I usually recommend best practices development practices to the Principal Manager and enterprise Cloud team.

Here is a raw draft of such expertise recommendations as part of routine review and analysis of Sony's Azure's platform.

Some Azure confidentiality, integrity, security and availability, management best practices.

1. Applying the defense in depth practices (using a layered approach and address security in each layer)
2. Identity management practices: Azure Ad has number of features and capabilities to improve the identity security.
3. Infrastructure Protection: such as enabling locks on resources
4. Encryption

Review current role-based access in resources like Sql storage/virtual machines/

- delete resources that are expired like the certificates in the redirectwww portal

- review current virtual machines especially in dev RG and de-commission non used ones. apply auto shut downs to active VMs

- secure access to virtual machines and implements end point protection and keep systems patched and current

- Apply delete and read locks on resources (resource groups, apps and resources) -- infrastructure and resources protection

-review access to global key vault, limit list of members that have access to the vault, potentially assign Just in time access on request.

- Review network access - restrict inbound internet access

-control access to infrastructure change control

-periodic review of events and changes using the activity log

-apply alerts (email, webhook or SMS) in highly vulnerable resources

- make use of Azure security center. Its enabled in the prod subscription.

-encrypt the high risk sensitive and private date in disks: Example is the transparent data encryption (TDE) which helps to protect Azure SQL Database and Azure Data Warehouse against the threat of malicious activity. It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application. By default, TDE is enabled for all newly deployed Azure SQL Databases.

- if there is security team, more hands off to the security team to lead the security implementations

- enable multifactor authentication with active directory features.

- **Buy reserved instances to save money over pay-as-you-go.** This will review your virtual machine usage over the last 30 days and determine if you could save money in the future by purchasing reserved instances. Advisor will show you the regions and sizes where you potentially have the most savings and will show you the estimated savings you might achieve from purchasing reserved instances.

- **Right-size or shutdown underutilized virtual machines.** This monitors your virtual machine usage for 14 days and then identifies underutilized virtual machines. Virtual machine whose average CPU utilization is 5 percent or less and network usage is 7 MB or less for four or more days are considered underutilized virtual machines. The average CPU utilization threshold is adjustable up to 20 percent. By identifying these virtual machines, you can decide to resize them to a smaller instance type, reducing your costs.
- Use the azure total cost calculator https://azure.microsoft.com/en-us/pricing/tco/ when starting out and moving the on premise to cloud.

Not sure if the team/org has disaster recovery plans in place. Would be best pratices to draft a business continuity and disaster recovery (BCDR) strategy by orchestrating the replication, fail-over, and recovery of workloads and applications if the primary location fails.

- Norbert Obiekwe - 2019