**Portfolio 2 Report:**

This report aims to outline the cloud infrastructure I created along with evidence and justification for each of my choices and how it was made along with completing the 5 requirements set out in the coursework.

**Requirement 1:**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated  
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

In the screenshots above you can see the process I went through to create the VPC, internet gateway along with the subnets and nat gateway. I used a single VPC as I wanted the whole organization under the same VPC and not multiple VPCs making it easier to communicate in the company. I created the IGW for the teams that require internet access to be able to access it along with the nat gateway being configured to the private subnet for internet access securely.

**Requirement 2:**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

In the screenshots above you can see an example of a security group I made along with the complete security groups for every team and their IAM roles. I chose each team to have their own group and roles to clearly define security parameters as each team needed different levels of permissions in inbound and outbound traffic. The IAM roles are based on least privilege to ensure teams only have access to what they need to complete their tasks

**Requirement 3:**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

In the screenshots above you can see the creation of a launch template, auto scaling group and application load balancer. The launch template is to standardise instances, so they all have the same base. The auto scaling means you have scalability with the amount of resources you use ensuring you can have cost optimisation too as you aren’t paying for resources you aren’t using. The load balancer distributes traffic evenly across the network making you less susceptible to DoS attacks and increasing network security

**Requirement 4:**

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

In the screenshot above you can see I chose a bucket as the storage service used for the customers information as its was the cheapest option and can still be secured and encrypted to protect against breaches. The bucket also has access control meaning not every team can read/write only the necessary ones, for example sales team can view only. I also enabled bucket versioning to retain data integrity along with cloud trail to log the activity of the bucket to check for suspicious activity if it occurs.

**Requirement 5:**

Certain challenges I encountered were instance type availability when trying to create the load balancer and auto scaling group in eu-west-2c they were unavailable meaning I had to create new subnets in available zones. Another challenge I encountered was cost optimising, as the company is a small one I wanted to reduce unnecessary costs while still maintaining a high level of security which was one of the reasons I chose a S3 bucket to use over RDS as its more cost-effective.

Some recommendations I have are keeping up to date with monitoring the infrastructure for example by using cloud watch and setting up alarms and being proactive with it to stay ahead. I also recommend documenting any changes in the system for example editing IAM roles/policies so you can easily audit the system and the necessary people can tell what’s going on in the infrastructure at any time. My final recommendation is setting up a budget in AWS to try keep costs low and not spend unnecessary amounts on services you don’t need or aren’t using.