# ThreatModel for Google 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).

| **Google BigQuery** Data Flow Diagram | Security Scorecard  | ***Security in the Cloud*** | | | --- | --- | | Number of Actions\* | 140 | | Identity management | Cloud IAM | | Number of IAM permissions\* | 95 | | Resource-based access | tables  rows  columns  connections | | VPC Service Controls | Yes | | Network Filtering | No | | Encryption-at-rest | Yes | | Encryption-in-transit | Yes |   \* See details in Appendixes |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

## Mitre ATT&CK matrix for Google 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] | Malicious code execution by importing data from cross Cloud Storage [Bigquery.T16] |  | Restricting access to datasets, tables, and connections by modification of privileges [Bigquery.T10] |  |  |  |  |  |  | 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 a table [Bigquery.T9] | Loss of integrity and availability by copying datasets and overwriting the destination table(s) [Bigquery.T3] |
|  |  |  |  |  |  |  |  |  |  |  |  | Data exfiltration by updating the destination dataset in transfer and transfer credentials [Bigquery.T13] | Loss of integrity of training model [Bigquery.T4] |
|  |  |  |  |  |  |  |  |  |  |  |  | Data exfiltration by exporting query results [Bigquery.T15] | Loss of integrity and availability by appending, overwriting data, or creating a table [Bigquery.T5] |
|  |  |  |  |  |  |  |  |  |  |  |  | Model exfiltration by registering BigQuery ML models with the Vertex AI Model Registry [Bigquery.T18] | DoS by throttling limit [Bigquery.T7] |
|  |  |  |  |  |  |  |  |  |  |  |  | Table exfiltration by cloning [Bigquery.T19] | Loss of integrity and availability by manipulating data using UDFs [Bigquery.T8] |
|  |  |  |  |  |  |  |  |  |  |  |  |  | Disruption of application functionality by modification of table and views configurations [Bigquery.T11] |
|  |  |  |  |  |  |  |  |  |  |  |  |  | Denial of Service by removing reservations [Bigquery.T12] |
|  |  |  |  |  |  |  |  |  |  |  |  |  | Loss of data during recovery by deleting a snapshot [Bigquery.T14] |

## Feature Classes

Google 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 | class | You can create a table inside a dataset. You can run SQL queries and jobs on datasets in a very fast way. Jobs are actions that BigQuery runs on your behalf to load data, export data, query data, or copy data. |
| User-Defined Functions | subclass of Dataset and tables | A User-Defined Function (UDF) lets you create a function by using a SQL expression or JavaScript code. |
| BigQuery connections and BigQuery Omni | 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 reservation | subclass of Dataset and tables | You can purchase dedicated query processing capacity. |
| BigQuery Data Transfer | subclass of Dataset and tables | You can transfer external data from SaaS applications to Google BigQuery on a regular basis. |
| BigQuery ML | subclass of Dataset and tables | You can create and execute machine learning models in BigQuery using standard SQL queries. |
| Table snapshot | 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 | subclass of Dataset and tables | You can provide different levels of visibility to different groups of users by using policy tags. |

| Dataset and tables *(class, FC1)* *You can create a table inside a dataset. You can run SQL queries and jobs on datasets in a very fast way. 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 a table | [High (8.8)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/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) | | Disruption of application functionality by modification of table and views 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) | | Loss of integrity and availability by appending, overwriting data, or creating a table | [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:N/I:H/A:N) | | Restricting access to datasets, tables, and connections by modification of 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) | | 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) | | 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) | | DoS by throttling limit | [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:N/I:N/A:L) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Escalate privileges, loss of availability or integrity of data, or exfiltrate data via an unauthorized query on a dataset or a 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 a 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. An attacker can also update or drop columns of a table, change the case sensitivity of datasets and its tables to escalate privileges while avoiding detection by a poorly designed access management system, or set unauthorized default values of a column to corrupt or steal data. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **CVSS** | [High (8.8)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H) | | **IAM Access** | {  "AND": ["bigquery.jobs.create", "bigquery.tables.getData"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Ensure authorized configuration(s) is used with the BigQuery dataset**    Ensure no dataset is accessible to "AllUsers" or "AllAuthenticatedUsers", except if allowed. | Very High | 1 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Control access at the table and view level**    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).    Ensure only authorized IAM entities are allowed to access the tables, views, and table data in a specific dataset. | High | 2 | - | - |
| **Restrict access to columns with BigQuery column-level security**    Define the criteria for the sensitivity of columns in a table.    Ensure only authorized IAM entities are allowed to access sensitive columns of a table (e.g., using BigQuery column-level security or column-level data masking). | High | 2 | - | - |
| **Restrict access to rows with BigQuery row-level security**    Define the criteria for the sensitivity of rows in a table.    Ensure only authorized IAM entities are allowed to access sensitive rows of a table (e.g., using BigQuery row-level security). | 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 of 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** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Secure the authorized destinations**    Maintain a list of authorized destinations (e.g., Cloud Storage, BigQuery, etc.) to be used with each table.    Ensure each table uses authorized sources and destinations (e.g., Cloud Storage, BigQuery, etc.).    Protect the sources and destinations used for infiltration/exfiltration with each table, using their respective service's ThreatModel. | High | 3 | - | - |
| **Control access at the table and view level**    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).    Ensure only authorized IAM entities are allowed to access the tables, views, and table data in a specific dataset. | High | 2 | - | - |
| **Encrypt datasets and models at rest and protect the keys**    Maintain a list of authorized CMEKs to be used with each BigQuery dataset and model, ideally dedicated.    Protect the CMEKs used by BigQuery datasets and models, using the Cloud KMS ThreatModel. | Medium | 2 | - | - |

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

| | **Threat Id** | Bigquery.T11 | | --- | --- | | **Name** | Disruption of application functionality by modification of table and views configurations | | **Description** | Specific properties are associated with tables and views during the creation. An attacker can modify these properties (e.g., schema, expiration time) 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** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Control access at the table and view level**    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).    Ensure only authorized IAM entities are allowed to access the tables, views, and table data in a specific dataset. | High | 2 | - | - |
| **Set the expiration time of BigQuery tables as per the requirements**    Define the requirement for the expiration time of each BigQuery table.    Ensure the expiration time of each BigQuery table is set according to its requirement. | Medium | 2 | - | - |
| **Encrypt datasets and models at rest and protect the keys**    Maintain a list of authorized CMEKs to be used with each BigQuery dataset and model, ideally dedicated.    Ensure only authorized CMEKs are used with each BigQuery dataset and model (e.g., using [default configuration](https://cloud.google.com/bigquery/docs/default-configuration)), and any unauthorized CMEKs are restricted following the Cloud KMS ThreatModel.    Protect the CMEKs used by BigQuery datasets and models, using the Cloud KMS ThreatModel.    Ensure [AEAD encryption functions](https://cloud.google.com/bigquery/docs/column-key-encrypt) are used to encrypt data at the column level. | Medium | 4 | - | - |
| **Ensure authorized configuration(s) is used with the BigQuery dataset**    Define the authorized configuration (i.e., encryption key, table expiry, labels) for each BigQuery dataset.    Ensure the configuration of each BigQuery dataset is authorized. | Medium | 2 | - | - |

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

| | **Threat Id** | Bigquery.T5 | | --- | --- | | **Name** | Loss of integrity and availability by appending, overwriting data, or 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 (4.5)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N) | | **IAM Access** | {  "OR": ["bigquery.tables.create", "bigquery.tables.updateData", "bigquery.jobs.create"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Control access at the table and view level**    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).    Ensure only authorized IAM entities are allowed to access the tables, views, and table data in a specific dataset. | High | 2 | - | - |
| **Monitor data ingestion**    Monitor the abnormal number of concurrent connections and throughput for BigQuery table (e.g., by using Monitoring metric CONSUMER QUOTA - QUOTA LIMIT). | Very Low | - | - | 1 |

#### Restricting access to datasets, tables, and connections by modification of privileges

| | **Threat Id** | Bigquery.T10 | | --- | --- | | **Name** | Restricting access to datasets, tables, and connections by modification of privileges | | **Description** | IAM permissions can be used to allow access to perform actions on BigQuery datasets, tables, and connections. An attacker can limit access to tables, rows, or columns for legitimate users or allow unauthorized users to access 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"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |

#### 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 it. | | **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.insert"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Clone BigQuery tables as per the requirement**    Define the requirement for the cloning of each BigQuery table.    Ensure the cloning of each BigQuery table is according to its requirement. | High | 2 | - | - |
| **Set the time travel of a BigQuery dataset as per the requirements**    Define the requirement for the time travel of each BigQuery dataset.    Ensure the time travel of each BigQuery dataset is set according to its requirement. | Medium | 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 it. 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** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Control access at the table and view level**    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).    Ensure only authorized IAM entities are allowed to access the tables, views, and table data in a specific dataset. | High | 2 | - | - |
| **De-identify sensitive data using Cloud DLP**    Ensure sensitive data is identified and redacted (e.g., using Cloud DLP). | Medium | 1 | - | - |

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

| | **Threat Id** | Bigquery.T1 | | --- | --- | | **Name** | Destruction of data by deleting dataset or table | | **Description** | A project has a dataset. Inside a dataset, a table is created, and data is stored inside this table. An attacker can delete the table or a dataset causing a 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** | {  "OR": ["bigquery.tables.delete", "bigquery.datasets.delete"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Clone BigQuery tables as per the requirement**    Define the requirement for the cloning of each BigQuery table.    Ensure the cloning of each BigQuery table is according to its requirement. | High | 2 | - | - |
| **Create and secure backups (e.g., by snapshots or exports) of BigQuery dataset(s) and table(s)**    Define the requirement for the backup of each BigQuery dataset and table.    Ensure each BigQuery dataset and table is backed up (e.g., by creating snapshots or exports) according to its requirement and is restorable. | Medium | 2 | - | - |

#### DoS by throttling limit

| | **Threat Id** | Bigquery.T7 | | --- | --- | | **Name** | DoS by throttling limit | | **Description** | DoS by exhausting quota limit for BigQuery GCP enforces [quotas](https://cloud.google.com/bigquery/quotas) on BigQuery resources (e.g., concurrent rate limit for interactive queries is limited to 100 queries). An attacker can exhaust the current quota limit for interactive and federated queries, load or export jobs, table and metadata, streaming inserts, and UDF limits to perform Denial of Service by sending many requests. | | **Goal** | Disruption of Service | | **MITRE ATT&CK®** | [TA0040](https://attack.mitre.org/tactics/TA0040) | | **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:N/I:N/A:L) | | **IAM Access** | {  "UNIQUE": "bigquery.depends"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Set the quotas on BigQuery as per the API usage statistics**    Ensure the [quotas](https://cloud.google.com/bigquery/quotas) on BigQuery (e.g., query limits, streaming insert limits, etc.) are set as per the API usage statistics. | Medium | 1 | - | - |

| User-Defined Functions *(subclass of Dataset and tables, FC2)* *A UDF accepts columns of input, performs actions on the input, and returns the result of those actions as a value.* 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 UDFs | [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 UDFs

| | **Threat Id** | Bigquery.T8 | | --- | --- | | **Name** | Loss of integrity and availability by manipulating data using UDFs | | **Description** | A User-Defined Function (UDF) or routine allows the creation of a function using a SQL expression or JavaScript code. A UDF accepts columns of input, performs actions on the input, and returns the result of those actions as a value. An attacker can write temporary UDFs to perform actions like updating columns or extracting PII from the tables. | | **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** | {  "UNIQUE": "bigquery.routines.insert"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Ensure authorized configuration(s) is used with the BigQuery dataset**    Ensure no dataset is accessible to "AllUsers" or "AllAuthenticatedUsers", except if allowed.    Define the authorized configuration (i.e., encryption key, table expiry, labels) for each BigQuery dataset.    Ensure the configuration of each BigQuery dataset is authorized. | Very High | 3 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Control access at the table and view level**    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).    Ensure only authorized IAM entities are allowed to access the tables, views, and table data in a specific dataset. | High | 2 | - | - |
| **Restrict access to columns with BigQuery column-level security**    Define the criteria for the sensitivity of columns in a table.    Ensure only authorized IAM entities are allowed to access sensitive columns of a table (e.g., using BigQuery column-level security or column-level data masking). | High | 2 | - | - |
| **Restrict access to rows with BigQuery row-level security**    Define the criteria for the sensitivity of rows in a table.    Ensure only authorized IAM entities are allowed to access sensitive rows of a table (e.g., using BigQuery row-level security). | Medium | 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** | | --- | --- | | Malicious code execution by importing data from cross Cloud Storage | [Medium (6.1)](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:H) | | 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) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Malicious code execution by importing data from cross Cloud Storage

| | **Threat Id** | Bigquery.T16 | | --- | --- | | **Name** | Malicious code execution by importing data from cross Cloud Storage | | **Description** | BigQuery Omni uses BigQuery connections to import data from Amazon S3 or Azure Storage. An attacker can create a connection to import malicious code as data from their Amazon S3 or Azure Storage to BigQuery for code execution. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0002](https://attack.mitre.org/tactics/TA0002) | | **CVSS** | [Medium (6.1)](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:H) | | **IAM Access** | {  "UNIQUE": "bigquery.connections.create"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit usage of BigQuery Omni**    Define the requirement for using BigQuery Omni (AWS and/or Azure).    Ensure the usage of BigQuery Omni as per the requirement (e.g. using organizational constraint [constraints/bigquery.disableBQOmniAWS](https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints) and [constraints/bigquery.disableBQOmniAzure](https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints)). | Very High | 2 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Secure the authorized destinations**    Maintain a list of authorized destinations (e.g., Cloud Storage, BigQuery, etc.) to be used with each table.    Ensure each table uses authorized sources and destinations (e.g., Cloud Storage, BigQuery, etc.).    Protect the sources and destinations used for infiltration/exfiltration with each table, using their respective service's ThreatModel. | High | 3 | - | - |

#### 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.getIamPolicy", "bigquery.connections.use"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Control access at the table and view level**    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).    Ensure only authorized IAM entities are allowed to access the tables, views, and table data in a specific dataset. | High | 2 | - | - |
| **Restrict access to columns with BigQuery column-level security**    Define the criteria for the sensitivity of columns in a table.    Ensure only authorized IAM entities are allowed to access sensitive columns of a table (e.g., using BigQuery column-level security or column-level data masking).    Define a criteria to use authorized data policies for each column in a table.    Ensure only authorized IAM entities are allowed to access sensitive columns of a table by using data policies. | High | 4 | - | - |
| **Restrict access to rows with BigQuery row-level security**    Define the criteria for the sensitivity of rows in a table.    Ensure only authorized IAM entities are allowed to access sensitive rows of a table (e.g., using BigQuery row-level security). | Medium | 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, 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** | {  "UNIQUE": "bigquery.connections.create"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Limit usage of BigQuery Omni**    Define the requirement for using BigQuery Omni (AWS and/or Azure).    Ensure the usage of BigQuery Omni as per the requirement (e.g. using organizational constraint [constraints/bigquery.disableBQOmniAWS](https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints) and [constraints/bigquery.disableBQOmniAzure](https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints)). | Very High | 2 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Secure the authorized destinations**    Maintain a list of authorized destinations (e.g., Cloud Storage, BigQuery, etc.) to be used with each table.    Ensure each table uses authorized sources and destinations (e.g., Cloud Storage, BigQuery, etc.).    Protect the sources and destinations used for infiltration/exfiltration with each table, using their respective service's ThreatModel. | High | 3 | - | - |

| 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 by removing reservations | [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:N/A:H) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Denial of Service by removing reservations

| | **Threat Id** | Bigquery.T12 | | --- | --- | | **Name** | Denial of Service by removing 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 or decreasing the performance for future jobs. | | **Goal** | Disruption of Service | | **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:N/A:H) | | **IAM Access** | {  "UNIQUE": "bigquery.reservations.delete"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Monitor system performance**    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).    Monitor slot capacity (e.g. using slot estimator) to estimate the right number of slots for the BigQuery workload. | Medium | - | - | 2 |

| 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 | [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:L/I:H/A:N) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Data exfiltration by updating the destination dataset in transfer and transfer credentials

| | **Threat Id** | Bigquery.T13 | | --- | --- | | **Name** | Data exfiltration by updating the destination dataset in transfer and transfer credentials | | **Description** | The BigQuery Data Transfer Service automates data movement into BigQuery on a scheduled, managed basis using the credentials of the user who created it. An attacker can update the destination dataset or transfer credentials of a transfer job and configuration to their own dataset and give them full control over the transfer. | | **Goal** | Data theft | | **MITRE ATT&CK®** | [TA0010](https://attack.mitre.org/tactics/TA0010) | | **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:L/I:H/A:N) | | **IAM Access** | {  "UNIQUE": "bigquery.transfers.update"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Enable logs for BigQuery Data Transfer**    Ensure Cloud Audit logs for BigQuery Data Transfer are enabled ([ref](https://cloud.google.com/bigquery-transfer/docs/audit-logging)). | Low | 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** | | --- | --- | | Model exfiltration by registering BigQuery ML models with the Vertex AI Model Registry | [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) | | Loss of integrity of 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) | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

#### Model exfiltration by registering BigQuery ML models with the Vertex AI Model Registry

| | **Threat Id** | Bigquery.T18 | | --- | --- | | **Name** | Model exfiltration by registering BigQuery ML models with the Vertex AI Model Registry | | **Description** | BigQuery ML models can be integrated with the Vertex AI Model Registry for management purposes. An attacker can register an existing model with their Vertex AI Model Registry 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** | {  "UNIQUE": "bigquery.models.updateData"  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Register BigQuery models as per requirement**    Define the requirement to register the BigQuery models with the Vertex AI Model Registry for each BigQuery model.    Ensure each BigQuery model is registered with the Vertex AI Model Registry according to its requirement. | Medium | 2 | - | - |

#### Loss of integrity of training model

| | **Threat Id** | Bigquery.T4 | | --- | --- | | **Name** | Loss of integrity of training model | | **Description** | ML models data to train on and the accuracy of the model depends on the quantity and quality of 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 into tables and views or removing data from them, decreasing the efficiency of the model created and harming the business decisions made on the basis of 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** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Monitor data ingestion**    Monitor the abnormal number of concurrent connections and throughput for BigQuery table (e.g., by using Monitoring metric CONSUMER QUOTA - QUOTA LIMIT). | Very Low | - | - | 1 |

| 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 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 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** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Create and secure backups (e.g., by snapshots or exports) of BigQuery dataset(s) and table(s)**    Define the requirement for the backup of each BigQuery dataset and table.    Ensure each BigQuery dataset and table is backed up (e.g., by creating snapshots or exports) according to its requirement 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 sub-resources.* 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 | [Low (2.9)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:C/C:N/I:L/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 a data policy and associate it with a column by attaching the policy tags associated with the column policy to the column in order to escalate privileges. | | **Goal** | Launch another attack | | **MITRE ATT&CK®** | [TA0004](https://attack.mitre.org/tactics/TA0004) | | **CVSS** | [Low (2.9)](https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:H/UI:R/S:C/C:N/I:L/A:N) | | **IAM Access** | {  "AND": ["bigquery.dataPolicies.create", "bigquery.dataPolicies.setIamPolicy", "bigquery.tables.setCategory", "bigquery.dataPolicies.update"]  } | |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |

| **Control Objectives** | **Priority** | **# of associated Controls** | | |
| --- | --- | --- | --- | --- |
| **Directive** | **Preventative** | **Detective** |
| **Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni**    Enforce VPC origin (e.g., using DNS redirection on a VPC-based proxy), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Very High | 1 | - | - |
| **Limit the access to the IAM actions required to execute the threats**    Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | High | 1 | - | - |
| **Restrict access to columns with BigQuery column-level security**    Define a criteria to use authorized data policies for each column in a table.    Ensure only authorized IAM entities are allowed to access sensitive columns of a table by using data policies. | Medium | 2 | - | - |

# Control Implementation

## Limit the access to the IAM actions required to execute the threats [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 the attack, following the IAM Operating Model and using the IAM ThreatModel. | Request the list of authorized IAM members with the permissions required to launch the attack, 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.T1 (Very High)  Bigquery.T2 (Very High)  Bigquery.T3 (Very High)  Bigquery.T4 (Very High)  Bigquery.T5 (Very High)  Bigquery.T6 (Very High)  Bigquery.T7 (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.T16 (Very High)  Bigquery.T17 (Very High)  Bigquery.T18 (Very High)  Bigquery.T19 (Very High) | High |

## Enforce VPC origin, and configure VPC Service Controls for BigQuery and BigQuery Omni [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), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Request the process and records of enabling and protecting VPC Service Controls for BigQuery and BigQuery-connected services, using the Compute ThreatModel. | Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC4  Bigquery.FC5  Bigquery.FC6  Bigquery.FC7  Bigquery.FC8 | Bigquery.T1 (High)  Bigquery.T3 (High)  Bigquery.T4 (High)  Bigquery.T5 (High)  Bigquery.T6 (High)  Bigquery.T7 (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) | Very High |

## Create and secure backups (e.g., by snapshots or exports) of BigQuery dataset(s) and table(s) [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 requirement for the backup of each BigQuery dataset and table. | Request the backup requirement of each BigQuery dataset and table. | Low | Bigquery.FC1  Bigquery.FC7 | Bigquery.T1 (Very Low)  Bigquery.T14 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C4, depends on Bigquery.C3, assured by Bigquery.C5]  Ensure each BigQuery dataset and table is backed up (e.g., by creating snapshots or exports) according to its requirement and is restorable. | Request the mechanism ensuring BigQuery datasets and tables are backed up (e.g., by creating snapshots or exports) according to its requirement, the evidence of its execution, and its regular testing of restoration. | High | Bigquery.FC1  Bigquery.FC7 | Bigquery.T1 (High)  Bigquery.T14 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C5]  Verify all BigQuery datasets and tables are backed up according to its requirement. | Change the backup mechanism to be outside requirements; it should be detected. | High | Bigquery.FC1  Bigquery.FC7 | - | Medium |

## Control access at the table and view level [Bigquery.CO4]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| 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) | 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 a specific 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) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C8]  Verify only authorized IAM entities are allowed to access the tables, views, and table data in a specific 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 |

## Restrict access to columns with BigQuery column-level security [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 a table. | Request the criteria for the sensitivity of columns in a table. | Very Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3 | Bigquery.T2 (Very Low)  Bigquery.T8 (Very Low)  Bigquery.T9 (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 a table (e.g., using BigQuery column-level security or column-level data masking). | Request 1) the mechanism ensuring only authorized IAM entities are allowed to access sensitive columns 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.T2 (High)  Bigquery.T8 (Medium)  Bigquery.T9 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C11]  Verify only authorized IAM entities are allowed to access sensitive columns of a table. | Configure an unauthorized IAM entity with access to a sensitive column; it should be detected. | Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C44]  Define a criteria to use authorized data policies for each column in a table. | Request the criteria for using data policies for each column in a 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, 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. | Configure an unauthorized IAM entity with access to a sensitive column; 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 a table. | Request the criteria for the sensitivity of rows in a table. | Very Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3 | Bigquery.T2 (Very Low)  Bigquery.T8 (Very Low)  Bigquery.T9 (Very Low) | Medium |
| 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.T2 (Medium)  Bigquery.T8 (Medium)  Bigquery.T9 (Medium) | Medium |
| 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 | - | Medium |

## Encrypt datasets and models at rest 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 dataset and model, ideally dedicated. | Request the list of authorized CMEKs to be used by the BigQuery dataset and model, its review process, and its review records. | Very Low | Bigquery.FC1 | Bigquery.T3 (Very Low)  Bigquery.T11 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C27, depends on Bigquery.C26, assured by Bigquery.C29]  Ensure only authorized CMEKs are used with each BigQuery dataset and model (e.g., using [default configuration](https://cloud.google.com/bigquery/docs/default-configuration)), and any unauthorized CMEKs are restricted following the Cloud KMS ThreatModel. | Request 1) the mechanism ensuring only authorized CMEKs are configured, 2) its records of execution for all new CMEKs, 3) the plan to move any older CMEKs, 4) the mechanism ensuring unauthorized CMEKs are restricted, and its records of execution. | Medium | Bigquery.FC1 | Bigquery.T11 (Medium) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C28, depends on Bigquery.C26]  Protect the CMEKs used by BigQuery datasets and models, using the Cloud KMS ThreatModel. | Request how the Cloud KMS ThreatModel is applied to BigQuery datasets and models. | High | Bigquery.FC1 | Bigquery.T3 (Medium)  Bigquery.T11 (Medium) | Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C29]  Verify each BigQuery dataset and model is encrypted using an authorized CMEK. | Use unauthorized CMEK with a BigQuery dataset; 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://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 |

## Ensure authorized configuration(s) is used with the BigQuery dataset [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://cloud.google.com/security-command-center/docs/concepts-vulnerabilities-findings#dataset-findings)). | Modify a dataset to be accessible to no dataset is accessible 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., encryption key, table expiry, labels) for each BigQuery dataset. | Request the authorized configuration for each BigQuery dataset. | Low | Bigquery.FC1  Bigquery.FC2 | Bigquery.T8 (Very Low)  Bigquery.T11 (Very Low) | 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) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C19]  Verify all BigQuery datasets have authorized configuration. | Create a dataset with an unauthorized configuration; it should be detected. | High | Bigquery.FC1  Bigquery.FC2 | - | 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). | Do not identify and redact sensitive data; it should be detected. | High | Bigquery.FC1 | - | Medium |

## Secure the authorized destinations [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 destinations (e.g., Cloud Storage, BigQuery, etc.) to be used with each table. | Request the list of all authorized destinations (e.g., Cloud Storage, BigQuery, etc.) to be used with each table. | High | Bigquery.FC1  Bigquery.FC3 | Bigquery.T3 (Very Low)  Bigquery.T15 (Very Low)  Bigquery.T16 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C23, depends on Bigquery.C22, assured by Bigquery.C24]  Ensure each table uses authorized sources and destinations (e.g., Cloud Storage, BigQuery, etc.). | Request 1) the mechanism ensuring only authorized sources and destinations (e.g., Cloud Storage, BigQuery, etc.) are configured, 2) its records of execution for all new sources and destinations (e.g., Cloud Storage, BigQuery, etc.), and 3) the plan to move any older sources and destinations (e.g., Cloud Storage, BigQuery, etc.). | Medium | Bigquery.FC1  Bigquery.FC3 | Bigquery.T3 (High)  Bigquery.T15 (High)  Bigquery.T16 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C24]  Verify each table uses authorized sources and destinations (e.g., Cloud Storage, BigQuery, etc.). | For a BigQuery table, use an unauthorized 1) source and 2) destination (e.g., Cloud Storage, BigQuery, etc.); it should be detected. | Medium | Bigquery.FC1  Bigquery.FC3 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C25, depends on Bigquery.C22]  Protect the sources and destinations used for infiltration/exfiltration with each table, using their respective service's ThreatModel. | Request how the respective source and destination ThreatModel is applied to BigQuery. | High | Bigquery.FC1  Bigquery.FC3 | Bigquery.T3 (High)  Bigquery.T15 (High)  Bigquery.T16 (High) | Medium |

## Set the quotas on BigQuery as per the API usage statistics [Bigquery.CO11]

| **Type** | **Control** | **Testing** | **Effort** | **Feature**  **Class(es)** | **Threat(s)**  **and Impact** | **CVSS-weighted**  **Priority** |
| --- | --- | --- | --- | --- | --- | --- |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C30, assured by Bigquery.C31]  Ensure the [quotas](https://cloud.google.com/bigquery/quotas) on BigQuery (e.g., query limits, streaming insert limits, etc.) are set as per the API usage statistics. | Request the mechanism to ensure the [quotas](https://cloud.google.com/bigquery/quotas) on BigQuery (e.g., query limits, streaming insert limits, etc.) are set as per the API usage statistics. | High | Bigquery.FC1 | Bigquery.T7 (High) | Very Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C31]  Verify the quotas on BigQuery are set as per the API usage statistics. | Do not set the quotas on BigQuery as per the API usage statistics; it should be detected. | High | Bigquery.FC1 | - | Very Low |

## 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 requirement for the expiration time of each BigQuery table. | Request the requirement for the expiration time of each BigQuery table. | Low | Bigquery.FC1 | Bigquery.T11 (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 its requirement. | Request the mechanism ensuring expiration time of each BigQuery table is set according to its requirement. | 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 requirement. | Set the expiration time of a BigQuery table to be outside requirement; it should be detected. | High | Bigquery.FC1 | - | Medium |

## Monitor system performance [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). | Stop a job using slots; it should be detected. | Low | Bigquery.FC5 | Bigquery.T12 (Medium) | Medium |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C43]  Monitor slot capacity (e.g. using slot estimator) to estimate the right number of slots for the BigQuery workload. | Stop unnecessary slots; it should be detected. | Low | Bigquery.FC5 | Bigquery.T12 (Low) | Low |

## Limit usage 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 requirement for using BigQuery Omni (AWS and/or Azure). | Request the requirement for the usage of BigQuery Omni. | Low | Bigquery.FC3 | Bigquery.T15 (Very Low)  Bigquery.T16 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C39, depends on Bigquery.C38, assured by Bigquery.C40]  Ensure the usage of BigQuery Omni as per the requirement (e.g. using organizational constraint [constraints/bigquery.disableBQOmniAWS](https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints) and [constraints/bigquery.disableBQOmniAzure](https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints)). | Request the implementation to ensure the usage of BigQuery Omni as per the requirement, and its records of execution. | Medium | Bigquery.FC3 | Bigquery.T15 (Very High)  Bigquery.T16 (Medium) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C40]  Verify the usage of BigQuery Omni as per the requirement. | Use BigQuery Omni outside the requirement; it should be detected. | Low | Bigquery.FC3 | - | 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://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 |

## Monitor data ingestion [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 BigQuery table (e.g., by using Monitoring metric CONSUMER QUOTA - QUOTA LIMIT). | Ingest large amount of data to a BigQuery table; it should be detected. | Low | Bigquery.FC1  Bigquery.FC6 | Bigquery.T4 (Very Low)  Bigquery.T5 (Very Low) | Very Low |

## Register BigQuery models as per requirement [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 requirement to register the BigQuery models with the Vertex AI Model Registry for each BigQuery model. | Request the registration requirement of 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 requirement. | Request the mechanism ensuring BigQuery model is registered according to its requirement, the evidence of its 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 its requirement. | Register the model with a Vertex AI Model Registry outside the requirement; it should be detected. | High | Bigquery.FC6 | - | Medium |

## Set the time travel of a BigQuery dataset as per the requirements [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 requirement for the time travel of each BigQuery dataset. | Request the requirement for the time travel of each BigQuery dataset. | Low | Bigquery.FC1 | Bigquery.T19 (Very Low) | Medium |
| 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 requirement. | Request the mechanism ensuring the time travel of each BigQuery dataset is set according to its requirement. | Medium | Bigquery.FC1 | Bigquery.T19 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C52]  Verify the time travel of each BigQuery dataset is set to its requirement. | Set the time travel of a BigQuery dataset to an unauthorized value; it should be detected. | High | Bigquery.FC1 | - | Medium |

## Clone BigQuery tables as per the requirement [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 requirement for the cloning of each BigQuery table. | Request the requirement for the cloning of each BigQuery table. | Low | Bigquery.FC1 | Bigquery.T1 (Very Low)  Bigquery.T19 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C54, depends on Bigquery.C53, assured by Bigquery.C55]  Ensure the cloning of each BigQuery table is according to its requirement. | Request the mechanism ensuring cloning of each BigQuery table is set according to its requirement. | Medium | Bigquery.FC1 | Bigquery.T1 (Medium)  Bigquery.T19 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C55]  Verify the cloning of each BigQuery table is set to its requirement. | Clone a BigQuery table outside the requirement; it should be detected. | High | Bigquery.FC1 | - | Medium |

# 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), allow port 443 only on Firewall, and configure VPC Service Controls (if applicable) for BigQuery and BigQuery-connected services (e.g., Pub/Sub, KMS) considering different sensitivity of environment (e.g., Prod vs. Non-Prod), using the Compute ThreatModel. | Request the process and records of enabling and protecting VPC Service Controls for BigQuery and BigQuery-connected services, using the Compute ThreatModel. | Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC4  Bigquery.FC5  Bigquery.FC6  Bigquery.FC7  Bigquery.FC8 | Bigquery.T1 (High)  Bigquery.T3 (High)  Bigquery.T4 (High)  Bigquery.T5 (High)  Bigquery.T6 (High)  Bigquery.T7 (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) | 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://cloud.google.com/security-command-center/docs/concepts-vulnerabilities-findings#dataset-findings)). | Modify a dataset to be accessible to no dataset is accessible to 1) "AllUsers", or 2) "AllAuthenticatedUsers"; it should be detected. | Very Low | Bigquery.FC1  Bigquery.FC2 | - | Very High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C1]  Limit the access to the IAM actions required to perform the attack, following the IAM Operating Model and using the IAM ThreatModel. | Request the list of authorized IAM members with the permissions required to launch the attack, 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.T1 (Very High)  Bigquery.T2 (Very High)  Bigquery.T3 (Very High)  Bigquery.T4 (Very High)  Bigquery.T5 (Very High)  Bigquery.T6 (Very High)  Bigquery.T7 (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.T16 (Very High)  Bigquery.T17 (Very High)  Bigquery.T18 (Very High)  Bigquery.T19 (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) | 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 a specific 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) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C8]  Verify only authorized IAM entities are allowed to access the tables, views, and table data in a specific 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 |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C9]  Define the criteria for the sensitivity of columns in a table. | Request the criteria for the sensitivity of columns in a table. | Very Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3 | Bigquery.T2 (Very Low)  Bigquery.T8 (Very Low)  Bigquery.T9 (Very Low) | High |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C38]  Define the requirement for using BigQuery Omni (AWS and/or Azure). | Request the requirement for the usage of BigQuery Omni. | Low | Bigquery.FC3 | Bigquery.T15 (Very Low)  Bigquery.T16 (Very Low) | High |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C39, depends on Bigquery.C38, assured by Bigquery.C40]  Ensure the usage of BigQuery Omni as per the requirement (e.g. using organizational constraint [constraints/bigquery.disableBQOmniAWS](https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints) and [constraints/bigquery.disableBQOmniAzure](https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#available_constraints)). | Request the implementation to ensure the usage of BigQuery Omni as per the requirement, and its records of execution. | Medium | Bigquery.FC3 | Bigquery.T15 (Very High)  Bigquery.T16 (Medium) | High |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C40]  Verify the usage of BigQuery Omni as per the requirement. | Use BigQuery Omni outside the requirement; it should be detected. | Low | Bigquery.FC3 | - | High |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C3]  Define the requirement for the backup of each BigQuery dataset and table. | Request the backup requirement of each BigQuery dataset and table. | Low | Bigquery.FC1  Bigquery.FC7 | Bigquery.T1 (Very Low)  Bigquery.T14 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C4, depends on Bigquery.C3, assured by Bigquery.C5]  Ensure each BigQuery dataset and table is backed up (e.g., by creating snapshots or exports) according to its requirement and is restorable. | Request the mechanism ensuring BigQuery datasets and tables are backed up (e.g., by creating snapshots or exports) according to its requirement, the evidence of its execution, and its regular testing of restoration. | High | Bigquery.FC1  Bigquery.FC7 | Bigquery.T1 (High)  Bigquery.T14 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C5]  Verify all BigQuery datasets and tables are backed up according to its requirement. | Change the backup mechanism to be outside requirements; it should be detected. | High | Bigquery.FC1  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 a table (e.g., using BigQuery column-level security or column-level data masking). | Request 1) the mechanism ensuring only authorized IAM entities are allowed to access sensitive columns 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.T2 (High)  Bigquery.T8 (Medium)  Bigquery.T9 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C11]  Verify only authorized IAM entities are allowed to access sensitive columns of a table. | Configure an unauthorized IAM entity with access to a sensitive column; it should be detected. | Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C44]  Define a criteria to use authorized data policies for each column in a table. | Request the criteria for using data policies for each column in a 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, 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. | Configure an unauthorized IAM entity with access to a sensitive column; it should be detected. | Low | Bigquery.FC3  Bigquery.FC8 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C12]  Define the criteria for the sensitivity of rows in a table. | Request the criteria for the sensitivity of rows in a table. | Very Low | Bigquery.FC1  Bigquery.FC2  Bigquery.FC3 | Bigquery.T2 (Very Low)  Bigquery.T8 (Very Low)  Bigquery.T9 (Very Low) | Medium |
| 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.T2 (Medium)  Bigquery.T8 (Medium)  Bigquery.T9 (Medium) | Medium |
| 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 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C26]  Maintain a list of authorized CMEKs to be used with each BigQuery dataset and model, ideally dedicated. | Request the list of authorized CMEKs to be used by the BigQuery dataset and model, its review process, and its review records. | Very Low | Bigquery.FC1 | Bigquery.T3 (Very Low)  Bigquery.T11 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C27, depends on Bigquery.C26, assured by Bigquery.C29]  Ensure only authorized CMEKs are used with each BigQuery dataset and model (e.g., using [default configuration](https://cloud.google.com/bigquery/docs/default-configuration)), and any unauthorized CMEKs are restricted following the Cloud KMS ThreatModel. | Request 1) the mechanism ensuring only authorized CMEKs are configured, 2) its records of execution for all new CMEKs, 3) the plan to move any older CMEKs, 4) the mechanism ensuring unauthorized CMEKs are restricted, and its records of execution. | Medium | Bigquery.FC1 | Bigquery.T11 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C29]  Verify each BigQuery dataset and model is encrypted using an authorized CMEK. | Use unauthorized CMEK with a BigQuery dataset; 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://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.C17]  Define the authorized configuration (i.e., encryption key, table expiry, labels) for each BigQuery dataset. | Request the authorized configuration for each BigQuery dataset. | Low | Bigquery.FC1  Bigquery.FC2 | Bigquery.T8 (Very Low)  Bigquery.T11 (Very Low) | 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) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C19]  Verify all BigQuery datasets have authorized configuration. | Create a dataset with an unauthorized configuration; it should be detected. | High | Bigquery.FC1  Bigquery.FC2 | - | 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). | Do not identify and redact sensitive data; it should be detected. | High | Bigquery.FC1 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C22]  Maintain a list of authorized destinations (e.g., Cloud Storage, BigQuery, etc.) to be used with each table. | Request the list of all authorized destinations (e.g., Cloud Storage, BigQuery, etc.) to be used with each table. | High | Bigquery.FC1  Bigquery.FC3 | Bigquery.T3 (Very Low)  Bigquery.T15 (Very Low)  Bigquery.T16 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C23, depends on Bigquery.C22, assured by Bigquery.C24]  Ensure each table uses authorized sources and destinations (e.g., Cloud Storage, BigQuery, etc.). | Request 1) the mechanism ensuring only authorized sources and destinations (e.g., Cloud Storage, BigQuery, etc.) are configured, 2) its records of execution for all new sources and destinations (e.g., Cloud Storage, BigQuery, etc.), and 3) the plan to move any older sources and destinations (e.g., Cloud Storage, BigQuery, etc.). | Medium | Bigquery.FC1  Bigquery.FC3 | Bigquery.T3 (High)  Bigquery.T15 (High)  Bigquery.T16 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C24]  Verify each table uses authorized sources and destinations (e.g., Cloud Storage, BigQuery, etc.). | For a BigQuery table, use an unauthorized 1) source and 2) destination (e.g., Cloud Storage, BigQuery, etc.); it should be detected. | Medium | Bigquery.FC1  Bigquery.FC3 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C25, depends on Bigquery.C22]  Protect the sources and destinations used for infiltration/exfiltration with each table, using their respective service's ThreatModel. | Request how the respective source and destination ThreatModel is applied to BigQuery. | High | Bigquery.FC1  Bigquery.FC3 | Bigquery.T3 (High)  Bigquery.T15 (High)  Bigquery.T16 (High) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C32]  Define the requirement for the expiration time of each BigQuery table. | Request the requirement for the expiration time of each BigQuery table. | Low | Bigquery.FC1 | Bigquery.T11 (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 its requirement. | Request the mechanism ensuring expiration time of each BigQuery table is set according to its requirement. | 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 requirement. | Set the expiration time of a BigQuery table to be outside requirement; it should be detected. | High | Bigquery.FC1 | - | 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). | Stop a job using slots; it should be detected. | Low | Bigquery.FC5 | Bigquery.T12 (Medium) | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C47]  Define the requirement to register the BigQuery models with the Vertex AI Model Registry for each BigQuery model. | Request the registration requirement of 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 requirement. | Request the mechanism ensuring BigQuery model is registered according to its requirement, the evidence of its 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 its requirement. | Register the model with a Vertex AI Model Registry outside the requirement; it should be detected. | High | Bigquery.FC6 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C50]  Define the requirement for the time travel of each BigQuery dataset. | Request the requirement for the time travel of each BigQuery dataset. | Low | Bigquery.FC1 | Bigquery.T19 (Very Low) | Medium |
| 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 requirement. | Request the mechanism ensuring the time travel of each BigQuery dataset is set according to its requirement. | Medium | Bigquery.FC1 | Bigquery.T19 (Medium) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C52]  Verify the time travel of each BigQuery dataset is set to its requirement. | Set the time travel of a BigQuery dataset to an unauthorized value; it should be detected. | High | Bigquery.FC1 | - | Medium |
| Directive (COSO)  Identify (NIST CSF) | [Bigquery.C53]  Define the requirement for the cloning of each BigQuery table. | Request the requirement for the cloning of each BigQuery table. | Low | Bigquery.FC1 | Bigquery.T1 (Very Low)  Bigquery.T19 (Very Low) | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C54, depends on Bigquery.C53, assured by Bigquery.C55]  Ensure the cloning of each BigQuery table is according to its requirement. | Request the mechanism ensuring cloning of each BigQuery table is set according to its requirement. | Medium | Bigquery.FC1 | Bigquery.T1 (Medium)  Bigquery.T19 (High) | Medium |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C55]  Verify the cloning of each BigQuery table is set to its requirement. | Clone a BigQuery table outside the requirement; it should be detected. | High | Bigquery.FC1 | - | Medium |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C28, depends on Bigquery.C26]  Protect the CMEKs used by BigQuery datasets and models, using the Cloud KMS ThreatModel. | Request how the Cloud KMS ThreatModel is applied to BigQuery datasets and models. | High | Bigquery.FC1 | Bigquery.T3 (Medium)  Bigquery.T11 (Medium) | Low |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C43]  Monitor slot capacity (e.g. using slot estimator) to estimate the right number of slots for the BigQuery workload. | Stop unnecessary slots; 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://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 |
| Directive (COSO)  Protect (NIST CSF) | [Bigquery.C30, assured by Bigquery.C31]  Ensure the [quotas](https://cloud.google.com/bigquery/quotas) on BigQuery (e.g., query limits, streaming insert limits, etc.) are set as per the API usage statistics. | Request the mechanism to ensure the [quotas](https://cloud.google.com/bigquery/quotas) on BigQuery (e.g., query limits, streaming insert limits, etc.) are set as per the API usage statistics. | High | Bigquery.FC1 | Bigquery.T7 (High) | Very Low |
| Assurance (COSO)  Detect (NIST CSF) | [Bigquery.C31]  Verify the quotas on BigQuery are set as per the API usage statistics. | Do not set the quotas on BigQuery as per the API usage statistics; it should be detected. | High | Bigquery.FC1 | - | Very Low |
| Detective (COSO)  Detect (NIST CSF) | [Bigquery.C42]  Monitor the abnormal number of concurrent connections and throughput for BigQuery table (e.g., by using Monitoring metric CONSUMER QUOTA - QUOTA LIMIT). | Ingest large amount of data to a BigQuery table; it should be detected. | Low | Bigquery.FC1  Bigquery.FC6 | Bigquery.T4 (Very Low)  Bigquery.T5 (Very Low) | 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 | - | 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 | - | - |
| Bigquery.A11 | Delete table snapshots. | Bigquery.FC7 | bigquery.tables.deleteSnapshot | - | - |
| Bigquery.A12 | Export table data out of BigQuery. | Bigquery.FC1 | bigquery.tables.export | - | - |
| Bigquery.A13 | Restore table snapshots. | Bigquery.FC7 | bigquery.tables.restoreSnapshot | - | - |
| 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 | - | 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 | - | 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  bigquery.tables.getData | 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 | TODO | bigquery.routines.list |
| Bigquery.A27 | Gets the specified routine resource by routine ID. | Bigquery.FC2 | bigquery.routines.get | TODO | bigquery.routines.get |
| Bigquery.A28 | Creates a new routine in the dataset. | Bigquery.FC2 | bigquery.routines.create | TODO | bigquery.routines.insert |
| Bigquery.A29 | Deletes the routine specified by routineid from the dataset. | Bigquery.FC2 | bigquery.routines.delete | datasetservice.delete | bigquery.routines.delete |
| Bigquery.A30 | Updates information in an existing routine. The update method replaces the entire routine resource. | Bigquery.FC2 | bigquery.routines.update | TODO | bigquery.routines.update |
| Bigquery.A31 | Returns the dataset specified by datasetid. | Bigquery.FC1 | bigquery.datasets.get | TODO | 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 | TODO | bigquery.datasets.patch |
| Bigquery.A33 | Lists all datasets in the specified project. | Bigquery.FC1 | bigquery.datasets.get | TODO | 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 | 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 | - | 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 | - | - |
| Bigquery.A41 | Delete a row-level access policy from a table. | Bigquery.FC1 | bigquery.rowAccessPolicies.delete | - | - |
| 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 | - | - |
| 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.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 | - | - |
| 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 | - | 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 | datasetservice.delete | 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 | - | - |
| 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 | jobservice.insert | - |
| Bigquery.A64 | Returns specified connection. | Bigquery.FC3 | bigquery.connections.get | - | bigqueryconnection.projects.locations.connections.get |
| Bigquery.A65 | Deletes connection and associated credential. | Bigquery.FC3 | bigquery.connections.delete | - | 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 | - | bigqueryconnection.projects.locations.connections.patch |
| Bigquery.A67 | Returns a list of connections in the given project. | Bigquery.FC3 | bigquery.connections.list | - | 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 | - | 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 | - | bigqueryconnection.projects.locations.connections.setIamPolicy |
| Bigquery.A72 | Sets the credential for the specified connection. | Bigquery.FC3 | - | - | bigqueryconnection.projects.locations.connections.updateCredential |
| Bigquery.A73 | Lists information about the supported locations for this service. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.locations.list |
| Bigquery.A74 | Gets information about a location. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.locations.get |
| Bigquery.A75 | Deletes the specified transfer run. | Bigquery.FC4 | bigquery.transfers.update | - | bigquerydatatransfer.projects.locations.transferConfigs.runs.delete |
| Bigquery.A76 | Returns information about the particular transfer run. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.locations.transferConfigs.runs.get |
| Bigquery.A77 | Returns information about running and completed jobs. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.locations.transferConfigs.runs.list |
| Bigquery.A78 | Returns user facing log messages for the data transfer run. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.locations.transferConfigs.runs.transferLogs.list |
| Bigquery.A79 | 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.A80 | Returns information about a data transfer config. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.locations.transferConfigs.get |
| Bigquery.A81 | 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 | - | bigquerydatatransfer.projects.locations.transferConfigs.startManualRuns |
| Bigquery.A82 | Returns information about all data transfers in the project. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.locations.transferConfigs.list |
| Bigquery.A83 | Creates a new data transfer configuration. | Bigquery.FC4 | bigquery.transfers.update | - | bigquerydatatransfer.projects.locations.transferConfigs.create |
| Bigquery.A84 | Deletes a data transfer configuration, including any associated transfer runs and logs. | Bigquery.FC4 | bigquery.transfers.update | - | bigquerydatatransfer.projects.locations.transferConfigs.delete |
| Bigquery.A85 | Updates a data transfer configuration. All fields must be set, even if they are not updated. | Bigquery.FC4 | bigquery.transfers.update | - | bigquerydatatransfer.projects.locations.transferConfigs.patch |
| Bigquery.A86 | Retrieves a supported data source and returns its settings, which can be used for ui rendering. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.locations.dataSources.get |
| Bigquery.A87 | 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 | - | - | bigquerydatatransfer.projects.locations.dataSources.checkValidCreds |
| Bigquery.A88 | Lists supported data sources and returns their settings, which can be used for ui rendering. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.locations.dataSources.list |
| Bigquery.A89 | 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.A90 | Lists supported data sources and returns their settings, which can be used for ui rendering. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.dataSources.list |
| Bigquery.A91 | 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 | - | - | bigquerydatatransfer.projects.dataSources.checkValidCreds |
| Bigquery.A92 | Returns information about running and completed jobs. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.transferConfigs.runs.list |
| Bigquery.A93 | Deletes the specified transfer run. | Bigquery.FC4 | bigquery.transfers.update | - | bigquerydatatransfer.projects.transferConfigs.runs.delete |
| Bigquery.A94 | Returns information about the particular transfer run. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.transferConfigs.runs.get |
| Bigquery.A95 | Returns user facing log messages for the data transfer run. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.transferConfigs.runs.transferLogs.list |
| Bigquery.A96 | Returns information about a data transfer config. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.transferConfigs.get |
| Bigquery.A97 | Returns information about all data transfers in the project. | Bigquery.FC4 | bigquery.transfers.get | - | bigquerydatatransfer.projects.transferConfigs.list |
| Bigquery.A98 | Updates a data transfer configuration. All fields must be set, even if they are not updated. | Bigquery.FC4 | bigquery.transfers.update | - | bigquerydatatransfer.projects.transferConfigs.patch |
| Bigquery.A99 | 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.A100 | 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 | - | bigquerydatatransfer.projects.transferConfigs.startManualRuns |
| Bigquery.A101 | Creates a new data transfer configuration. | Bigquery.FC4 | bigquery.transfers.update | - | bigquerydatatransfer.projects.transferConfigs.create |
| Bigquery.A102 | Deletes a data transfer configuration, including any associated transfer runs and logs. | Bigquery.FC4 | bigquery.transfers.update | - | bigquerydatatransfer.projects.transferConfigs.delete |
| Bigquery.A103 | Returns information about the capacity commitment. | Bigquery.FC5 | bigquery.capacityCommitments.get | - | bigqueryreservation.projects.locations.capacityCommitments.get |
| Bigquery.A104 | 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.A105 | Lists all the capacity commitments for the admin project. | Bigquery.FC5 | bigquery.capacityCommitments.list | - | bigqueryreservation.projects.locations.capacityCommitments.list |
| Bigquery.A106 | Creates a new capacity commitment resource. | Bigquery.FC5 | bigquery.capacityCommitments.create | - | bigqueryreservation.projects.locations.capacityCommitments.create |
| Bigquery.A107 | 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.A108 | 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.A109 | 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.A110 | 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 | - | bigqueryreservation.projects.locations.reservations.assignments.create |
| Bigquery.A111 | Deletes a assignment. | Bigquery.FC5 | bigquery.reservationAssignments.delete | - | bigqueryreservation.projects.locations.reservations.assignments.delete |
| Bigquery.A112 | Lists assignments. Only explicitly created assignments will be returned. | Bigquery.FC5 | bigquery.reservationAssignments.list | - | bigqueryreservation.projects.locations.reservations.assignments.list |
| Bigquery.A113 | 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.A114 | Lists all the reservations for the project in the specified location. | Bigquery.FC5 | bigquery.reservations.list | - | bigqueryreservation.projects.locations.reservations.list |
| Bigquery.A115 | Returns information about the reservation. | Bigquery.FC5 | bigquery.reservations.get | - | bigqueryreservation.projects.locations.reservations.get |
| Bigquery.A116 | Deletes a reservation. Returns google. Rpc. Code. Failed\_precondition when reservation has assignments. | Bigquery.FC5 | bigquery.reservations.delete | - | bigqueryreservation.projects.locations.reservations.delete |
| Bigquery.A117 | Creates a new reservation resource. | Bigquery.FC5 | bigquery.reservations.create | - | bigqueryreservation.projects.locations.reservations.create |
| Bigquery.A118 | Updates an existing reservation resource. | Bigquery.FC5 | bigquery.reservations.update | - | bigqueryreservation.projects.locations.reservations.patch |
| Bigquery.A119 | Retrieves a BI reservation. | Bigquery.FC5 | bigquery.bireservations.get | - | bigqueryreservation.projects.locations.getBiReservation |
| Bigquery.A120 | 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.A121 | 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.A122 | 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.A125 | Updates the tags for an existing connection. | Bigquery.FC3 | bigquery.connections.updateTag | - | - |
| Bigquery.A126 | Updates the tags for an existing model. | Bigquery.FC6 | bigquery.models.updateTag | - | - |
| Bigquery.A130 | Updates the tags for an existing routine. | Bigquery.FC2 | bigquery.routines.updateTag | - | - |
| Bigquery.A131 | Enroll data sources in a user project. This allows users to create transfer configurations for these data sources. | Bigquery.FC4 | - | - | bigquerydatatransfer.projects.enrollDataSources |
| Bigquery.A132 | 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.A134 | Access historical data for a table that has, or has previously had, row-level access policies. | Bigquery.FC1 | bigquery.rowAccessPolicies.overrideTimeTravelRestrictions | - | - |
| Bigquery.A135 | Delegate connection to create authorized external tables and remote functions. | Bigquery.FC3 | bigquery.connections.delegate | - | - |
| Bigquery.A136 | Retrieve execution metadata on any job. | Bigquery.FC1 | bigquery.jobs.listExecutionMetadata | - | - |
| Bigquery.A137 | Create index of a table. | Bigquery.FC1 | bigquery.tables.createIndex | - | - |
| Bigquery.A138 | Delete index of a table. | Bigquery.FC1 | bigquery.tables.deleteIndex | - | - |
| Bigquery.A139 | 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 | TODO | bigquerydatapolicy.projects.locations.dataPolicies.create |
| Bigquery.A140 | Deletes the data policy specified by its resource name. | Bigquery.FC8 | bigquery.dataPolicies.delete | TODO | bigquerydatapolicy.projects.locations.dataPolicies.delete |
| Bigquery.A141 | Gets the data policy specified by its resource name. | Bigquery.FC8 | bigquery.dataPolicies.get | TODO | bigquerydatapolicy.projects.locations.dataPolicies.get |
| Bigquery.A142 | Gets the IAM policy for the specified data policy. | Bigquery.FC8 | bigquery.dataPolicies.getIamPolicy | TODO | bigquerydatapolicy.projects.locations.dataPolicies.getIamPolicy |
| Bigquery.A143 | List all of the data policies in the specified parent project. | Bigquery.FC8 | bigquery.dataPolicies.list | TODO | bigquerydatapolicy.projects.locations.dataPolicies.list |
| Bigquery.A144 | -. | Bigquery.FC8 | bigquery.dataPolicies.maskedGet | TODO | - |
| Bigquery.A145 | Sets the IAM policy for the specified data policy. | Bigquery.FC8 | bigquery.dataPolicies.setIamPolicy | TODO | bigquerydatapolicy.projects.locations.dataPolicies.setIamPolicy |
| Bigquery.A146 | Updates the metadata for an existing data policy. The target data policy can be specified by the resource name. | Bigquery.FC8 | bigquery.dataPolicies.update | TODO | bigquerydatapolicy.projects.locations.dataPolicies.patch |