**Identify a cloud-related risk that would fall into the "Relationship issues" section.**

* Digital asset downloading and destruction when the service is terminated
* Risk: Improper handling of data during the termination of a cloud service contract.

**What risk-event might occur? How would that negatively impact the client organization?**

Risk Events:

* Does not return data: The cloud provider fails to return the client's data.
* Returns data in an unsecure way: Data is returned in an unencrypted or otherwise insecure manner, leading to potential data leaks.
* Does not destroy data: The cloud provider fails to securely destroy data, leaving it vulnerable to theft or unauthorized access.
* Keeps data illegally: The cloud provider retains data without authorization, potentially using it inappropriately.

Negative Impact:

* Data Breach: Unauthorized access to sensitive information can lead to data breaches.
* Regulatory Penalties: Non-compliance with data protection regulations can result in significant fines and legal consequences.
* Operational Disruption: Loss or corruption of critical data can disrupt business operations.
* Financial Loss: Costs associated with managing data breaches, legal fees, and loss of business.

**Explain how a control for this risk would help.**

* Data Encryption: Ensures that even if data is kept or lost by the service, it remains inaccessible without the company's decryption methods. Protects data from unauthorized access during transfer and storage.
* Data Integrity Checks: Verifies that data is not missing or corrupted. If data is missing, it helps identify where it might be and facilitates retrieval. This ensures completeness and accuracy of data during transfer.
* Access Controls: Restricts which data is stored off-site and who can access it. This limits exposure of sensitive data and ensures only authorized personnel can access it.

**Would it reduce likelihood or impact? How?**

Yes, implementing these controls reduces both the likelihood and impact of data-related risks by ensuring data is encrypted and access is restricted. Data integrity checks and encryption ensure that even if data is lost or stolen, it remains inaccessible and useless to unauthorized parties.

**Explain what an auditor might do to gather evidence about the effectiveness of the control.**

To gather evidence about the effectiveness of controls, an auditor might review encryption policies, test the encryption process, and verify data integrity checks by examining logs and performing tests. They would also review access policies and observe implementations to ensure only authorized personnel have access to sensitive data stored off-site.

Explain the evidence on which the finding is based.

What criteria was used to determine that the control was deficient?

What did the auditors see?.

The auditor addresses provider IAM responsibilities and their potential impact on data from user account breaches. The evidence for this includes potential unauthorized access to the IAM environment through compromised credentials via phishing attacks, weak passwords, or unpatched software. The auditor saw a lack of evidence proving the existence and effectiveness of controls, such as comprehensive IAM policies, effective implementation of MFA and RBAC, and regular review of access logs. The criteria for determining the deficiency included the adequacy of IAM policies, the effectiveness of access controls, and the comprehensiveness of logging and monitoring.