2.1 Ensure That Cloud Audit Logging Is Configured Properly Across All Services and All Users From a Project

***Sentinel Policy Name:***

* + 2.1 Ensure That Cloud Audit Logging Is Configured Properly Across All Services and All Users From a Project

***Category:***

* + Logging and Monitoring

***Description of Policy:***

* + As per CIS benchmarks, it is recommended that Cloud Audit Logging is configured to track all admin activities as well as read/write access of user data.

There are three kinds of Data Access audit log information:

* + Admin read: Records operations that read metadata or configuration information. Admin Activity audit logs record writes of metadata and configuration information that cannot be disabled.
  + Data read: Records operations that read user-provided data.
  + Data write: Records operations that write user-provided data

***Sentinel Policy Restriction:***

* + we are checking to ensure that DATA\_READ, DATA\_WRITE, and ADMIN\_READ audit logs are properly defined within the resource **'google\_project\_iam\_audit\_config'**
  + DATA\_READ, DATA\_WRITE, and ADMIN\_READ should be enabled for all services at the project- level.
  + This policy will ensure the **'exempted\_members'** attribute is always empty for all of the affected resources to ensure that all Google Cloud users are subjected to this policy.
  + This will ensure that all of the Cloud Audit logs are collected and stored appropriately. This will promote accountability among all users.

***Terraform attributes:***

Provider Ref: [google\_project\_iam | Resources | hashicorp/google | Terraform Registry](https://registry.terraform.io/providers/hashicorp/google/latest/docs/resources/google_project_iam#google_project_iam_audit_config)

Attributes affected

* + log\_type
  + Exempted\_members
  + service

***Test cases:***

**Pass cases**

NOTE: In order for a pass to occur, **all** of the requirements **must** be fulfilled:

* + For all **'iam\_audit\_config'** resources, the **'log\_type'** attribute is defined for DATA\_READ, DATA\_WRITE, and ADMIN\_READ per the CIS recommendation.
  + For all **'iam\_audit\_config'** resources, the **'exempted\_members'** attribute is not defined.
  + For all **'iam\_audit\_config'** resources, the 'service' attribute is set to **'allServices'**

**Fail case:**

NOTE: If only one, two, or none of the "Pass Cases" are present, policy will consistently result in a fail. The following are some examples of fail cases:

* + For 'google\_project\_iam\_audit\_config', the 'log\_type is set to something other than DATA\_READ, DATA\_WRITE, ADMIN\_READ
  + The 'service' attribute is set to something other than "allServices"
  + For iam\_audit\_config' resources, the 'log\_type' attribute has DATA\_READ defined (not DATA\_WRITE or ADMIN\_READ)