Activity 3: Data Governance Policy Development

Objective: To understand the process of developing data governance policies and procedures and to create a set of policies and procedures for a fictional organization.

Instructions:

1. Each group will be given a scenario of a fictional organization that needs to develop data governance policies and procedures. The scenario should include information about the organization, its data, and its goals for data governance.
2. The groups will need to work together to develop a set of data governance policies and procedures that align with the organization's goals and are compliant with relevant regulations and standards.
3. The policies and procedures should cover the following areas:
    - Data management
    - Data security and privacy
    - Metadata management
    - Data breaches
    - Data retention and disposal
4. Each group will present their policies and procedures to the class and explain the reasoning behind their decisions.
5. The class will discuss and provide feedback on the policies and procedures, highlighting any areas that may need improvement.
6. As a class, discuss the importance of communicating data governance policies and procedures to all stakeholders and the role of training and awareness programs in ensuring compliance.
7. Finally, each group will reflect on what they learned during the activity and how they can apply it to real-world scenarios.

Assessment:

- Participation and engagement during the group activity (20 points)
- Quality of the data governance policies and procedures developed by the group (30 points)
- Presentation of the policies and procedures to the class (20 points)
- Reflection and self-assessment of the learning experience (30 points)

Scenarios:

Scenario 1: "E-Commerce Inc."
E-Commerce Inc. is an online retailer that sells a variety of products, including clothing, electronics, and home goods. The company has experienced rapid growth over the past few years and now has thousands of employees and millions of customers. As the company continues to expand, it realizes the need to develop a comprehensive data governance policy to protect customer data and ensure compliance with regulations.

Scenario 2: "Healthcare Providers United"
Healthcare Providers United is a non-profit organization that represents a network of healthcare providers, including hospitals, clinics, and physician groups. The organization is responsible for managing patient data, including medical records, billing information, and personal information. With the increasing number of data breaches in the healthcare industry, Healthcare Providers United recognizes the importance of implementing a robust data governance policy to protect patient data and maintain public trust.

Scenario 3: "Financial Services Corp."

Financial Services Corp. is a financial institution that provides a range of services, including banking, investing, and insurance. The company handles large amounts of sensitive data, including financial information, personal identifiable information, and credit card data. As a result, it is subject to a variety of regulations, including the Gramm-Leach-Bliley Act (GLBA) and the Payment Card Industry Data Security Standard (PCI DSS). Financial Services Corp. needs to develop a data governance policy that ensures compliance with these regulations and protects customer data.

Scenario 4: "Educational Institution"

The Educational Institution is a large university with multiple campuses, offering a range of undergraduate and graduate programs. The university has a diverse student body and faculty, and it is committed to providing a safe and inclusive learning environment. The university has a strong focus on research and innovation, and it is home to a number of research centers and institutes. The university is subject to a number of data privacy regulations, including the Family Educational Rights and Privacy Act (FERPA), and it is struggling to ensure compliance with these regulations. The university needs to develop a data governance policy that ensures compliance with these regulations and protects customer data.