Azure disaster strategy:

**- Number of virtual machines and their function.**

4 virtual machines.

* Web server: This will be the server that supports the website for the company.
* DNS server: This will be the dns server that will handle routing people who are viewing the online web server.
* File server: This will be for company information so that employees can access all the relevant data on a day-to-day basis.
* Database server: This will be the server that supports the web server in its needs to store customer and site visitor data.

**- Location of your virtual machines.**

The database server and web server will be located on Azure, but the file server and DNS server will be located on site.

**- RPO**

For the Database server the maximum amount of data that can be lost is 0. For the web server 50% of data can be lost because a copy of the site will exist in the file server since it will need to be regularly updated by supporting staff.

**- RTO**

The Web server can have a large RTO since it is not integral to the functions of the company, so it can be anywhere from 12 hours to 24 hours. But the database server is very important to company function so the desired rto would be as much as 4 hours.

**- What virtual machines have two or more instances in the same availability set**

The web server will have multiple instances in different regions to help with load distribution. The database will do the same but have 1/2 the instances because its load will not be as much of the web server. So, for specifics the web server will have 6 instances for different geo regions, and the database server will have 3 instances.

**- Type of storage: LRS or GRS**

The web server will have LRS storage since it is not integral to the company and can handle loss of data. The database on the other hand will have geo redundant storage to help with loss. The file server will also have LRS.

**- How you will protect your passphrase that would be used for restoring backups.**

There will be several locations in which the passphrases will be stored. One will be on the main file server in a restricted access drive so that only high-level employees have access to it. Then there will be a copy on every high-level managers personal computer with the same restricted access. Then finally the CTO of the company will have a personal locked drive that has all the passphrases as well.

**- Azure “Protection Procedures”.**

Recovery Services vault: this will be where all the backups are held and accessible. This is important because you will need to access the backed-up data if something happens.

Azure virtual machines back up: This will be used to back up the database and web server for the company in order to limit the loss of data.

Azure backup server: This will be used to back up the servers that we have and there configuration so that there is no loss so configuration data and also it will take less time to reinitialize if there is a failure.

Protect Azure SQL database: This will be used to back up the database server for "long term" data, since other backup options do not backup data for more than 1 month of data. This will allow the large amount of data in the database server to be saved for a long period of time.

**- Backup policies and replication frequency.**

Since I detailed that the different kinds of storage in the above section the backup policies will have to be adjusted to fit these needs, whether there LRS storage or GRS. Then for each server there are different frequencies that will be required. The database server will be backed-up every hour and then stored in the protected azure sql database. Then the webserver will be backed-up every week and stored for 30 days. The file server will be backed-up every day for 30 days.

**- How to get to the backups**

The backups are all available in the Recovery Services vault that was created for your backups, where you change the policy types. Finding said backups can vary between just clicking on save points that have been created or going into the drive where you specified where backups will be stored.

**- Recovery plan strategy.**

Since the servers that I detailed are not overly dependent on each other this is not entirely necessary but for extra protection the database server should be starting before the webserver so there will not be errors on the website when it tries to read/write data. To go along with this even though the DNS server is not supported in any way by virtualization through azure it too should start before the webserver so that connection routing will be ready when the web server restarts.

**- Initial steps to perform a site recovery.**

In order to have site recovery you need to setup a resource group and assign a storage account. Then you need to create the recovery service vault with the same resource group. Next is adding a virtual network to the resource group.

**- Why isn’t replicating a virtual machine considered an appropriate backup? See the video called “Protect an Azure virtual machine”.**

The copies are only replicated virtual machines. Replications are not backups; they are just the same machines over different locations. So, any problems from errors could be put on those replications.

**- When would you install the Azure Backup Server? See the video called “Installing the Azure Backup Server”.**

This would be necessary when you want uninterrupted server work between your on-site server and your backup server. So, for instance if you have a azure backup server you can have backed-up workloads that will continue to work even after a problem with the on site server. You will not have to reinitialize the workload and have possible lost data because of that re-initialization.