExpirationMs, defaultEncryptionConfiguration, linkedDatasetSource, externalDatasetReference, defaultCollation, defaultRoundingMode, maxTimeTravelHours, storageBillingModel, and defaultEncryptionConfiguration) for each BigQuery dataset. | Request the authorized configuration for each BigQuery dataset, its review process, and its review records. | Low | Bigquery.FC1  Bigquery.FC2 | Bigquery.T8 (Very Low)  Bigquery.T11 (Very Low)  Bigquery.T21 (Very Low)  Bigquery.T25 (Very Low) | High |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C75]  Define the authorized configuration (e.g., createDisposition, writeDisposition, schemaUpdateOptions) for each asynchronous query job. | Request the authorized configuration for each asynchronous query job, its review process, and its review records. | Low | Bigquery.FC1 | Bigquery.T20 (Very Low) | High |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C81]  Define the authorized configuration (i.e., schema, clustering, expirationTime, view, materializedView, externalDataConfiguration, encryptionConfiguration, defaultCollation, defaultRoundingMode, and tableConstraints) for each BigQuery table. | Request the authorized configuration for each BigQuery table, its review process, and its review records. | Medium | Bigquery.FC1 | Bigquery.T1 (Very Low)  Bigquery.T5 (Very Low)  Bigquery.T25 (Very Low) | High |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C38]  Define the requirements for using BigQuery Omni (AWS and/or Azure). | Request the requirements for the use of BigQuery Omni. | Low | Bigquery.FC3  Bigquery.FC5 | Bigquery.T15 (Very Low)  Bigquery.T36 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C39, depends on Bigquery.C38, assured by Bigquery.C40]  Ensure the use of BigQuery Omni as per the requirements (e.g., using organizational constraints [constraints/bigquery.disableBQOmniAWS](https://docs.cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints) and [constraints/bigquery.disableBQOmniAzure](https://docs.cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints)). | Request the implementation to ensure the use of BigQuery Omni as per the requirements and its records of execution. | Medium | Bigquery.FC3  Bigquery.FC5 | Bigquery.T15 (Very High)  Bigquery.T36 (Very Low) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C40]  Verify the use of BigQuery Omni as per the requirements. | Use BigQuery Omni outside the requirements; it should be detected. | Low | Bigquery.FC3  Bigquery.FC5 | - | High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C122]  Enforce secure SDLC processes on queries (e.g., using source control, static analysis, dynamic analysis, and peer review). | Request 1) the processes and records of enforcing a secure SDLC on queries, 2) the records of execution for all new queries, and 3) the plan to move any older queries. | Medium | Bigquery.FC1 | Bigquery.T9 (High) | High |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C3]  Define the requirements for the backup of each BigQuery dataset, table, and model. | Request the backup requirements for each BigQuery dataset, table, and model. | Low | Bigquery.FC1  Bigquery.FC6  Bigquery.FC7 | Bigquery.T1 (Very Low)  Bigquery.T14 (Very Low)  Bigquery.T21 (Very Low)  Bigquery.T22 (Very Low)  Bigquery.T27 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C4, depends on Bigquery.C3, assured by Bigquery.C5]  Ensure each BigQuery dataset, table, and model is backed up (e.g., by creating snapshots or exports) according to the requirements and is restorable. | Request the mechanism ensuring BigQuery datasets, tables, and models are backed up (e.g., by creating snapshots or exports) according to their requirements, the evidence of their execution, and their regular testing of restoration. | High | Bigquery.FC1  Bigquery.FC6  Bigquery.FC7 | Bigquery.T1 (High)  Bigquery.T14 (High)  Bigquery.T21 (High)  Bigquery.T22 (High)  Bigquery.T27 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C5]  Verify all BigQuery datasets, tables, and models are backed up according to the requirements. | Change the backup mechanism to be outside the requirements; it should be detected. | High | Bigquery.FC1  Bigquery.FC6  Bigquery.FC7 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C10, depends on Bigquery.C9, assured by Bigquery.C11]  Ensure only authorized IAM entities are allowed to access sensitive columns of tables and views. | Request 1) the mechanism ensuring only authorized IAM entities are allowed to access sensitive columns of tables and views, 2) its records of execution for all new IAM entities, and 3) the plan to move any older IAM entities. | Medium | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3  Bigquery.FC9 | Bigquery.T2 (High)  Bigquery.T6 (High)  Bigquery.T8 (Medium)  Bigquery.T9 (Medium)  Bigquery.T26 (Medium)  Bigquery.T28 (Medium)  Bigquery.T30 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C11]  Verify only authorized IAM entities are allowed to access sensitive columns of each table and each view. | Configure an unauthorized IAM entity with access to a sensitive column; it should be detected. | Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3  Bigquery.FC9 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C44]  Define the criteria to use authorized data policies for each column in each table. | Request the criteria for using data policies for each column in each table. | Very Low | Bigquery.FC3  Bigquery.FC8 | Bigquery.T2 (Very Low)  Bigquery.T17 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C45, depends on Bigquery.C44, assured by Bigquery.C46]  Ensure only authorized IAM entities are allowed to access sensitive columns of a table by using data policies. | Request 1) the mechanism ensuring only authorized IAM entities are allowed to access sensitive columns of a table with data policies, 2) its records of execution for all new IAM entities, and 3) the plan to move any older IAM entities. | Medium | Bigquery.FC3  Bigquery.FC8 | Bigquery.T2 (Medium)  Bigquery.T17 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C46]  Verify only authorized IAM entities are allowed to access sensitive columns of a table by using data policies. | Configure an unauthorized IAM entity with access to a sensitive column in a data policy; it should be detected. | Low | Bigquery.FC3  Bigquery.FC8 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C26]  Maintain a list of authorized CMEKs to be used with each BigQuery resource (e.g., dataset, DLP function, model, data transfer), ideally dedicated (e.g., using Autokey on bigquery.googleapis.com/Dataset), and of the default CMEK at the project or organization level, and define the requirement to rotate key versions for tables. | Request the list of authorized CMEKs and their versions to be used by the BigQuery resource and the default CMEK per project or at the organization level, and the requirement to rotate key versions for tables, their review process, and their review records. | Very Low | Bigquery.FC1 | Bigquery.T11 (Very Low)  Bigquery.T20 (Very Low)  Bigquery.T21 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C27, depends on Bigquery.C26, assured by Bigquery.C29]  Ensure only authorized CMEKs and their versions are used with the BigQuery resource. | Request 1) the mechanism ensuring only authorized CMEKs are configured, 2) its records of execution for all new BigQuery resources, and 3) the plan to move any older BigQuery resources. | Medium | Bigquery.FC1 | Bigquery.T11 (Medium)  Bigquery.T20 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C29]  Verify each BigQuery resource is encrypted using an authorized CMEK and its version. | Use an unauthorized 1) CMEK or a 2) version with a BigQuery resource; it should be detected. | Low | Bigquery.FC1 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C36, depends on Bigquery.C26, assured by Bigquery.C37]  Ensure [AEAD encryption functions](https://docs.cloud.google.com/bigquery/docs/column-key-encrypt) are used to encrypt data at the column level. | Request the mechanism ensuring AEAD encryption functions are used to encrypt data at the column level. | Medium | Bigquery.FC1 | Bigquery.T11 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C37]  Verify AEAD encryption functions are used to encrypt data at the column level. | Do not encrypt the data at the column level; it should be detected. | Low | Bigquery.FC1 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C85, depends on Bigquery.C26]  Define the requirements for generating, storing, accessing, distributing, rotating, backing up, and destroying encryption keys for applications (e.g., by using a dedicated secret management tool such as HashiCorp Vault or GCP Secret Manager) as per the security standards. | Request the requirements for generating, storing, accessing, distributing, using, rotating, backing up, and destroying keys for applications, their review process, and its review records. | Medium | Bigquery.FC1 | Bigquery.T20 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C86, depends on Bigquery.C85,Bigquery.C26]  Ensure the keys for applications are generated, stored, accessed, distributed, rotated, backed up, and destroyed as per the security standards. | Request 1) the mechanism ensuring the keys for applications are generated, stored, accessed, distributed, rotated, backed up, and destroyed as per the security standards, 2) its records of execution for all new keys, and 3) the plan to move any older keys. | Medium | Bigquery.FC1 | Bigquery.T20 (High) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Bigquery.C134, depends on Bigquery.C26]  Prevent the creation of a dataset without an authorized key (e.g., using a custom constraint resourceType:[bigquery.googleapis.com/Dataset](https://docs.cloud.google.com/bigquery/docs/custom-constraints#supported_resources), resource(s): resource.defaultEncryptionConfiguration.kmsKeyName != an authorized encryption key, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | Create a dataset with unauthorized key; it should be denied. | Medium | Bigquery.FC1 | Bigquery.T21 (High) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C18, depends on Bigquery.C17, assured by Bigquery.C19]  Ensure the configuration of each BigQuery dataset is authorized. | Request the mechanism ensuring the configuration of each BigQuery dataset is authorized, and the evidence of its execution. | High | Bigquery.FC1  Bigquery.FC2 | Bigquery.T8 (High)  Bigquery.T11 (High)  Bigquery.T21 (High)  Bigquery.T25 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C19]  Verify all BigQuery datasets have authorized configurations. | Create a dataset with an unauthorized configuration; it should be detected. | High | Bigquery.FC1  Bigquery.FC2 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C61, depends on Bigquery.C60, assured by Bigquery.C62]  Ensure each reservation and its assignments use an authorized configuration. | Request the mechanism ensuring the reservation and its assignments use an authorized configuration, and the evidence of its execution. | High | Bigquery.FC5 | Bigquery.T12 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C62]  Verify all reservations and their assignments use an authorized configuration. | Use an unauthorized configuration with 1) a reservation, or 2) an assignment; it should be detected. | High | Bigquery.FC5 | - | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C63, depends on Bigquery.C60]  Monitor the creation/modification of unauthorized reservations (e.g., by using Cloud Logging event "google.cloud.bigquery.reservation.v1.ReservationService.CreateReservation" and "google.cloud.bigquery.reservation.v1.ReservationService.UpdateReservation", and their fields request.reservation.autoscale.maxSlots and request.reservation.edition). | Create/update the reservation with unauthorized values; it should be detected. | Medium | Bigquery.FC5 | Bigquery.T12 (Medium) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C64, depends on Bigquery.C60]  Monitor the creation/modification of unauthorized assignments (e.g., by using Cloud Logging event "google.cloud.bigquery.reservation.v1.ReservationService.CreateAssignment" and its fields request.assignment.assignee, request.assignment.jobType, and request.parent, and event "google.cloud.bigquery.reservation.v1.ReservationService.UpdateAssignment" and its fields request.assignment.assignee and request.assignment.jobType). | Create/update the assignment with unauthorized values; it should be detected. | Medium | Bigquery.FC5 | Bigquery.T12 (Medium) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C82, depends on Bigquery.C81, assured by Bigquery.C83]  Ensure the configuration of each BigQuery table is authorized. | Request the mechanism ensuring the configuration of each BigQuery table is authorized, and the evidence of its execution. | High | Bigquery.FC1 | Bigquery.T1 (Low)  Bigquery.T5 (Medium)  Bigquery.T25 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C83]  Verify all BigQuery tables have authorized configurations. | Create a table with an unauthorized configuration; it should be detected. | High | Bigquery.FC1 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C98]  Define the authorized configuration (i.e., displayName, description, documentation, icon, discoveryType, RestrictedExportConfig, logLinkedDatasetQueryUserEmail = true) for each listing and identify the requirements for deploying a public listing. | Request the authorized configuration for each listing and requirement for its discovery type, its review process, and its review records. | Low | Bigquery.FC9 | Bigquery.T28 (Very Low)  Bigquery.T30 (Very Low)  Bigquery.T31 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C106, depends on Bigquery.C98]  Protect the Pub/Sub topic used by a listing, using the Pub/Sub ThreatModel. | Request how the Pub/Sub ThreatModel is applied to topics used by a listing. | High | Bigquery.FC9 | Bigquery.T30 (High) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Bigquery.C133, depends on Bigquery.C17]  Prevent the creation/update of a dataset without an authorized configuration (e.g., using a custom constraint resourceType:[bigquery.googleapis.com/Dataset](https://docs.cloud.google.com/bigquery/docs/custom-constraints#supported_resources), resource(s): resource.defaultCollation != an authorized collation, resource.defaultRoundingMode != an authorized rounding mode, resource.maxTimeTravelHours != an authorized time travel window, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | Create or update a dataset with unauthorized configuration; it should be denied. | Medium | Bigquery.FC1 | Bigquery.T21 (High) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C20, assured by Bigquery.C21]  Ensure sensitive data is identified and redacted (e.g., using Cloud DLP). | Request the mechanism to identify and redact sensitive data. | High | Bigquery.FC1 | Bigquery.T6 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C21]  Verify sensitive data is identified and redacted (e.g., using Cloud DLP). | Add non-redacted sensitive data; it should be detected. | High | Bigquery.FC1 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C22]  Maintain a list of authorized sources and destinations (e.g., Cloud Storage, BigQuery, Vertex AI (for LLM, via BigQuery connection only)) to be used with each dataset, table, model, connection, job, and listing. | Request the list of all authorized sources and destinations to be used with each dataset, table, model, connection, job, and listing, its review process, and its review records. | High | Bigquery.FC1  Bigquery.FC3  Bigquery.FC6  Bigquery.FC9 | Bigquery.T2 (Very Low)  Bigquery.T3 (Very Low)  Bigquery.T6 (Very Low)  Bigquery.T15 (Very Low)  Bigquery.T18 (Very Low)  Bigquery.T20 (Very Low)  Bigquery.T21 (Very Low)  Bigquery.T24 (Very Low)  Bigquery.T28 (Very Low)  Bigquery.T29 (Very Low)  Bigquery.T30 (Very Low)  Bigquery.T32 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C23, depends on Bigquery.C22, assured by Bigquery.C24]  Ensure each dataset, table, model, connection, job, and listing uses authorized sources and destinations. | Request 1) the mechanism ensuring only authorized sources and destinations are configured, 2) its records of execution for all new sources and destinations, and 3) the plan to move any older sources and destinations. | Medium | Bigquery.FC1  Bigquery.FC3  Bigquery.FC6  Bigquery.FC9 | Bigquery.T2 (High)  Bigquery.T3 (High)  Bigquery.T6 (High)  Bigquery.T15 (High)  Bigquery.T18 (High)  Bigquery.T20 (High)  Bigquery.T24 (High)  Bigquery.T29 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C24]  Verify each dataset, table, model, connection, job, and listing uses authorized sources and destinations. | For a BigQuery dataset, table, model, connection, job, or listing, use an unauthorized 1) source or 2) destination; it should be detected. | Medium | Bigquery.FC1  Bigquery.FC3  Bigquery.FC6  Bigquery.FC9 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C25, depends on Bigquery.C22]  Protect the sources and destinations used by each table, model, connection, job, and listing, using their respective services' ThreatModels. | Request how the respective source and destination ThreatModels are applied to BigQuery. | High | Bigquery.FC1  Bigquery.FC3  Bigquery.FC9 | Bigquery.T2 (High)  Bigquery.T3 (High)  Bigquery.T6 (High)  Bigquery.T15 (High)  Bigquery.T29 (Medium) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Bigquery.C135, depends on Bigquery.C22]  Prevent the creation of a dataset without an authorized source (e.g., using a custom constraint resourceType:[bigquery.googleapis.com/Dataset](https://docs.cloud.google.com/bigquery/docs/custom-constraints#supported_resources), resource(s): resource.linkedDatasetSource.sourceDataset.datasetId != an authorized linked data source, resource.externalDatasetReference != an authorized external dataset reference, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | Create a dataset with an unauthorized source; it should be denied. | Medium | Bigquery.FC1 | Bigquery.T21 (High) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C32]  Define the requirements for the expiration time of each BigQuery table. | Request the requirements for the expiration time of each BigQuery table. | Low | Bigquery.FC1 | Bigquery.T11 (Very Low)  Bigquery.T21 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C33, depends on Bigquery.C32, assured by Bigquery.C34]  Ensure the expiration time of each BigQuery table is set according to the requirements. | Request the mechanism ensuring the expiration time of each BigQuery table is set according to its requirements. | Medium | Bigquery.FC1 | Bigquery.T11 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C34]  Verify the expiration time of each BigQuery table is set to its requirements. | Set the expiration time of a BigQuery table to be outside its requirements; it should be detected. | High | Bigquery.FC1 | - | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Bigquery.C136, depends on Bigquery.C32]  Prevent the creation or update of a dataset without an authorized expiration time (e.g., using a custom constraint resourceType:[bigquery.googleapis.com/Dataset](https://docs.cloud.google.com/bigquery/docs/custom-constraints#supported_resources), resource(s): resource.defaultTableExpirationMs != an authorized expiration time, resource.defaultPartitionExpirationMs != an authorized partition expiration time, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | Create or update a dataset with an unauthorized expiration time; it should be denied. | Medium | Bigquery.FC1 | Bigquery.T21 (High) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C35]  Monitor slot consumption (e.g., using slot recommender), job concurrency, job execution time, job errors, and bytes processed across the entire organization (e.g., using BigQuery Admin Resource Charts). | Create a job and use slots in an abnormal way; it should be detected. | Low | Bigquery.FC5 | Bigquery.T12 (Medium) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C88, depends on Bigquery.C66]  Monitor the creation/modification of unauthorized data transfers (e.g., by using Cloud Logging events "google.cloud.bigquery.datatransfer.v1.DataTransferService.CreateTransferConfig" and "google.cloud.bigquery.datatransfer.v1.DataTransferService.UpdateTransferConfig" and their fields request.serviceAccountName, request.transferConfig.dataSourceId, request.transferConfig.destinationDatasetId, request.transferConfig.emailPreferences, request.transferConfig.notificationPubsubTopic, and request.transferConfig.schedule). | Create/update an unauthorized data transfer; it should be detected. | Medium | Bigquery.FC4 | Bigquery.T13 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C47]  Define the requirements to register the BigQuery models with the Vertex AI Model Registry for each BigQuery model. | Request the registration requirements for each BigQuery model. | Low | Bigquery.FC6 | Bigquery.T18 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C48, depends on Bigquery.C47, assured by Bigquery.C49]  Ensure each BigQuery model is registered with the Vertex AI Model Registry according to its requirements. | Request the mechanism ensuring the BigQuery model is registered according to its requirements, and its records of execution. | High | Bigquery.FC6 | Bigquery.T18 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C49]  Verify all BigQuery models are registered with the Vertex AI Model Registry according to their requirements. | Register a model with a Vertex AI Model Registry outside the requirements; it should be detected. | High | Bigquery.FC6 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C53]  Define the authorized configuration for each job. | Request the authorized configuration for each job, its review process, and its review records. | Low | Bigquery.FC1 | Bigquery.T19 (Very Low)  Bigquery.T26 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C54, depends on Bigquery.C53, assured by Bigquery.C55]  Ensure each job uses an authorized configuration. | Request the mechanism ensuring the job uses an authorized configuration and its records of execution. | High | Bigquery.FC1 | Bigquery.T19 (High)  Bigquery.T26 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C55]  Verify all jobs use an authorized configuration. | Use an unauthorized configuration with a job; it should be detected. | High | Bigquery.FC1 | - | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C56]  Monitor the abnormal behavior, such as unexpected increases in execution time or unusual resource utilization, of a query (e.g., by using the query execution graph or administrative jobs explorer). | Run a query with abnormal behavior; it should be detected. | Low | Bigquery.FC1 | Bigquery.T9 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C57]  Define the requirements for metadata cache mode and staleness (30 minutes to 7 days) for each external table. | Request the requirements for enabling metadata cache and setting its staleness (30 minutes to 7 days) for each external table. | Low | Bigquery.FC1 | Bigquery.T9 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C58, depends on Bigquery.C57, assured by Bigquery.C59]  Ensure the metadata cache mode and staleness of each external table are set according to its requirements. | Request the mechanism ensuring the metadata cache mode and staleness of each external table are set according to its requirements. | Medium | Bigquery.FC1 | Bigquery.T9 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C59]  Verify the metadata cache mode and staleness of each external table are set to their requirements. | Set the metadata cache mode and staleness of an external table outside the requirements; it should be detected. | Medium | Bigquery.FC1 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C66]  Maintain a list of authorized sources (e.g., Cloud Storage, Amazon S3, Oracle, Salesforce) and their respective authorized configurations (i.e., destination dataset, schedule, config status, encryption key, parameters) to be used with each transfer. | Request the list of all authorized sources and their respective authorized configurations to be used with each transfer, its review process, and its review records. | Low | Bigquery.FC4 | Bigquery.T13 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C67, depends on Bigquery.C66, assured by Bigquery.C68]  Ensure each transfer uses an authorized source and its authorized configuration. | Request 1) the mechanism ensuring only an authorized source and its authorized configuration are configured, 2) its records of execution for all new sources, and 3) the plan to move any older sources. | Medium | Bigquery.FC4 | Bigquery.T13 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C68]  Verify each transfer uses an authorized source and its authorized configuration. | For a transfer, 1) use an unauthorized source, 2) remove an authorized source, or 3) use an unauthorized configuration for a source; it should be detected. | Medium | Bigquery.FC4 | - | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Bigquery.C119, depends on Bigquery.C66]  Prevent the creation/update of a transfer without an authorized source and/or destination (e.g., using a custom constraint resourceType:[bigquerydatatransfer.googleapis.com/TransferConfig](https://docs.cloud.google.com/bigquery/docs/transfer-custom-constraints#supported_resources), resource(s): resource.dataSourceId != an authorized data source, resource.destinationDatasetId != an authorized dataset, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | Create a transfer with an unauthorized 1) data source or create/update with an unauthorized 2) destination dataset; it should be denied. | Medium | Bigquery.FC4 | Bigquery.T13 (Medium) | Medium |
| Preventative (COSO)  Protect (NIST CSF) | [Bigquery.C120, depends on Bigquery.C66]  Prevent the create/update of a transfer without an authorized ingestion (i.e., schedule, refresh window, and status of transfer configuration) (e.g., using a custom constraint resourceType:[bigquerydatatransfer.googleapis.com/TransferConfig](https://docs.cloud.google.com/bigquery/docs/transfer-custom-constraints#supported_resources), resource(s): resource.dataRefreshWindowDays != authorized data refresh window, resource.disabled != authorized config status, resource.emailPreferences.enableFailureEmail != authorized failure email status, resource.encryptionConfiguration.kmsKeyName != authorized KMS key, resource.schedule != authorized schedule, resource.scheduleOptions.disableAutoScheduling != authorized autoscheduling status, resource.scheduleOptions.endTime != authorized end time, resource.scheduleOptions.startTime != authorized start time, resource.scheduleOptionsV2.timeBasedSchedule.endTime != authorized end time, resource.scheduleOptionsV2.timeBasedSchedule.schedule != authorized schedule, resource.scheduleOptionsV2.timeBasedSchedule.startTime != authorized start time, resource.scheduleOptionsV2.eventDrivenSchedule.pubsubSubscription != authorized Pub/Sub subscription, resource.notificationPubsubTopic != authorized Pub/Sub topic, methodTypes="UPDATE" and "CREATE", and actionType="DENY"). | Create a transfer with an unauthorized key or create/update a transfer with an unauthorized schedule; it should be denied. | Medium | Bigquery.FC4 | Bigquery.T13 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C70]  Maintain a list of authorized Cloud Storage buckets to be used with query jobs for User-Defined Functions (UDFs). | Request the list of Cloud Storage buckets used with query jobs for User-Defined Functions (UDFs). | High | Bigquery.FC2 | Bigquery.T8 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C71, depends on Bigquery.C70, assured by Bigquery.C72]  Ensure each query uses an authorized Cloud Storage bucket for a UDF. | Request 1) the mechanism ensuring queries use an authorized Cloud Storage bucket for UDFs, 2) its records of execution for all new UDFs, and 3) the plan to move any older UDFs. | Medium | Bigquery.FC2 | Bigquery.T8 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C72]  Verify each query uses an authorized Cloud Storage bucket for its UDF. | For a UDF, use an unauthorized bucket; it should be detected. | Medium | Bigquery.FC2 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C74]  Enforce secure SDLC processes on routines (e.g., using source control, static analysis, dynamic analysis, peer review). | Request the process and records of enforcing the SDLC process on routines to ensure the review of their code. | Medium | Bigquery.FC2 | Bigquery.T8 (High) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C78]  Define the authorized expiration time for each ML model. | Request the authorized expiration time for each ML model. | Low | Bigquery.FC6 | Bigquery.T22 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C79, depends on Bigquery.C78, assured by Bigquery.C80]  Ensure the expiration time for each ML model is authorized. | Request the mechanism ensuring the expiration time for each ML model is authorized, and the evidence of its execution. | High | Bigquery.FC6 | Bigquery.T22 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C80]  Verify all ML models have an authorized expiration time. | Create an ML model with an unauthorized expiration time; it should be detected. | High | Bigquery.FC6 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C89]  Define the requirements for generating, embedding, storing, accessing, updating, revoking, and destroying fingerprints for ML models as per the security requirements. | Request the requirements for generating, embedding, storing, accessing, updating, revoking, and destroying fingerprints for ML models, their review process, and its review records. | Medium | Bigquery.FC6 | Bigquery.T4 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C90, depends on Bigquery.C89, assured by Bigquery.C91]  Ensure the fingerprints for ML models are generated, embedded, stored, accessed, updated, revoked, and destroyed as per the security requirements. | Request 1) the mechanism ensuring the fingerprints for ML models are generated, embedded, stored, accessed, updated, revoked, and destroyed as per the security requirements, 2) their records of execution for all new keys, and 3) the plan to move any older keys. | Medium | Bigquery.FC6 | Bigquery.T4 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C91]  Verify the fingerprints for ML models are generated, embedded, stored, accessed, updated, revoked, and destroyed as per the security requirements. | 1) Generate, 2) embed, 3) store, 4) access, 5) update, 6) revoke, or 7) destroy a fingerprint outside the security requirements; it should be detected. | High | Bigquery.FC6 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C110, depends on Bigquery.C22]  Maintain a list of authorized emails or URLs (i.e., primaryContact, requestAccess, dataProvider, or publisher) to be used by listings and data exchanges. | Request the list of all authorized emails to be used by listings and data exchanges, its review process, and its review records. | High | Bigquery.FC9 | Bigquery.T30 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C111, depends on Bigquery.C110, assured by Bigquery.C112]  Ensure listings and data exchanges use authorized emails. | Request 1) the mechanism ensuring only authorized emails are configured, 2) its records of execution for all new emails, and 3) the plan to move any older emails. | Medium | Bigquery.FC9 | Bigquery.T30 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C112]  Verify listings and data exchanges use authorized emails. | For a listing or data exchange, use an unauthorized email; it should be detected. | Medium | Bigquery.FC9 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C92]  Define the requirements to configure a data exchange as a data clean room (e.g., sharing sensitive data with 3rd parties). | Request the requirements to configure a data exchange as a data clean room, its review process, and its review records. | Low | Bigquery.FC9 | Bigquery.T28 (Very Low)  Bigquery.T30 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C93, depends on Bigquery.C92, assured by Bigquery.C94]  Ensure required data exchanges are configured as data clean rooms (i.e., sharingEnvironmentConfig.dcrExchangeConfig). | Request 1) the mechanism ensuring required data exchanges are configured as data clean rooms, 2) its records of execution for all new data exchanges, and 3) the plan to move any older data exchanges. | Medium | Bigquery.FC9 | Bigquery.T28 (High)  Bigquery.T30 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C94]  Verify all required data exchanges are configured as data clean rooms. | Configure a data exchange required to be a data clean room as a non-data clean room; it should be detected. | Low | Bigquery.FC9 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C103, depends on Bigquery.C22]  Maintain the list of authorized subscriptions for each listing and data exchange. | Request the list of authorized subscriptions for each listing and/or data exchange, its review process, and its review records. | Low | Bigquery.FC9 | Bigquery.T28 (Very Low)  Bigquery.T29 (Very Low)  Bigquery.T32 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C104, depends on Bigquery.C103, assured by Bigquery.C105]  Ensure only authorized subscriptions for listings and data exchanges are configured. | Request 1) the mechanism ensuring only authorized subscriptions for listings and data exchanges are configured, 2) its records of execution for all new listings and/or data exchanges, and 3) the plan to move any older listings and/or data exchanges. | Medium | Bigquery.FC9 | Bigquery.T28 (High)  Bigquery.T29 (High)  Bigquery.T32 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C105]  Verify listings and data exchanges have only authorized subscriptions. | 1) Add an unauthorized subscription, or 2) remove the authorized subscription from a listing and/or data exchange; it should be detected. | Medium | Bigquery.FC9 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C114, depends on Bigquery.C92, assured by Bigquery.C115]  Ensure the restricted export for listings is enabled according to the requirements. | Request 1) the mechanism ensuring only restricted export is configured, 2) its records of execution for all new listings, and 3) the plan to move any older listings. | Medium | Bigquery.FC9 | Bigquery.T30 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C115]  Verify the restricted export for listings is enabled according to the requirements. | Enable the restricted export for listings outside the requirements; it should be detected. | High | Bigquery.FC9 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C116]  Maintain the list of authorized access entities (i.e., role, userByEmail, groupByEmail, domain, specialGroup, iamMember, view, routine, or dataset) for each dataset. | Request the list of authorized access entities of each dataset, its review process, and its review records. | Low | Bigquery.FC1 | Bigquery.T21 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C117, depends on Bigquery.C116, assured by Bigquery.C118]  Ensure only authorized access entities of each dataset are configured. | Request 1) the mechanism ensuring only authorized access entities of each dataset are configured, 2) its records of execution for all new datasets, and 3) the plan to move any older datasets. | Medium | Bigquery.FC1 | Bigquery.T21 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C118]  Verify all datasets use their authorized access entity. | 1) Allow an unauthorized access entity on a dataset, or 2) remove an authorized access entity on a dataset; it should be detected. | Medium | Bigquery.FC1 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C123]  Maintain the list of authorized configuration settings (e.g., default\_batch\_query\_queue\_timeout\_ms, default\_interactive\_query\_queue\_timeout\_ms, default\_query\_job\_timeout\_ms, enable\_fine\_grained\_dataset\_acls\_option) for each organization or project. | Request the list of authorized configuration settings for each organization or project, its review process, and its review records. | Low | Bigquery.FC1  Bigquery.FC4 | Bigquery.T9 (Very Low)  Bigquery.T13 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C124, depends on Bigquery.C123, assured by Bigquery.C125]  Ensure only authorized configuration settings for each organization or project are configured. | Request 1) the mechanism ensuring only authorized configuration settings for each organization or project are configured, 2) its records of execution for all new organizations or projects, and 3) the plan to move any older organizations or projects. | Medium | Bigquery.FC1  Bigquery.FC4 | Bigquery.T9 (Medium)  Bigquery.T13 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C125]  Verify all organizations or projects use their authorized configuration settings. | 1) Deploy unauthorized configuration settings on an organization or project, or 2) remove authorized configuration settings on an organization or project; it should be detected. | Medium | Bigquery.FC1  Bigquery.FC4 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C130]  Define the failover process (e.g., use soft failover mode by default, document the justification for any hard failover, require approval for exceptions, record the chosen failover mode in the change process, validate replication status) for reservations. | Request the failover process for reservations, its review process, and its review records. | Low | Bigquery.FC5 | Bigquery.T36 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C131, depends on Bigquery.C130]  Ensure a reservation is failed over according to the process. | Request the mechanism ensuring that the reservation is failed over according to the process. | Medium | Bigquery.FC5 | Bigquery.T36 (High) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C28, depends on Bigquery.C26]  Protect the CMEKs used by each BigQuery resource using the Cloud KMS ThreatModel (including enforcing CMEK protection using organization policy constraints/gcp.restrictCmekCryptoKeyProjects and constraints/gcp.restrictNonCmekServices as per Cloudkms.C32 and Cloudkms.C34). | Request how the Cloud KMS ThreatModel is applied to BigQuery resources. | High | Bigquery.FC1 | Bigquery.T11 (Medium)  Bigquery.T20 (Medium) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C76, depends on Bigquery.C75, assured by Bigquery.C77]  Ensure the configuration of each asynchronous query job is authorized. | Request the mechanism ensuring the configuration of each asynchronous query job is authorized, and the evidence of its execution. | High | Bigquery.FC1 | Bigquery.T20 (Medium) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C77]  Verify all asynchronous query jobs have authorized configurations. | Create an asynchronous query job with unauthorized configurations; it should be detected. | High | Bigquery.FC1 | - | Low |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C95]  Define the authorized configuration (i.e., displayName, description, documentation, icon, discoveryType, logLinkedDatasetQueryUserEmail = true) for each data exchange and identify the requirements for deploying the public data exchange. | Request the authorized configuration for each data exchange and the criteria for its discovery type, its review process, and its review records. | Low | Bigquery.FC9 | Bigquery.T28 (Very Low)  Bigquery.T31 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C96, depends on Bigquery.C95, assured by Bigquery.C97]  Ensure the configuration of each data exchange is authorized, and discoveryType is public only if required. | Request 1) the mechanism ensuring authorized configurations are used, 2) its records of execution for all new data exchanges, and 3) the plan to move any older data exchanges. | High | Bigquery.FC9 | Bigquery.T28 (Medium)  Bigquery.T31 (Medium) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C97]  Verify all data exchanges have authorized configurations. | Create a data exchange with an unauthorized configuration; it should be detected. | High | Bigquery.FC9 | - | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C99, depends on Bigquery.C98, assured by Bigquery.C100]  Ensure the configuration of each listing is authorized, and discoveryType is public only if required. | Request 1) the mechanism ensuring that authorized configurations are used, 2) its records of execution for all new listings, and 3) the plan to move any older listings. | High | Bigquery.FC9 | Bigquery.T28 (Medium)  Bigquery.T30 (Medium)  Bigquery.T31 (Medium) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C100]  Verify all listings have authorized configurations. | Create a listing with an unauthorized configuration; it should be detected. | High | Bigquery.FC9 | - | Low |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C43]  Monitor slot capacity (e.g., using the slot estimator) to estimate the correct number of slots for the BigQuery workload. | Increase or decrease slot capacity widely; it should be detected. | Low | Bigquery.FC5 | Bigquery.T12 (Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C41]  Ensure Cloud Audit Logs for BigQuery Data Transfer are enabled ([ref](https://docs.cloud.google.com/bigquery-transfer/docs/audit-logging)). | Request the implementation for enabling the Cloud Audit Logs for BigQuery Data Transfer and its records for execution. | Medium | Bigquery.FC4 | Bigquery.T13 (Low) | Low |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C42]  Monitor the abnormal number of concurrent connections and throughput for the BigQuery table (e.g., by using the Monitoring metric CONSUMER QUOTA - QUOTA LIMIT). | Create 1) an abnormal number of concurrent connections and 2) abnormal throughput for a BigQuery table; it should be detected. | Low | Bigquery.FC1  Bigquery.FC6 | Bigquery.T4 (Low)  Bigquery.T5 (Very Low) | Low |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C65]  Monitor the quality of data used with the ML models (e.g., by [data profiling](https://docs.cloud.google.com/bigquery/docs/data-profile-scan)). | Ingest bogus data in a table; it should be detected. | Low | Bigquery.FC6 | Bigquery.T4 (Low) | Low |
| Directive (COSO)  Respond (NIST CSF) | [Bigquery.C87]  Establish, document, and train on procedures for responding to key compromise events, including key leaks and unapproved access. Implement a key revocation process to invalidate compromised keys and replace them with new, secure keys. | Request the plan for key compromised events, and the records and results of the last Incident Response simulation. | High | Bigquery.FC1 | Bigquery.T20 (Medium) | Low |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C50]  Define the requirements for setting the time travel of each BigQuery dataset. | Request the requirements for setting time travel for each BigQuery dataset. | Low | Bigquery.FC1 | Bigquery.T19 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C51, depends on Bigquery.C50, assured by Bigquery.C52]  Ensure the time travel of each BigQuery dataset is set according to its requirements. | Request the mechanism ensuring the time travel of each BigQuery dataset is set according to its requirements. | Medium | Bigquery.FC1 | Bigquery.T19 (Low) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C52]  Verify the time travel of each BigQuery dataset is set to its requirements. | Set the time travel of a BigQuery dataset to an unauthorized value; it should be detected. | High | Bigquery.FC1 | - | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C69, depends on Bigquery.C66]  Protect the sources used with each transfer, using the respective service's ThreatModel. | Request how the respective service ThreatModel is applied to protect each BigQuery Data Transfer source. | High | Bigquery.FC4 | Bigquery.T13 (Medium) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C137, depends on Bigquery.C66]  Protect the network attachments used with private database sources, using the Compute Engine ThreatModel. | Request how the Compute Engine ThreatModel is applied to protect network attachments used with private database sources. | High | Bigquery.FC4 | Bigquery.T13 (Medium) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C73, depends on Bigquery.C70]  Protect the Cloud Storage buckets used for storing UDFs using Cloud Storage ThreatModel. | Request how the Cloud Storage ThreatModel is applied to buckets used for storing UDFs. | High | Bigquery.FC2 | Bigquery.T8 (Medium) | Low |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C107]  Maintain the list of listings and/or data exchanges authorized to be subscribed to, and by whom. | Request the list of listings and data exchanges authorized to be subscribed to and by whom, their review process, and their review records. | Low | Bigquery.FC10 | Bigquery.T33 (Very Low) | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C108, depends on Bigquery.C107, assured by Bigquery.C109]  Ensure only authorized entities you control are subscribed to the authorized listings and data exchanges. | Request 1) the mechanism ensuring only authorized entities you control are subscribed to authorized listings and data exchanges, 2) its records of execution for all new subscriptions on listings or data exchanges, and 3) the plan to move any older subscriptions on listings or data exchanges. | Medium | Bigquery.FC10 | Bigquery.T33 (High) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C109]  Verify only authorized entities you control are subscribed to authorized listings and data exchanges. | 1) Subscribe to an unauthorized listing and/or data exchange with an entity you control, or 2) subscribe with an unauthorized entity you control to a listing or exchange authorized for other entities you control; it should be detected. | Medium | Bigquery.FC10 | - | Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C126, depends on Bigquery.C127]  Ensure the Cloud AI Companion API is enabled/disabled for the BigQuery project following the Service Usage ThreatModel and is protected using Cloud AI Companion ThreatModel. | Request how the Service Usage ThreatModel and Cloud AI Companion ThreatModel are applied to the Cloud AI Companion API in the BigQuery project. | Medium | Bigquery.FC1 | Bigquery.T35 (High) | Low |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C127]  Maintain the list of authorized BigQuery projects allowed to use Gemini. | Request the list of authorized BigQuery projects allowed to use Gemini, its review process, and its review records. | Low | Bigquery.FC1 | Bigquery.T35 (Very Low) | Low |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C132, depends on Bigquery.C130]  Monitor the failover mode of a reservation (e.g., by using Cloud Logging event "google.cloud.bigquery.reservation.v1.ReservationService.FailoverReservation" and its field request.failoverMode). | Fail over a reservation in hard mode; it should be detected. | Medium | Bigquery.FC5 | Bigquery.T36 (Medium) | Very Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C101, assured by Bigquery.C102]  Ensure no sensitive data is included in the fields of the listings (i.e., displayName, description, documentation, icon). | Request the mechanism ensuring sensitive data is not included in the fields of listings, and the evidence of its execution. | Medium | Bigquery.FC9 | Bigquery.T31 (Medium) | Very Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C102]  Verify no sensitive data is included in the fields of listings. | Add sensitive data to a field of a listing; it should be detected. | High | Bigquery.FC9 | - | Very Low |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C113, depends on Bigquery.C22]  Define the requirements for enabling restricted export for listings. | Request the requirements for enabling restricted export for listings, their review process, and their review records. | Low | Bigquery.FC9 | Bigquery.T30 (Very Low) | Very Low |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C128, depends on Bigquery.C127, assured by Bigquery.C129]  Ensure only authorized BigQuery projects are allowed to use Gemini. | Request 1) the mechanism ensuring only authorized BigQuery projects are allowed to use Gemini, 2) its records of execution for all new BigQuery projects, and 3) the plan to move any older BigQuery projects. | Medium | Bigquery.FC1 | Bigquery.T35 (Medium) | Very Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C129]  Verify all authorized BigQuery projects are allowed to use Gemini. | 1) Enable Gemini in an unauthorized BigQuery project, or 2) disable Gemini from an authorized BigQuery project; it should be detected. | Medium | Bigquery.FC1 | - | Very Low |

## Appendix 2 - List of all Actions and their details

| **Id** | **Description** | **Feature Class ID** | **IAM Permission** | **Event** | **API** |
| --- | --- | --- | --- | --- | --- |
| Bigquery.A1 | Gets the access control policy for a resource. Returns an empty policy if the resource exists and does not have a policy set. | Bigquery.FC1 | bigquery.tables.getIamPolicy | - | bigquery.tables.getIamPolicy |
| Bigquery.A2 | Updates information in an existing table. The update method replaces the entire table resource, whereas the patch method only replaces fields that are provided in the submitted table resource. This method supports patch semantics. | Bigquery.FC1 | bigquery.tables.update | google.cloud.bigquery.v2.TableService.PatchTable | bigquery.tables.patch |
| Bigquery.A3 | Returns permissions that a caller has on the specified resource. If the resource does not exist, this will return an empty set of permissions, not a not\_found error. | Bigquery.FC1 | - | - | bigquery.tables.testIamPermissions |
| Bigquery.A4 | Updates information in an existing table. The update method replaces the entire table resource, whereas the patch method only replaces fields that are provided in the submitted table resource. | Bigquery.FC1 | bigquery.tables.update | jobservice.insert,tableservice.update | bigquery.tables.update |
| Bigquery.A5 | Creates a new, empty table in the dataset. | Bigquery.FC1 | bigquery.tables.create | jobservice.insert,tableservice.insert,google.cloud.bigquery.v2.TableService.InsertTable | bigquery.tables.insert |
| Bigquery.A6 | Gets the specified table resource by table ID. This method does not return the data in the table, it only returns the table resource, which describes the structure of this table. | Bigquery.FC1 | bigquery.tables.get | - | bigquery.tables.get |
| Bigquery.A7 | Sets the access control policy on the specified resource. Replaces any existing policy. | Bigquery.FC1 | bigquery.tables.setIamPolicy | jobservice.insert,google.iam.v1.IAMPolicy.SetIamPolicy | bigquery.tables.setIamPolicy |
| Bigquery.A8 | Lists all tables in the specified dataset. | Bigquery.FC1 | bigquery.tables.list | - | bigquery.tables.list |
| Bigquery.A9 | Deletes the table specified by tableid from the dataset. If the table contains data, all the data will be deleted. | Bigquery.FC1 | bigquery.tables.delete | datasetservice.delete,tableservice.delete,google.cloud.bigquery.v2.TableService.DeleteTable | bigquery.tables.delete |
| Bigquery.A10 | Create new table snapshots. | Bigquery.FC7 | bigquery.tables.createSnapshot | google.cloud.bigquery.v2.JobService.InsertJob | bigquery.jobs.insert |
| Bigquery.A11 | Delete table snapshots. | Bigquery.FC7 | bigquery.tables.deleteSnapshot | google.cloud.bigquery.v2.TableService.DeleteTable,tableservice.delete | - |
| Bigquery.A12 | Export table data out of BigQuery. | Bigquery.FC1 | bigquery.tables.export | google.cloud.bigquery.v2.JobService.InsertJob,jobservice.insert,jobservice.jobcompleted | - |
| Bigquery.A13 | Restore table snapshots. | Bigquery.FC7 | bigquery.tables.restoreSnapshot | google.cloud.bigquery.v2.JobService.InsertJob,jobservice.jobcompleted | bigquery.jobs.insert |
| Bigquery.A14 | Set policy tags in table schema. | Bigquery.FC1 | bigquery.tables.setCategory | - | - |
| Bigquery.A15 | Update tags for a table. | Bigquery.FC1 | bigquery.tables.updateTag | - | - |
| Bigquery.A16 | Streams data into BigQuery one record at a time without needing to run a load job. | Bigquery.FC1 | bigquery.tables.updateData | - | bigquery.tabledata.insertAll |
| Bigquery.A17 | Retrieves table data from a specified set of rows. | Bigquery.FC1 | bigquery.tables.getData | tabledataservice.list,google.cloud.bigquery.v2.TableDataService.List | bigquery.tabledata.list |
| Bigquery.A18 | Returns information about a specific job. Job information is available for a six-month period after creation. | Bigquery.FC1 | bigquery.jobs.get | - | bigquery.jobs.get |
| Bigquery.A19 | Starts a new asynchronous job. | Bigquery.FC1 | bigquery.jobs.create | jobservice.insert,google.cloud.bigquery.v2.JobService.InsertJob | bigquery.jobs.insert |
| Bigquery.A20 | Lists all jobs that you started in the specified project. Job information is available for a six-month period after creation. The job list is sorted in reverse chronological order, by job creation time. | Bigquery.FC1 | bigquery.jobs.list | - | bigquery.jobs.list |
| Bigquery.A21 | List all jobs and retrieve metadata on any job submitted by any user. | Bigquery.FC1 | bigquery.jobs.listAll | - | bigquery.jobs.listAll |
| Bigquery.A22 | Requests that a job be cancelled. This call will return immediately, and the client will need to poll for the job status to see if the cancel completed successfully. | Bigquery.FC1 | bigquery.jobs.update | jobservice.cancel | bigquery.jobs.cancel |
| Bigquery.A23 | Requests that a job is deleted. This call will return when the job is deleted. This method is available in limited preview. | Bigquery.FC1 | bigquery.jobs.delete | google.cloud.bigquery.v2.JobService.DeleteJob | bigquery.jobs.delete |
| Bigquery.A24 | Runs a BigQuery SQL query synchronously and returns query results if the query completes within a specified timeout. | Bigquery.FC1 | bigquery.jobs.create | google.cloud.bigquery.v2.JobService.Query,jobservice.query | bigquery.jobs.query |
| Bigquery.A25 | Retrieves the results of a query job. | Bigquery.FC1 | bigquery.tables.getData | jobservice.getqueryresults | bigquery.jobs.getQueryResults |
| Bigquery.A26 | Lists all routines in the specified dataset. | Bigquery.FC2 | bigquery.routines.list | - | bigquery.routines.list |
| Bigquery.A27 | Gets the specified routine resource by routine ID. | Bigquery.FC2 | bigquery.routines.get | - | bigquery.routines.get |
| Bigquery.A28 | Creates a new routine in the dataset. | Bigquery.FC2 | bigquery.routines.create | google.cloud.bigquery.v2.RoutineService.InsertRoutine | bigquery.routines.insert |
| Bigquery.A29 | Deletes the routine specified by routineid from the dataset. | Bigquery.FC2 | bigquery.routines.delete | google.cloud.bigquery.v2.RoutineService.DeleteRoutine | bigquery.routines.delete |
| Bigquery.A30 | Updates information in an existing routine. The update method replaces the entire routine resource. | Bigquery.FC2 | bigquery.routines.update | google.cloud.bigquery.v2.RoutineService.UpdateRoutine | bigquery.routines.update |
| Bigquery.A31 | Returns the dataset specified by datasetid. | Bigquery.FC1 | bigquery.datasets.get | - | bigquery.datasets.get |
| Bigquery.A32 | Updates information in an existing dataset. The update method replaces the entire dataset resource, whereas the patch method only replaces fields that are provided in the submitted dataset resource. This method supports patch semantics. | Bigquery.FC1 | bigquery.datasets.update | datasetservice.update,google.cloud.bigquery.v2.DatasetService.PatchDataset | bigquery.datasets.patch |
| Bigquery.A33 | Lists all datasets in the specified project. | Bigquery.FC1 | bigquery.datasets.get | - | bigquery.datasets.list |
| Bigquery.A34 | Deletes the dataset specified by the datasetid value. Before you can delete a dataset, you must delete all its tables, either manually or by specifying deleteContents. Immediately after deletion, you can create another dataset with the same name. | Bigquery.FC1 | bigquery.datasets.delete | datasetservice.delete,google.cloud.bigquery.v2.DatasetService.DeleteDataset | bigquery.datasets.delete |
| Bigquery.A35 | Creates a new empty dataset. | Bigquery.FC1 | bigquery.datasets.create | google.cloud.bigquery.v2.DatasetService.InsertDataset,datasetservice.insert | bigquery.datasets.insert |
| Bigquery.A36 | Updates information in an existing dataset. The update method replaces the entire dataset resource, whereas the patch method only replaces fields that are provided in the submitted dataset resource. | Bigquery.FC1 | bigquery.datasets.update | datasetservice.update,google.cloud.bigquery.v2.DatasetService.UpdateDataset | bigquery.datasets.update |
| Bigquery.A37 | Read a dataset's IAM permissions (via the console). | Bigquery.FC1 | bigquery.datasets.getIamPolicy | - | - |
| Bigquery.A38 | Change a dataset's IAM permissions (via the console). | Bigquery.FC1 | bigquery.datasets.setIamPolicy | - | - |
| Bigquery.A39 | Update tags for a dataset. | Bigquery.FC1 | bigquery.datasets.updateTag | - | - |
| Bigquery.A40 | Create a new row-level access policy on a table. | Bigquery.FC1 | bigquery.rowAccessPolicies.create | jobservice.insert,google.cloud.bigquery.v2.JobService.InsertJob | - |
| Bigquery.A41 | Delete a row-level access policy from a table. | Bigquery.FC1 | bigquery.rowAccessPolicies.delete | jobservice.insert,google.cloud.bigquery.v2.JobService.InsertJob | - |
| Bigquery.A42 | Gets data in a table that you want to be visible only to the members of a row-level access policy's grantee list. We recommend this permission only be granted on a row-level access policy resource. | Bigquery.FC1 | bigquery.rowAccessPolicies.getFilteredData | - | - |
| Bigquery.A43 | Re-create a row-level access policy. | Bigquery.FC1 | bigquery.rowAccessPolicies.update | jobservice.insert,google.cloud.bigquery.v2.JobService.InsertJob | - |
| Bigquery.A44 | Returns permissions that a caller has on the specified resource. If the resource does not exist, this will return an empty set of permissions, not a not\_found error. | Bigquery.FC1 | - | - | bigquery.rowAccessPolicies.testIamPermissions |
| Bigquery.A45 | Gets the access control policy for a resource. Returns an empty policy if the resource exists and does not have a policy set. | Bigquery.FC1 | bigquery.rowAccessPolicies.getIamPolicy | - | bigquery.rowAccessPolicies.getIamPolicy |
| Bigquery.A46 | Lists all row access policies on the specified table. | Bigquery.FC1 | bigquery.rowAccessPolicies.list | - | bigquery.rowAccessPolicies.list |
| Bigquery.A47 | Sets the access control policy on the specified resource. Replaces any existing policy. | Bigquery.FC1 | bigquery.rowAccessPolicies.setIamPolicy | - | - |
| Bigquery.A48 | Returns the email address of the service account for your project used for interactions with Google Cloud KMS. | Bigquery.FC1 | - | - | bigquery.projects.getServiceAccount |
| Bigquery.A49 | Lists all projects to which you have been granted any project role. | Bigquery.FC1 | - | - | bigquery.projects.list |
| Bigquery.A50 | Create new models. | Bigquery.FC6 | bigquery.models.create | jobservice.insert,jobservice.jobcompleted,google.cloud.bigquery.v2.JobService.InsertJob | - |
| Bigquery.A51 | Get model data. | Bigquery.FC6 | bigquery.models.getData | - | bigquery.models.get |
| Bigquery.A52 | Get model metadata. | Bigquery.FC6 | bigquery.models.getMetadata | - | bigquery.models.get |
| Bigquery.A53 | Update model data. | Bigquery.FC6 | bigquery.models.updateData | google.cloud.bigquery.v2.ModelService.PatchModel | bigquery.models.patch |
| Bigquery.A54 | Update model metadata. | Bigquery.FC6 | bigquery.models.updateMetadata | - | bigquery.models.patch |
| Bigquery.A55 | Deletes the model specified by modelid from the dataset. | Bigquery.FC6 | bigquery.models.delete | google.cloud.bigquery.v2.ModelService.DeleteModel | bigquery.models.delete |
| Bigquery.A56 | Lists all models in the specified dataset. | Bigquery.FC6 | bigquery.models.list | - | bigquery.models.list |
| Bigquery.A57 | Export a model. | Bigquery.FC6 | bigquery.models.export | jobservice.insert,jobservice.jobcompleted,google.cloud.bigquery.v2.JobService.InsertJob | - |
| Bigquery.A58 | Create saved queries (console only). | Bigquery.FC1 | bigquery.savedqueries.create | - | - |
| Bigquery.A59 | Delete saved queries (console only). | Bigquery.FC1 | bigquery.savedqueries.delete | - | - |
| Bigquery.A60 | Get metadata on saved queries (console only). | Bigquery.FC1 | bigquery.savedqueries.get | - | - |
| Bigquery.A61 | List saved queries (console only). | Bigquery.FC1 | bigquery.savedqueries.list | - | - |
| Bigquery.A62 | Update saved queries (console only). | Bigquery.FC1 | bigquery.savedqueries.update | - | - |
| Bigquery.A63 | Use a connection configuration to connect to a remote data source. | Bigquery.FC3 | bigquery.connections.use | - | - |
| Bigquery.A64 | Returns specified connection. | Bigquery.FC3 | bigquery.connections.get | google.cloud.bigquery.connection.v1.ConnectionService.GetConnection | bigqueryconnection.projects.locations.connections.get |
| Bigquery.A65 | Deletes connection and associated credential. | Bigquery.FC3 | bigquery.connections.delete | google.cloud.bigquery.connection.v1.ConnectionService.DeleteConnection | bigqueryconnection.projects.locations.connections.delete |
| Bigquery.A66 | Updates the specified connection. For security reasons, also resets credential if connection properties are in the update field mask. | Bigquery.FC3 | bigquery.connections.update | google.cloud.bigquery.connection.v1.ConnectionService.UpdateConnection | bigqueryconnection.projects.locations.connections.patch |
| Bigquery.A67 | Returns a list of connections in the given project. | Bigquery.FC3 | bigquery.connections.list | google.cloud.bigquery.connection.v1.ConnectionService.ListConnections | bigqueryconnection.projects.locations.connections.list |
| Bigquery.A68 | Gets the access control policy for a resource. Returns an empty policy if the resource exists and does not have a policy set. | Bigquery.FC3 | bigquery.connections.getIamPolicy | google.cloud.bigquery.connection.v1.ConnectionService.GetIamPolicy | bigqueryconnection.projects.locations.connections.getIamPolicy |
| Bigquery.A69 | Creates a new connection. | Bigquery.FC3 | bigquery.connections.create | google.cloud.bigquery.connection.v1.ConnectionService.CreateConnection | bigqueryconnection.projects.locations.connections.create |
| Bigquery.A70 | Returns permissions that a caller has on the specified resource. If the resource does not exist, this will return an empty set of permissions, not a not\_found error. | Bigquery.FC3 | - | - | bigqueryconnection.projects.locations.connections.testIamPermissions |
| Bigquery.A71 | Sets the access control policy on the specified resource. Replaces any existing policy. | Bigquery.FC3 | bigquery.connections.setIamPolicy | google.cloud.bigquery.connection.v1.ConnectionService.SetIamPolicy | bigqueryconnection.projects.locations.connections.setIamPolicy |
| Bigquery.A72 | Lists information about the supported locations for this service. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.location.Locations.ListLocations | bigquerydatatransfer.projects.locations.list |
| Bigquery.A73 | Gets information about a location. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.location.Locations.GetLocation | bigquerydatatransfer.projects.locations.get |
| Bigquery.A74 | Deletes the specified transfer run. | Bigquery.FC4 | bigquery.transfers.update | google.cloud.bigquery.datatransfer.v1.DataTransferService.DeleteTransferRun | bigquerydatatransfer.projects.locations.transferConfigs.runs.delete |
| Bigquery.A75 | Returns information about the particular transfer run. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.bigquery.datatransfer.v1.DataTransferService.GetTransferRun | bigquerydatatransfer.projects.locations.transferConfigs.runs.get |
| Bigquery.A76 | Returns information about running and completed jobs. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.bigquery.datatransfer.v1.DataTransferService.ListTransferRuns | bigquerydatatransfer.projects.locations.transferConfigs.runs.list |
| Bigquery.A77 | Returns user facing log messages for the data transfer run. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.bigquery.datatransfer.v1.DataTransferService.ListTransferLogs | bigquerydatatransfer.projects.locations.transferConfigs.runs.transferLogs.list |
| Bigquery.A78 | (Deprecated) Creates transfer runs for a time range [start\_time, end\_time]. For each date - or whatever granularity the data source supports - in the range, one transfer run is created. Note that runs are created per utc time in the time range. Deprecated: use startmanualtransferruns instead. | Bigquery.FC4 | bigquery.transfers.update | - | bigquerydatatransfer.projects.locations.transferConfigs.scheduleRuns |
| Bigquery.A79 | Returns information about a data transfer config. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.bigquery.datatransfer.v1.DataTransferService.GetTransferConfig | bigquerydatatransfer.projects.locations.transferConfigs.get |
| Bigquery.A80 | Start manual transfer runs to be executed now with schedule\_time equal to current time. The transfer runs can be created for a time range where the run\_time is between start\_time (inclusive) and end\_time (exclusive), or for a specific run\_time. | Bigquery.FC4 | bigquery.transfers.update | google.cloud.bigquery.datatransfer.v1.DataTransferService.StartManualTransferRuns | bigquerydatatransfer.projects.locations.transferConfigs.startManualRuns |
| Bigquery.A81 | Returns information about all data transfers in the project. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.bigquery.datatransfer.v1.DataTransferService.ListTransferConfigs | bigquerydatatransfer.projects.locations.transferConfigs.list |
| Bigquery.A82 | Creates a new data transfer configuration. | Bigquery.FC4 | bigquery.transfers.update | google.cloud.bigquery.datatransfer.v1.DataTransferService.CreateTransferConfig,google.cloud.bigquery.datatransfer.v1.DataTransferService.IsDataTransferServiceEnabled | bigquerydatatransfer.projects.locations.transferConfigs.create |
| Bigquery.A83 | Deletes a data transfer configuration, including any associated transfer runs and logs. | Bigquery.FC4 | bigquery.transfers.update | google.cloud.bigquery.datatransfer.v1.DataTransferService.DeleteTransferConfig | bigquerydatatransfer.projects.locations.transferConfigs.delete |
| Bigquery.A84 | Updates a data transfer configuration. All fields must be set, even if they are not updated. | Bigquery.FC4 | bigquery.transfers.update | google.cloud.bigquery.datatransfer.v1.DataTransferService.UpdateTransferConfig | bigquerydatatransfer.projects.locations.transferConfigs.patch |
| Bigquery.A85 | Retrieves a supported data source and returns its settings, which can be used for ui rendering. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.bigquery.datatransfer.v1.DataTransferService.GetDataSource | bigquerydatatransfer.projects.locations.dataSources.get |
| Bigquery.A86 | Returns true if valid credentials exist for the given data source and requesting user. Some data sources doesn't support service account, so we need to talk to them on behalf of the end user. This API just checks whether we have OAuth token for the particular user, which is a pre-requisite before user can create a transfer config. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.bigquery.datatransfer.v1.DataTransferService.CheckValidCreds | bigquerydatatransfer.projects.locations.dataSources.checkValidCreds |
| Bigquery.A87 | Lists supported data sources and returns their settings, which can be used for ui rendering. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.bigquery.datatransfer.v1.DataTransferService.ListDataSources | bigquerydatatransfer.projects.locations.dataSources.list |
| Bigquery.A88 | Retrieves a supported data source and returns its settings, which can be used for ui rendering. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.dataSources.get |
| Bigquery.A89 | Lists supported data sources and returns their settings, which can be used for ui rendering. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.bigquery.datatransfer.v1.DataTransferService.ListDataSources | bigquerydatatransfer.projects.dataSources.list |
| Bigquery.A90 | Returns true if valid credentials exist for the given data source and requesting user. Some data sources doesn't support service account, so we need to talk to them on behalf of the end user. This API just checks whether we have OAuth token for the particular user, which is a pre-requisite before user can create a transfer config. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.bigquery.datatransfer.v1.DataTransferService.CheckValidCreds | bigquerydatatransfer.projects.dataSources.checkValidCreds |
| Bigquery.A91 | Returns information about running and completed jobs. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.bigquery.datatransfer.v1.DataTransferService.ListTransferRuns | bigquerydatatransfer.projects.transferConfigs.runs.list |
| Bigquery.A92 | Deletes the specified transfer run. | Bigquery.FC4 | bigquery.transfers.update | google.cloud.bigquery.datatransfer.v1.DataTransferService.DeleteTransferRun | bigquerydatatransfer.projects.transferConfigs.runs.delete |
| Bigquery.A93 | Returns information about the particular transfer run. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.bigquery.datatransfer.v1.DataTransferService.GetTransferRun | bigquerydatatransfer.projects.transferConfigs.runs.get |
| Bigquery.A94 | Returns user facing log messages for the data transfer run. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.bigquery.datatransfer.v1.DataTransferService.ListTransferLogs | bigquerydatatransfer.projects.transferConfigs.runs.transferLogs.list |
| Bigquery.A95 | Returns information about a data transfer config. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.bigquery.datatransfer.v1.DataTransferService.GetTransferConfig | bigquerydatatransfer.projects.transferConfigs.get |
| Bigquery.A96 | Returns information about all data transfers in the project. | Bigquery.FC4 | bigquery.transfers.get | google.cloud.bigquery.datatransfer.v1.DataTransferService.ListTransferConfigs | bigquerydatatransfer.projects.transferConfigs.list |
| Bigquery.A97 | Updates a data transfer configuration. All fields must be set, even if they are not updated. | Bigquery.FC4 | bigquery.transfers.update | google.cloud.bigquery.datatransfer.v1.DataTransferService.UpdateTransferConfig | bigquerydatatransfer.projects.transferConfigs.patch |
| Bigquery.A98 | (Deprecated) Creates transfer runs for a time range [start\_time, end\_time]. For each date - or whatever granularity the data source supports - in the range, one transfer run is created. Note that runs are created per utc time in the time range. Deprecated: use startmanualtransferruns instead. | Bigquery.FC4 | bigquery.transfers.update | - | bigquerydatatransfer.projects.transferConfigs.scheduleRuns |
| Bigquery.A99 | Start manual transfer runs to be executed now with schedule\_time equal to current time. The transfer runs can be created for a time range where the run\_time is between start\_time (inclusive) and end\_time (exclusive), or for a specific run\_time. | Bigquery.FC4 | bigquery.transfers.update | google.cloud.bigquery.datatransfer.v1.DataTransferService.StartManualTransferRuns | bigquerydatatransfer.projects.transferConfigs.startManualRuns |
| Bigquery.A100 | Creates a new data transfer configuration. | Bigquery.FC4 | bigquery.transfers.update | google.cloud.bigquery.datatransfer.v1.DataTransferService.CreateTransferConfig,google.cloud.bigquery.datatransfer.v1.DataTransferService.IsDataTransferServiceEnabled | bigquerydatatransfer.projects.transferConfigs.create |
| Bigquery.A101 | Deletes a data transfer configuration, including any associated transfer runs and logs. | Bigquery.FC4 | bigquery.transfers.update | google.cloud.bigquery.datatransfer.v1.DataTransferService.DeleteTransferConfig | bigquerydatatransfer.projects.transferConfigs.delete |
| Bigquery.A102 | Returns information about the capacity commitment. | Bigquery.FC5 | bigquery.capacityCommitments.get | - | bigqueryreservation.projects.locations.capacityCommitments.get |
| Bigquery.A103 | Merges capacity commitments of the same plan into a single commitment. The resulting capacity commitment has the greater commitment\_end\_time out of the to-be-merged capacity commitments. Attempting to merge capacity commitments of different plan will fail with the error code google. Rpc. Code. Failed\_precondition. | Bigquery.FC5 | - | - | bigqueryreservation.projects.locations.capacityCommitments.merge |
| Bigquery.A104 | Lists all the capacity commitments for the admin project. | Bigquery.FC5 | bigquery.capacityCommitments.list | - | bigqueryreservation.projects.locations.capacityCommitments.list |
| Bigquery.A105 | Creates a new capacity commitment resource. | Bigquery.FC5 | bigquery.capacityCommitments.create | - | bigqueryreservation.projects.locations.capacityCommitments.create |
| Bigquery.A106 | Splits capacity commitment to two commitments of the same plan and commitment\_end\_time. A common use case is to enable downgrading commitments. For example, in order to downgrade from 10000 slots to 8000, you might split a 10000 capacity commitment into commitments of 2000 and 8000. Then, you would change the plan of the first one to flex and then delete it. | Bigquery.FC5 | - | - | bigqueryreservation.projects.locations.capacityCommitments.split |
| Bigquery.A107 | Deletes a capacity commitment. Attempting to delete capacity commitment before its commitment\_end\_time will fail with the error code google. Rpc. Code. Failed\_precondition. | Bigquery.FC5 | bigquery.capacityCommitments.delete | - | bigqueryreservation.projects.locations.capacityCommitments.delete |
| Bigquery.A108 | Updates an existing capacity commitment. Only plan and renewal\_plan fields can be updated. Plan can only be changed to a plan of a longer commitment period. Attempting to change to a plan with shorter commitment period will fail with the error code google. Rpc. Code. Failed\_precondition. | Bigquery.FC5 | bigquery.capacityCommitments.update | - | bigqueryreservation.projects.locations.capacityCommitments.patch |
| Bigquery.A109 | Creates an assignment object which allows the given project to submit jobs of a certain type using slots from the specified reservation. | Bigquery.FC5 | bigquery.reservationAssignments.create | google.cloud.bigquery.reservation.v1.ReservationService.CreateAssignment | bigqueryreservation.projects.locations.reservations.assignments.create |
| Bigquery.A110 | Deletes a assignment. | Bigquery.FC5 | bigquery.reservationAssignments.delete | google.cloud.bigquery.reservation.v1.ReservationService.DeleteAssignment | bigqueryreservation.projects.locations.reservations.assignments.delete |
| Bigquery.A111 | Lists assignments. Only explicitly created assignments will be returned. | Bigquery.FC5 | bigquery.reservationAssignments.list | - | bigqueryreservation.projects.locations.reservations.assignments.list |
| Bigquery.A112 | Moves an assignment under a new reservation. This differs from removing an existing assignment and recreating a new one by providing a transactional change that ensures an assignee always has an associated reservation. | Bigquery.FC5 | - | - | bigqueryreservation.projects.locations.reservations.assignments.move |
| Bigquery.A113 | Lists all the reservations for the project in the specified location. | Bigquery.FC5 | bigquery.reservations.list | - | bigqueryreservation.projects.locations.reservations.list |
| Bigquery.A114 | Returns information about the reservation. | Bigquery.FC5 | bigquery.reservations.get | - | bigqueryreservation.projects.locations.reservations.get |
| Bigquery.A115 | Deletes a reservation. Returns google. Rpc. Code. Failed\_precondition when reservation has assignments. | Bigquery.FC5 | bigquery.reservations.delete | google.cloud.bigquery.reservation.v1.ReservationService.DeleteReservation | bigqueryreservation.projects.locations.reservations.delete |
| Bigquery.A116 | Creates a new reservation resource. | Bigquery.FC5 | bigquery.reservations.create | google.cloud.bigquery.reservation.v1.ReservationService.CreateAssignment | bigqueryreservation.projects.locations.reservations.create |
| Bigquery.A117 | Updates an existing reservation resource. | Bigquery.FC5 | bigquery.reservations.update | google.cloud.bigquery.reservation.v1.ReservationService.UpdateReservation | bigqueryreservation.projects.locations.reservations.patch |
| Bigquery.A118 | Retrieves a BI reservation. | Bigquery.FC5 | bigquery.bireservations.get | - | bigqueryreservation.projects.locations.getBiReservation |
| Bigquery.A119 | Looks up assignments for a specified resource for a particular region. If the request is about a project: 1. Assignments created on the project will be returned if they exist. 2. Otherwise assignments created on the closest ancestor will be returned. 3. Assignments for different jobtypes will all be returned. The same logic applies if the request is about a folder. If the request is about an organization, then assignments created on the organization will be returned (organization doesn't have ancestors). | Bigquery.FC5 | - | - | bigqueryreservation.projects.locations.searchAllAssignments |
| Bigquery.A120 | Updates a BI reservation. Only fields specified in the field\_mask are updated. A singleton BI reservation always exists with default size 0. In order to reserve BI capacity it needs to be updated to an amount greater than 0. In order to release BI Capacity Reservation size must be set to 0. | Bigquery.FC5 | bigquery.bireservations.update | - | bigqueryreservation.projects.locations.updateBiReservation |
| Bigquery.A121 | Looks up assignments for a specified resource for a particular region. If the request is about a project: 1. Assignments created on the project will be returned if they exist. 2. Otherwise assignments created on the closest ancestor will be returned. 3. Assignments for different jobtypes will all be returned. The same logic applies if the request is about a folder. If the request is about an organization, then assignments created on the organization will be returned (organization doesn't have ancestors). | Bigquery.FC5 | bigquery.reservationAssignments.search | - | bigqueryreservation.projects.locations.searchAssignments |
| Bigquery.A122 | Updates the tags for an existing connection. | Bigquery.FC3 | bigquery.connections.updateTag | - | - |
| Bigquery.A123 | Updates the tags for an existing model. | Bigquery.FC6 | bigquery.models.updateTag | - | - |
| Bigquery.A124 | Updates the tags for an existing routine. | Bigquery.FC2 | bigquery.routines.updateTag | - | - |
| Bigquery.A125 | Enroll data sources in a user project. This allows users to create transfer configurations for these data sources. | Bigquery.FC4 | - | - | bigquerydatatransfer.projects.enrollDataSources |
| Bigquery.A126 | Enroll data sources in a user project. This allows users to create transfer configurations for these data sources. | Bigquery.FC4 | - | - | bigquerydatatransfer.projects.locations.enrollDataSources |
| Bigquery.A127 | Access historical data for a table that has, or has previously had, row-level access policies. | Bigquery.FC1 | bigquery.rowAccessPolicies.overrideTimeTravelRestrictions | - | - |
| Bigquery.A128 | Delegate connection to create authorized external tables and remote functions. | Bigquery.FC3 | bigquery.connections.delegate | - | - |
| Bigquery.A129 | Retrieve execution metadata on any job. | Bigquery.FC1 | bigquery.jobs.listExecutionMetadata | - | - |
| Bigquery.A130 | Create index of a table. | Bigquery.FC1 | bigquery.tables.createIndex | - | - |
| Bigquery.A131 | Delete index of a table. | Bigquery.FC1 | bigquery.tables.deleteIndex | - | - |
| Bigquery.A132 | Creates a new data policy under a project with the given dataPolicyId (used as the display name), policy tag, and data policy type. | Bigquery.FC8 | bigquery.dataPolicies.create | google.cloud.bigquery.datapolicies.v1.DataPolicyService.CreateDataPolicy | bigquerydatapolicy.projects.locations.dataPolicies.create |
| Bigquery.A133 | Deletes the data policy specified by its resource name. | Bigquery.FC8 | bigquery.dataPolicies.delete | google.cloud.bigquery.datapolicies.v1.DataPolicyService.DeleteDataPolicy | bigquerydatapolicy.projects.locations.dataPolicies.delete |
| Bigquery.A134 | Gets the data policy specified by its resource name. | Bigquery.FC8 | bigquery.dataPolicies.get | google.cloud.bigquery.datapolicies.v1.DataPolicyService.GetDataPolicy | bigquerydatapolicy.projects.locations.dataPolicies.get |
| Bigquery.A135 | Gets the IAM policy for the specified data policy. | Bigquery.FC8 | bigquery.dataPolicies.getIamPolicy | google.cloud.bigquery.datapolicies.v1.DataPolicyService.GetIamPolicy | bigquerydatapolicy.projects.locations.dataPolicies.getIamPolicy |
| Bigquery.A136 | List all of the data policies in the specified parent project. | Bigquery.FC8 | bigquery.dataPolicies.list | google.cloud.bigquery.datapolicies.v1.DataPolicyService.ListDataPolicies | bigquerydatapolicy.projects.locations.dataPolicies.list |
| Bigquery.A137 | Masked read access to sub-resources tagged by the policy tag associated with a data policy, for example, BigQuery columns. | Bigquery.FC8 | bigquery.dataPolicies.maskedGet | - | - |
| Bigquery.A138 | Sets the IAM policy for the specified data policy. | Bigquery.FC8 | bigquery.dataPolicies.setIamPolicy | google.cloud.bigquery.datapolicies.v1.DataPolicyService.SetIamPolicy | bigquerydatapolicy.projects.locations.dataPolicies.setIamPolicy |
| Bigquery.A139 | Updates the metadata for an existing data policy. The target data policy can be specified by the resource name. | Bigquery.FC8 | bigquery.dataPolicies.update | google.cloud.bigquery.datapolicies.v1.DataPolicyService.UpdateDataPolicy | bigquerydatapolicy.projects.locations.dataPolicies.patch |
| Bigquery.A140 | Renames the ID (display name) of the specified data policy. | Bigquery.FC8 | bigquery.dataPolicies.update | google.cloud.bigquery.datapolicies.v1.DataPolicyService.RenameDataPolicy | bigquerydatapolicy.projects.locations.dataPolicies.rename |
| Bigquery.A141 | Returns the caller's permission on the specified data policy resource. | Bigquery.FC8 | - | - | bigquerydatapolicy.projects.locations.dataPolicies.testIamPermissions |
| Bigquery.A142 | Lists all data exchanges from projects in a given organization and location. | Bigquery.FC9 | analyticshub.dataExchanges.list | - | analyticshub.organizations.locations.dataExchanges.list |
| Bigquery.A143 | Creates a new data exchange. | Bigquery.FC9 | analyticshub.dataExchanges.create | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.CreateDataExchange | analyticshub.projects.locations.dataExchanges.create |
| Bigquery.A144 | Deletes an existing data exchange. | Bigquery.FC9 | analyticshub.dataExchanges.delete | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.DeleteDataExchange | analyticshub.projects.locations.dataExchanges.delete |
| Bigquery.A145 | Gets the details of a data exchange. | Bigquery.FC9 | analyticshub.dataExchanges.get | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.GetDataExchange | analyticshub.projects.locations.dataExchanges.get |
| Bigquery.A146 | Gets the IAM policy. | Bigquery.FC9 | analyticshub.dataExchanges.getIamPolicy | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.GetIamPolicy | analyticshub.projects.locations.dataExchanges.getIamPolicy |
| Bigquery.A147 | Lists all data exchanges in a given project and location. | Bigquery.FC9 | analyticshub.dataExchanges.list | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.ListDataExchanges | analyticshub.projects.locations.dataExchanges.list |
| Bigquery.A148 | Lists all subscriptions on a given data exchange or listing. | Bigquery.FC9 | analyticshub.dataExchanges.viewSubscriptions | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.ListSharedResourceSubscriptions | analyticshub.projects.locations.dataExchanges.listSubscriptions |
| Bigquery.A149 | Creates a new listing. | Bigquery.FC9 | analyticshub.listings.create | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.CreateListing | analyticshub.projects.locations.dataExchanges.listings.create |
| Bigquery.A150 | Deletes a listing. | Bigquery.FC9 | analyticshub.listings.delete | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.DeleteListing | analyticshub.projects.locations.dataExchanges.listings.delete |
| Bigquery.A151 | Gets the details of a listing. | Bigquery.FC9 | analyticshub.listings.get | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.GetListing | analyticshub.projects.locations.dataExchanges.listings.get |
| Bigquery.A152 | Gets the IAM policy. | Bigquery.FC9 | analyticshub.listings.getIamPolicy | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.GetIamPolicy | analyticshub.projects.locations.dataExchanges.listings.getIamPolicy |
| Bigquery.A153 | Lists all listings in a given project and location. | Bigquery.FC9 | analyticshub.listings.list | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.ListListings | analyticshub.projects.locations.dataExchanges.listings.list |
| Bigquery.A154 | Lists all subscriptions on a given data exchange or listing. | Bigquery.FC9 | analyticshub.listings.viewSubscriptions | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.ListSharedResourceSubscriptions | analyticshub.projects.locations.dataExchanges.listings.listSubscriptions |
| Bigquery.A155 | Updates an existing listing. | Bigquery.FC9 | analyticshub.listings.update | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.UpdateListing | analyticshub.projects.locations.dataExchanges.listings.patch |
| Bigquery.A156 | Sets the IAM policy. | Bigquery.FC9 | analyticshub.listings.setIamPolicy | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.SetIamPolicy | analyticshub.projects.locations.dataExchanges.listings.setIamPolicy |
| Bigquery.A157 | Subscribes to a listing. Currently, with BigQuery sharing, you can create listings that reference only BigQuery datasets. Upon subscription to a listing for a BigQuery dataset, BigQuery sharing creates a linked dataset in the subscriber's project. | Bigquery.FC10 | analyticshub.listings.subscribe | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.SubscribeListing | analyticshub.projects.locations.dataExchanges.listings.subscribe |
| Bigquery.A158 | Returns the permissions that a caller has. | Bigquery.FC9 | - | - | analyticshub.projects.locations.dataExchanges.listings.testIamPermissions |
| Bigquery.A159 | Updates an existing data exchange. | Bigquery.FC9 | analyticshub.dataExchanges.update | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.UpdateDataExchange | analyticshub.projects.locations.dataExchanges.patch |
| Bigquery.A160 | Sets the IAM policy. | Bigquery.FC9 | analyticshub.dataExchanges.setIamPolicy | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.SetIamPolicy | analyticshub.projects.locations.dataExchanges.setIamPolicy |
| Bigquery.A161 | Creates a subscription to a data clean room. | Bigquery.FC10 | analyticshub.dataExchanges.subscribe | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.SubscribeDataExchange | analyticshub.projects.locations.dataExchanges.subscribe |
| Bigquery.A162 | Returns the permissions that a caller has. | Bigquery.FC9 | - | - | analyticshub.projects.locations.dataExchanges.testIamPermissions |
| Bigquery.A163 | Deletes a subscription. | Bigquery.FC9 | analyticshub.subscriptions.delete | - | analyticshub.projects.locations.subscriptions.delete |
| Bigquery.A164 | Gets the details of a subscription. | Bigquery.FC9 | analyticshub.subscriptions.get | - | analyticshub.projects.locations.subscriptions.get |
| Bigquery.A165 | Gets the IAM policy. | Bigquery.FC9 | analyticshub.dataExchanges.getIamPolicy  analyticshub.listings.getIamPolicy  analyticshub.subscriptions.getIamPolicy | - | analyticshub.projects.locations.subscriptions.getIamPolicy |
| Bigquery.A166 | Lists all subscriptions in a given project and location. | Bigquery.FC9 | analyticshub.subscriptions.list | - | analyticshub.projects.locations.subscriptions.list |
| Bigquery.A167 | Refreshes a subscription to a data exchange. A data exchange can become stale when a publisher adds or removes data. | Bigquery.FC9 | analyticshub.subscriptions.update | - | analyticshub.projects.locations.subscriptions.refresh |
| Bigquery.A168 | Revokes a given subscription. | Bigquery.FC9 | analyticshub.listings.update | google.cloud.bigquery.analyticshub.v1.AnalyticsHubService.RevokeSubscription | analyticshub.projects.locations.subscriptions.revoke |
| Bigquery.A171 | Updates an existing assignment. | Bigquery.FC5 | bigquery.reservationAssignments.update | google.cloud.bigquery.reservation.v1.ReservationService.UpdateAssignment | bigqueryreservation.projects.locations.reservations.assignments.patch |
| Bigquery.A172 | Specify BigQuery configuration settings at an organization or project level. | Bigquery.FC1 | bigquery.config.update | - | - |
| Bigquery.A173 | Retrieve BigQuery configuration settings at an organization or project level. | Bigquery.FC1 | bigquery.config.get | - | - |
| Bigquery.A174 | Fail over a reservation to the secondary location. | Bigquery.FC5 | bigquery.reservations.update | - | bigqueryreservation.projects.locations.reservations.failoverReservation |
| Bigquery.A175 | Gets the access control policy for a resource. | Bigquery.FC5 | bigqueryreservation.reservations.getIamPolicy | google.cloud.bigquery.reservation.v1.ReservationService.GetIamPolicy | bigqueryreservation.projects.locations.reservations.getIamPolicy |
| Bigquery.A176 | Sets an access control policy for a resource. | Bigquery.FC5 | bigqueryreservation.reservations.setIamPolicy | google.cloud.bigquery.reservation.v1.ReservationService.SetIamPolicy | bigqueryreservation.projects.locations.reservations.setIamPolicy |
| Bigquery.A177 | Gets your permissions on a resource. | Bigquery.FC5 | - | - | bigqueryreservation.projects.locations.reservations.testIamPermissions |
| Bigquery.A178 | Gets the access control policy for a resource. | Bigquery.FC5 | bigqueryreservation.reservations.getIamPolicy | google.cloud.bigquery.reservation.v1.ReservationService.GetIamPolicy | bigqueryreservation.projects.locations.reservations.assignments.getIamPolicy |
| Bigquery.A179 | Sets an access control policy for a resource. | Bigquery.FC5 | bigqueryreservation.reservations.setIamPolicy | google.cloud.bigquery.reservation.v1.ReservationService.SetIamPolicy | bigqueryreservation.projects.locations.reservations.assignments.setIamPolicy |
| Bigquery.A180 | Gets your permissions on a resource. | Bigquery.FC5 | - | - | bigqueryreservation.projects.locations.reservations.assignments.testIamPermissions |