GCP STS Event-Driven IAM Role Matrix

Composer Service Account (GDW & APMF)

Resource	IAM Role	Purpose
STS API	roles/storagetransfer.user	Trigger STS jobs
GCS Source Bucket	roles/storage.objectViewer	Check for new files
GCS Dest Bucket (pull)	roles/storage.objectCreator	Allow STS pull
Cloud Functions (invoke)	roles/cloudfunctions.invoker	Only if triggered via HTTP
Cloud Composer	roles/composer.user	Trigger DAGs
(Optional) Project	roles/iam.serviceAccountTokenCreator	Only for SA impersonation

Cloud Function Service Account

Resource	IAM Role	Purpose
Pub/Sub Subscription	roles/pubsub.subscriber	Trigger on file upload
Composer REST API	roles/composer.user	Trigger DAGs remotely
Target GCS Bucket (optional)	roles/storage.objectViewer	Logging/Debugging access
(Optional)	roles/iam.serviceAccountTokenCreator	If impersonating Composer SA

Google-managed STS Service Account

Resource	IAM Role	Purpose
GCS Source Bucket	roles/storage.objectViewer	Read files
GCS Destination Bucket	roles/storage.objectCreator	Write files

AD Groups (Team Users)

Resource	IAM Role	Purpose
Service Account	roles/iam.serviceAccountUser	Allow impersonation of SA
	Do not assign TokenCreator	Never assign to AD group

Pub/Sub IAM Roles

Resource	IAM Role	Purpose
GCS Bucket -> Pub/Sub Topic	roles/pubsub.publisher	Publish object finalize events
Cloud Function SA -> Subscription	roles/pubsub.subscriber	Trigger Cloud Function