PROJECT RISK MITIGATION

A sufficiently detailed risk management plan identifying privacy and regulatory concerns, as well as issues relating to data storage, protection and replication. Failure to ensure appropriate security protection when using cloud storage services could ultimately result in higher costs and potential loss of business, thus eliminating any of the potential benefits of cloud computing. When considering a transition to cloud storage, Great Benefits must have a clear understanding of potential risks associated with cloud computing, and set realistic expectations with their cloud provider. As Great Benefits transition their applications and data to the cloud, it is critical for them to maintain, or preferably surpass, the level of security they had in their traditional IT environment.

Determine the appropriate risk manager

The risk manager is responsible for identifying and implementing the risk mitigation plan. Cloud aggies consulting firm has identified Likita Shetty as the risk manager for Great Benefits cloud storage implementation. She has the required knowledge, authority, and resources to implement the plan. risk mitigation activities. It may be necessary to engage higher levels in the customer organization to ensure the need for the risk manager is addressed. This can be difficult and usually involves engaging more senior levels of Great Benefits as well.

Process For Mitigating Risks

Process 1: Ensure effective governance, risk and compliance processes

Security controls for cloud storage services are similar to those in traditional IT environments. However, the risks may be different because of:

- The division of responsibilities between the cloud storage service customer and the cloud service provider.

- The fact that technical design and operational control of the cloud service is in the hands of the cloud service provider

a)Compliance

One useful approach to the security challenges of cloud storage implementation is for a cloud provider to demonstrate that they are compliant with an established set of security controls. Certification of the provider gives prospective customers more confidence in that provider, and the ability to show “due diligence” in provider selection. Which certification is most appropriate depends to some extent on the category of the cloud service and on the customer’s regional and industry requirements.

b)Governance

From a general governance perspective, cloud storage administrators should notify risk manager and Great benefits management about the occurrence of any breach of their system, regardless of the parties or data directly impacted. Administrator should include specific pertinent information in the notification, stop the data breach as quickly as possible, restore secure access to the service as soon as possible, apply best-practice forensics in investigating the circumstances and causes of the breach, and make long-term changes to correct the root causes of the breach to ensure that it does not recur. Due to the high financial and reputation costs

Process 2: Audit operational & business processes

As a baseline, Great Benefits should expect to see a report of the cloud operations by independent auditors. The level of access to essential audit information is a key consideration of project contract and SLA terms with the cloud provider. As part of contract, cloud providers offers timely access to audit events, log and report information relevant to a customer's specific data or applications.

Key Subprocesses

1. Understanding the internal control environment of cloud services, including risks, controls and other governance issues when that environment touches the provision of cloud services.

2. Access to the corporate audit trail, including workflow and authorization, when the audit trail spans cloud services

3. Assurance of the facilities for management and control of cloud services and how such facilities are secured.

Key controls for cloud services risk mitigation include:

- Ensuring isolation of customer applications and customer data in shared, multi-tenant environments

- Providing protection of customer assets from unauthorized access by the provider's staff

a) Access to the corporate audit trail

It is vital have appropriate access to cloud provider events, logs and audit trails that prove enforcement of provider security controls. Auditors need to assure that all the necessary information is being logged and stored appropriately by the cloud service provider, including authentication, authorization and management information relating to the use of particular applications and data against all security and compliance policies established by the provider or customer.

b)Assurance of the facilities for management and control of cloud services

Cloud management services generally have self-service facilities to manage and monitor the usage cloud services usage and associated assets. These facilities may include: service catalogs, subscription services, payment processes, the provision of streams of operational event data and logs, usage metering data, facilities for configuring services including adding and removing user identities and the management of authorizations. These facilities are often more sensitive in security terms than the services and applications to which they apply, since the potential for abuse and damage may be higher. A security audit must extend to these facilities as well as to the main services of the provider

c)Auditing is essential

The security audit of cloud services is an essential aspect of risk mitigation, typically as part of a certification process. Audits should be carried out by appropriately skilled staff typically belonging to an independent auditing organization. Security audits should be carried out on the basis of one of the established standards for security controls.

Sets of controls must be in place to meet the security requirements. There is also a need to ensure proper integration of the cloud service reporting and logging facilities with the customer's systems, so that appropriate operational and business data flows on a timely basis to enable customers to manage their use of cloud services.

Process 3: Manage people, roles and identities

Use of a cloud storage solution means that there will be employees of the provider with the ability to access the customer’s data and applications, as well as employees of the customer who need to perform operations on the provider’s systems.

It must be ensured that there are processes and functionality that govern who has access to the customer's data and applications. Conversely, cloud providers must allow the customer to assign and manage the roles and associated levels of authorization for each of their users in accordance with their security policies. These roles and authorization rights are applied on a per resource, service or application basis. For example, a cloud application, in accordance with its security policies, may have an employee whose role allows generation of purchase requests, but a different role and authorization rights is granted to another employee responsible for approving the request.

A secure system for provisioning and managing unique identities for the users and services. This Identity and Access Management (IdAM) functionality must support simple resource access and robust customer application and service workflows.
Any user access to the provider's management platform, regardless of role or entitlement, should be monitored and logged to provide auditing of all access to user data and applications.

Identity Provisioning and Delegation	**Great Benefits need to administer their own users; the cloud provider should support delegated administration.**
Single Sign-On (SSO), Single Sign-Off	**Federate identity across applications to provide single-sign-on (SSO) along with single sign-off to assure user sessions get terminated properly. For example, an using separate SaaS applications**

	for Great Benefit’s CRM and ERP may require single-sign-on, sign-off, and authorization across these applications (using standards such as SAML 2.0 [11], WS-Federation [12] and OAuth [13]).
Identity and Access Audit	**Auditing and logging reports relating to service usage for assurance as well as compliance with regulations.**
Robust Authentication	**For access to high value assets hosted in the cloud, customers may require that their provider support strong, multi-factor, mutual and/or even biometric authentication.**
Role, Entitlement and Policy Management	**Cloud users need to be able to describe and enforce their security policies, user roles, groups and entitlements to their business and operational applications and assets, with due consideration for any industry, regional or corporate requirements.Need to have fine-grained access control so that users can have different roles that do not create conflicts or violate compliance guidelines**

Process 4: Ensure proper protection of data and information for managing Data Risks

Data is at the core of IT security concerns for any organization, whatever the form of infrastructure that is used. Cloud computing does not change this, but brings an added focus because of the distributed nature of the cloud computing infrastructure and the shared responsibilities that it involves. Security considerations apply both to data at rest (held on some form of storage system) and also to data in motion (being transferred over some form of communication link), both of which may need particular consideration when using cloud services

Controls for Securing Data while doing cloud storage implementation

Creating a data asset catalog	• Identify all data assets, classifying them in terms of criticality to the business , specifying ownership and responsibility for the data and describing the location and acceptable use of the assets. • Relationships between data assets also need to be cataloged.
Considering all forms of data	• Organizations are increasing the amount of unstructured data held in IT systems, which can include items such as images of scanned documents, pictures and multimedia files. • For structured data, in a multi-tenancy cloud environment, data held in databases needs consideration. Database segmentation can be offered in a couple of varieties: shared or isolated data schema. • Database encryption should be employed to protect all data at rest.