# Compliance Center data copy from one storage account to another

Microsoft 365 Compliance Center *is a dedicated workspace for your compliance, privacy, and risk management specialists.*It’s packed with useful administrative tools to support you in meeting your legal, regulatory, and organizational requirements. Compliance center has a feature to export compliance data to a storage account in Azure. Currently this storage account cannot be secured with storage account firewalls or private links. This could be a challenge for highly regulated environment as the data exported from compliance center could be user email, Teams conversations etc. Below I have tried to address that problem by copying these files to a secure storage account as soon as they arrive thus reducing the risk of data leak. The data is copied as soon as “Summary.txt” arrives in the source storage container to a destination storage container via an Azure Function. The architecture is as below. The logic can be extended to cater to other use cases but some edits in the Function may be needed. As this implementation is written specifically for compliance center.

Timeline

Description automatically generated

The function implementation is as is in repository.

Follow the below steps to setup the environment (ARM template WIP) :

1. Create two storage accounts
   1. Source storage account with source blob container
   2. Target storage account with target blob container
2. Create a Function App in premium plan with Python version 3.~ and configure env variables listed below
   1. SOURCE\_ACCOUNT\_URL
   2. SOURCE\_CONTAINER\_NAME
   3. TARGET\_ACCOUNT\_URL
   4. TARGET\_CONTAINER\_NAME
3. Deploy a Function App with Premium Plan. Premium plan ensures that the function timeout is 60 mins and also allows vNET integration (For the target storage account).
4. Configure Function App System Assigned Managed identity and give this identity "Blob Data Contributor role" in both source and target storage containers (Limit scope to container only) .
5. Deploy a vNET and configure two subnets in it. The IP range in the vNET can be anything as the traffic will not travel outside of the vNET.
   1. Function-app-subnet
   2. Private-link-subnet
6. Configure target storage account for private access
   1. Disallow all networksGraphical user interface, text, application, email

      Description automatically generated
   2. Select Private endpointGraphical user interface, text, application, email

      Description automatically generated
   3. Configure Private Endpoint. Choose the right region and choose blob storage. In ‘Configuration’ step of private endpoint choose the vNet created earlier and private-link-subnet. Also configure the Private DNS zone and connect it to the same vNET. Follow the instructions in the Azure portal prompt.

Graphical user interface, text, application

Description automatically generated

1. Configure the Function App outbound connectivity to the vNET and choose function-app-subnet. This will allow private connectivity to target container. Graphical user interface, application, chat or text message

   Description automatically generated
2. Now publish the 2 functions to the FunctionApp. Clone the repository from GitHub and run the following commands in that directory. Once done the Function App will have two functions – EventGridTrigger1 & [DeleteSourceFilesEventGridTrigger](https://github.com/SahanaPrabhakar/Azure/tree/main/CopyDataBetweenStorageAccounts/DeleteSourceFilesEventGridTrigger)
   1. Az login
   2. Az account set --subscription <sub id>
   3. func azure functionapp publish <function app name>
3. In the source storage container, configure Event Grid system topic for "Blob created" and trigger Function app – EventGridTrigger1 function

Graphical user interface, text, application

Description automatically generated

Graphical user interface, application

Description automatically generated

1. Repeat the same steps for target storage container but connect with [DeleteSourceFilesEventGridTrigger](https://github.com/SahanaPrabhakar/Azure/tree/main/CopyDataBetweenStorageAccounts/DeleteSourceFilesEventGridTrigger) function
2. The setup is now ready. To test it initiate export from Compliance center. You should see the data land in source container and then get copied to target container. Once copied the source container is deleted.
   1. Login to <https://compliance.microsoft.com/> and initiate case export. Graphical user interface, text, application, email

      Description automatically generated
   2. Provide the Source Container SAS Token and URL

Graphical user interface, text, application, email

Description automatically generated