Cloud Security Assignment

When sharing user data with an organization through Cloud - AWS or Azure or GCP I would take the following aspect of the data sharing into consideration:

1. Resource Access Authorization
2. Protecting Data at Rest
3. Protect Data in Transit
4. Secure the Infrastructure
5. Test Security

Let's discuss each of the aspects below on the basis of AWS cloud features :

Resource Access Authorization:

We should plan which resource should be made available to the client and grant them IAM roles. Each such role should have operation specific policies(read/write/etc policies etc.)
IAM policies can be used to restrict access to a specific source- IP address range, or during specific days and times of the day, as well as based on other conditions.
Alternatively, we can grant users explicit access to manage permissions on a resource.

Protecting Data at Rest

For regulatory or business requirement reasons, we might want to further protect our data at rest stored in Amazon S3, or Amazon EBS, Amazon RDS, or other services from AWS.

If we are persisting data in RDS:
We could add protection at the application layer, for example, using a built-in encryption function that encrypts all sensitive database fields, using an application key, before storing them in the database. The application can manage keys by using symmetric encryption with PKI infrastructure or other asymmetric key techniques to provide for a master encryption key.

For example: We could add protection at the platform using MySQL cryptographic functions; which can take the form of a statement like the following: INSERT INTO Customers (CustomerFirstName,CustomerLastName) VALUES (AES_ENCRYPT('John',@key), AES_ENCRYPT('Smith',@key);

Platform level encryption can also be used for the RDS platform - for instance MySQL cryptographic functions include encryption, hashing, and compression.

Protect Data at Transit:

Cloud applications often communicate over public links, such as the Internet, so it is important to protect data in transit when we run applications in the cloud. This involves protecting network traffic between clients and servers, and network traffic between servers.
We should keep in mind the following rules:

1. Encrypt data in transit using IPSec ESP and/or SSL/TLS
2. Use IPSec with IKE with pre-shared keys or X.509 certificates to authenticate the remote end. Alternatively, use SSL/TLS with server certificate authentication based on the server common name (CN), or Alternative Name (AN/SAN).

We can alternatively use AWS APIs to manage services from AWS either directly from applications or third-party tools, or via SDKs, or via AWS command line tools. AWS APIs are web services (REST) over HTTPS. SSL/TLS sessions are established between the client and the specific AWS service endpoint, depending on the APIs used, and all subsequent traffic, including the REST envelope and user payload, is protected within the SSL/TLS session.

Secure the Infrastructure:

With Amazon Virtual Private Cloud (VPC) we can create private clouds within the AWS public cloud. Each customer Amazon VPC uses IP address space, allocated by customer. We can use private IP addresses (as recommended by RFC 1918) for Amazon VPCs, building private clouds and associated networks in the cloud that are not directly routable to the Internet. Amazon VPC provides not only isolation from other customers in the private cloud, it provides layer 3 (Network Layer IP routing) isolation from the Internet as well.

Test Security:

Verifying existing controls requires testing. As a consulting company we should undertake a number of test approaches:

- External Vulnerability Assessment: A third party evaluates system vulnerabilities with little or no knowledge of the infrastructure and its components;
- External Penetration Tests: A third party with little or no knowledge of the system actively tries to break into it, in a controlled fashion.
- Internal Gray/White-box Review of Applications and Platforms: A tester who has some or full knowledge of the system validates the efficiency of controls in place, or evaluates applications and platforms for known vulnerabilities.

Taking the above security concerns into consideration should be a must when sharing data with other organizations. Taking these steps in the beginning would help save the company millions to avoid any feud with the user’s data privacy.