**Ansh Ranjan**

**Azure Data**

**EXERCISE 3 - Data Security and Compliance in Azure**

**1. Research and Document Azure's Data Encryption Methods**

* **What to do**:
* Research how Azure secures data through encryption. Include details on encryption at rest, encryption in transit, and customer-managed keys.
* Cover services like Azure Storage encryption, SQL Database encryption (TDE), and Azure Key Vault.
* Summarize your findings in **1 page** and save it as a **PDF document**.
* **How to do it**:
* Use Azure documentation (<https://learn.microsoft.com/en-us/azure/>) for research.
* Tools like Word or Google Docs can help you write and export your document as a PDF.

**2. Enable Encryption for a Sample Azure Storage Account**

* **What to do**:
* Create or use an existing Azure Storage Account.
* Enable encryption for the storage account (Azure encrypts all storage accounts at rest by default).
* Optionally, configure **customer-managed keys** for encryption using Azure Key Vault.
* **How to do it**:
* Log in to the Azure Portal ([https://portal.azure.com](https://portal.azure.com/)).
* Navigate to your storage account.
* Under **Settings**, go to **Encryption** and verify or enable encryption.
* If using customer-managed keys, integrate Azure Key Vault.

**3. Explore Azure Compliance Manager for Data Regulation**

* **What to do**:
* Use Azure Compliance Manager to explore how Azure helps meet regulatory requirements (e.g., GDPR, HIPAA).
* Review the compliance score and understand how to improve it.
* **How to do it**:
* Log in to the Azure Portal.
* Search for **Compliance Manager** in the portal.
* Explore the dashboard, review assessments, and understand the regulatory frameworks Azure supports.

