instructions on how to manually set up the Lambda function, S3 bucket, and IAM role:

S3 Bucket:

1. In the left navigation pane, choose Buckets.
2. Choose Create bucket.
3. For Bucket name, enter a name for your bucket(for example mybucket).
4. Under **Object Ownership**, choose disable ACLs.
5. Choose Create bucket.

IAM role:

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. First you need to create a policy:
    a. In the navigation pane of the console, choose Roles and then choose Create policy.
    b. Under *policy editor* choose JSON and paste the Json below:

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                        "Sid": "VisualEditor0",
                        "Effect": "Allow",
                        "Action": [
                                "s3:PutObject",
                                "s3:ListBucket"
                        ],
                        "Resource": "arn:aws:s3:::*"
                }
        ]
}
```

    c. Press Next and write a Policy Name (for example s3_list_and_put), and create the policy.
3. In the navigation pane of the console, choose Roles and then choose Create role.
4. Choose the Custom trust policy role type.
5. In the Use case section, choose Lambda, then next.

6. Under the Permissions policies search and choose the policy you created in 2 (name suggested was s3_list_and_put)

7. Name the role “MylambdaRole” and create it.

Lambda Function:

1. Open the Functions page of the Lambda console.
2. Choose Create function.
3. Select Author from scratch.
4. In the Basic information pane, for Function name enter myLambdaFunction.
5. For Runtime, choose Python 3.12
6. Leave architecture set to x86_64 and choose Create function.
7. Open *Change default execution* **role** and *choose Use an existing role.*
8. Under Existing role choose the role you just created (MylambdaRole)
9. Choose create function
10. In the code source paste the attached lambda_function.py file.
11. Press Deploy.