### Chapter -5

**Security in Cloud Computing**

### Cloud Computing Security

**Security** in cloud computing is a major concern. Data in cloud should be stored in encrypted form. To restrict client from accessing the shared data directly, proxy and brokerage services should be employed.

### Security Planning

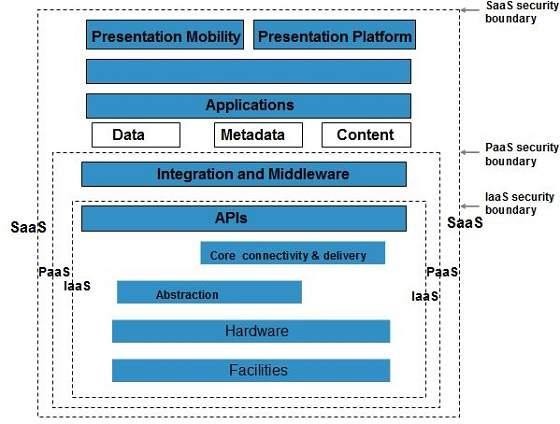
Before deploying a particular resource to cloud, one should need to analyze several aspects of the resource such as:

* Select resource that needs to move to the cloud and analyze its sensitivity to risk.
* Consider cloud service models such as IaaS, PaaS, and SaaS. These models require customer to be responsible for security at different levels of service.
* Consider the cloud type to be used such as public, private, community or hybrid.
* Understand the cloud service provider's system about data storage and its transfer into and out of the cloud.

The risk in cloud deployment mainly depends upon the service models and cloud types.

### Understanding Security of Cloud Security Boundaries

A particular service model defines the boundary between the responsibilities of service provider and customer. Cloud Security Alliance (CSA) stack model defines the boundaries between each service model and shows how different functional units relate to each other. The following diagram shows the CSA stack model:



### Key Points to CSA Model

* IaaS is the most basic level of service with PaaS and SaaS next two above levels of services.
* Moving upwards, each of the service inherits capabilities and security concerns of the model beneath.
* IaaS provides the infrastructure, PaaS provides platform development environment, and SaaS provides operating environment.
* IaaS has the least level of integrated functionalities and integrated security while SaaS has the most.
* This model describes the security boundaries at which cloud service provider's responsibilities end and the customer's responsibilities begin.
* Any security mechanism below the security boundary must be built into the system and should be maintained by the customer.

Although each service model has security mechanism, the security needs also depend upon where these services are located, in private, public, hybrid or community cloud.

### Understanding Data Security

Since all the data is transferred using Internet, data security is of major concern in the cloud. Here are key mechanisms for protecting data.

* Access Control
* Auditing
* Authentication
* Authorization

All of the service models should incorporate security mechanism operating in all above- mentioned areas.

### Isolated Access to Data

Since data stored in cloud can be accessed from anywhere, we must have a mechanism to isolate data and protect it from client’s direct access.

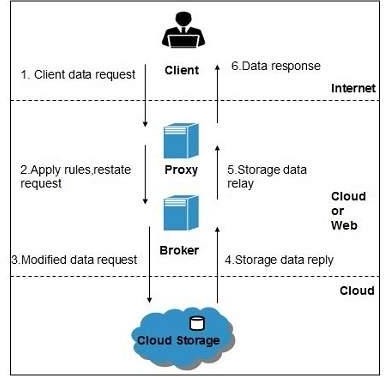
Brokered Cloud Storage Access is an approach for isolating storage in the cloud. In this approach, two services are created:

* A broker with full access to storage but no access to client.
* A proxy with no access to storage but access to both client and broker. Working Of Brokered Cloud Storage Access System

When the client issues request to access data:

* The client data request goes to the external service interface of proxy.
* The proxy forwards the request to the broker.
* The broker requests the data from cloud storage system.
* The cloud storage system returns the data to the broker.
* The broker returns the data to proxy.
* Finally the proxy sends the data to the client.

All of the above steps are shown in the following diagram:



Encryption

Encryption helps to protect data from being compromised. It protects data that is being transferred as well as data stored in the cloud. Although encryption helps to protect data from any unauthorized access, it does not prevent data loss.

Cloud Security Challenges

In our technology driven world, security in the cloud is an issue that should be discussed from the board level. These challenges are:

1. **DDoS attacks:** A DDoS attack is designed to overwhelm website servers so it can no longer respond to legitimate user requests. If a DDoS attack is successful, it renders a website useless for hours, or even days. This can result in a loss of revenue, customer trust and brand authority.
2. **Data breaches:** Traditionally, IT professionals have had great control over the network infrastructure and physical hardware (firewalls, etc.) securing proprietary data. In the cloud (in private, public and hybrid scenarios), some of those controls are relinquished to a trusted partner. Choosing the right vendor, with a strong record of security, is vital to overcoming this challenge.
3. **Data loss:** When business critical information is moved into the cloud, it’s understandable to be concerned with its security. Losing data from the cloud, either though accidental deletion, malicious tampering (i.e. DDoS) or an act of nature brings down a cloud service provider, could be disastrous for an enterprise business. Often a DDoS attack is only a diversion for a greater threat, such as an attempt to steal or delete data.
4. **Insecure access points:** A behavioral web application firewall examines HTTP requests to a website to ensure it is legitimate traffic. This always-on device helps protect web applications from security breaches.
5. **Notifications and alerts:** Awareness and proper communication of security threats is a cornerstone of network security and the same goes for cloud security. Alerting the appropriate website or application managers as soon as a threat is identified should be part of a thorough security plan. Speedy mitigation of a threat relies on clear and prompt communication so steps can be taken by the proper entities and impact of the threat minimized.

Cloud security challenges are not insurmountable. With the right partners, technology and forethought, enterprises can leverage the benefits of cloud technology.

### Software as a Service Security:

The seven security issues which one should discuss with a cloud-computing vendor:

1. **Privileged user access** —inquire about who has specialized access to data, and about the hiring and management of such administrators.
2. **Regulatory compliance**—make sure that the vendor is willing to undergo external audits and/or security certifications.
3. **Data location**—does the provider allow for any control over the location of data?
4. **Data segregation** —make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.
5. **Recovery** —Find out what will happen to data in the case of a disaster. Do they offer complete restoration? If so, how long would that take?
6. **Investigative support** —Does the vendor have the ability to investigate any inappropriate or illegal activity?
7. **Long-term viability** —What will happen to data if the company goes out of business? How will data be returned, and in what format?

To address the security issues listed above, SaaS providers will need to incorporate and enhance security practices used by the managed service providers and develop new ones as the cloud computing environment evolves. The baseline security practices for the SaaS environment as currently formulated are discussed in the following sections.

### Security Management (People):

One of the most important actions for a security team is to develop a formal charter for the security organization and program. This will foster a shared vision among the team of what security leadership is driving toward and expects, and will also foster “ownership” in the success of the collective team. The charter should be aligned with the strategic plan of the organization or company the security team works for. Lack of clearly defined roles and responsibilities, and agreement on expectations, can result in a general feeling of loss and confusion among the security team about what is expected of them, how their skills and experienced can be leveraged, and meeting their performance goals. Morale among the team and pride in the team is lowered, and security suffers as a result.

### Security Governance:

A security steering committee should be developed whose objective is to focus on providing guidance about security initiatives and alignment with business and IT strategies. A charter for the security team is typically one of the first deliverables from the steering committee. This charter must clearly define the roles and responsibilities of the security team and other groups involved in performing information security functions. Lack of a formalized strategy can lead to an unsustainable operating model and security level as it evolves. In addition, lack of attention to security governance can result in key needs of the business not being met, including but not limited to, risk management, security monitoring, application security, and sales support. Lack of proper governance and management of duties can also result in potential security risks being left unaddressed and opportunities to improve the business being missed because the security team is not focused on the key security functions and activities that are critical to the business.

### Risk Management:

Effective risk management entails identification of technology assets; identification of data and its links to business processes, applications, and data stores; and assignment of ownership and custodial responsibilities. Actions should also include maintaining a repository of information assets. Owners have authority and accountability for information assets including protection requirements, and custodians implement confidentiality, integrity, availability, and privacy

controls. A formal risk assessment process should be created that allocates security resources linked to business continuity.

### Risk Assessment:

Security risk assessment is critical to helping the information security organization make informed decisions when balancing the dueling priorities of business utility and protection of assets. Lack of attention to completing formalized risk assessments can contribute to an increase in information security audit findings, can jeopardize certification goals, and can lead to inefficient and ineffective selection of security controls that may not adequately mitigate information security risks to an acceptable level. A formal information security risk management process should proactively assess information security risks as well as plan and manage them on a periodic or as- needed basis. More detailed and technical security risk assessments in the form of threat modeling should also be applied to applications and infrastructure. Doing so can help the product management and engineering groups to be more proactive in designing and testing the security of applications and systems and to collaborate more closely with the internal security team. Threat modeling requires both IT and business process knowledge, as well as technical knowledge of how the applications or systems under review work.

### Security Monitoring and Incident Response:

Centralized security information management systems should be used to provide notification of security vulnerabilities and to monitor systems continuously through automated technologies to identify potential issues. They should be integrated with network and other systems monitoring processes (e.g., security information management, security event management, security information and event management, and security operations centers that use these systems for dedicated 24/7/365 monitoring). Management of periodic, independent third-party security testing should also be included. Many of the security threats and issues in SaaS center around application and data layers, so the types and sophistication of threats and attacks for a SaaS organization require a different approach to security monitoring than traditional infrastructure and perimeter monitoring. The organization may thus need to expand its security monitoring capabilities to include application- and data-level activities. This may also require subject-matter experts in applications security and the unique aspects of maintaining privacy in the cloud. Without this capability and expertise, a company may be unable to detect and prevent security threats and attacks to its customer data and service stability.

### Third-Party Risk Management:

As SaaS moves into cloud computing for the storage and processing of customer data, there is a higher expectation that the SaaS will effectively manage the security risks with third parties. Lack of a third-party risk management program may result in damage to the provider’s reputation, revenue losses, and legal actions should the provider be found not to have performed due diligence on its third-party vendors.

### Benefits of SaaS

Security-as-a-Service offers a number of benefits, including:

* Constant virus definition updates that are not reliant on user compliance.
* Greater security expertise than is typically available within an organization.
* Faster user provisioning.
* Outsourcing of administrative tasks, such as log management, to save time and money and allow an organization to devote more time to its core competencies.
* A Web interface that allows in-house administration of some tasks as well as a view of the security environment and on-going activities

### Security Architecture Design:

A security architecture framework should be established with consideration of processes (enterprise authentication and authorization, access control, confidentiality, integrity, non-repudiation, security management, etc.), operational procedures, technology specifications, people and organizational management, and security program compliance and reporting. A security architecture document should be developed that defines security and privacy principles to meet business objectives. Documentation is required for management controls and metrics specific to asset classification and control, physical security, system access controls, network and computer management, application development and maintenance, business continuity, and compliance. A design and implementation program should also be integrated with the formal system development life cycle to include a business case, requirements definition, design, and implementation plans. Technology and design methods should be included, as well as the security processes necessary to provide the following services across all technology layers:

* 1. Authentication
  2. Authorization
  3. Availability
  4. Confidentiality
  5. Integrity
  6. Accountability
  7. Privacy

The creation of a secure architecture provides the engineers, data center operations personnel, and network operations personnel a common blueprint to design, build, and test the security of the applications and systems. Design reviews of new changes can be better assessed against this architecture to assure that they conform to the principles described in the architecture, allowing for more consistent and effective design reviews.

### Vulnerability Assessment:

Vulnerability assessment classifies network assets to more efficiently prioritize vulnerability-mitigation programs, such as patching and system upgrading. It measures the effectiveness of risk mitigation by setting goals of reduced vulnerability exposure and faster mitigation. Vulnerability management should be integrated with discovery, patch management, and upgrade management processes to close vulnerabilities before they can be exploited.

### Data Privacy:

A risk assessment and gap analysis of controls and procedures must be conducted. Based on this data, formal privacy processes and initiatives must be defined, managed, and sustained. As with security, privacy controls and protection must an element of the secure architecture design. Depending on the size of the organization and the scale of operations, either an individual or a team should be assigned and given responsibility for maintaining privacy. A member of the security team who is responsible for privacy or a corporate security compliance team should collaborate with the company legal team to address data privacy issues and concerns. As with security, a privacy steering committee should also be created to help make decisions related to data privacy. Typically, the security compliance team, if one even exists, will not have formalized training on data privacy, which will limit the ability of the organization to address adequately the data privacy issues they currently face and will be continually challenged on in the future. The answer is to hire a consultant in this area, hire a privacy expert, or have one of your existing team members trained properly. This will ensure that your organization is prepared to meet the data privacy demands of its customers and regulators.

For example, customer contractual requirements/agreements for data privacy must be adhered to, accurate inventories of customer data, where it is stored, who can access it, and how it is used must be known, and, though often overlooked, Request for Interest/Request for Proposal questions regarding privacy must answered accurately. This requires special skills, training, and experience that do not typically exist within a security team. As companies move away from a service model under which they do not store customer data to one under which they do store customer data, the data privacy concerns of customers increase exponentially. This new service model pushes companies into the cloud computing space, where many companies do not have sufficient experience in dealing with customer privacy concerns, permanence of customer data throughout its globally distributed systems, cross-border data sharing, and compliance with regulatory or lawful intercept requirements.

### Data Security:

The ultimate challenge in cloud computing is data-level security, and sensitive data is the domain of the enterprise, not the cloud computing provider. Security will need to move to the data level so that enterprises can be sure their data is protected wherever it goes. For example, with data-level security, the enterprise can specify that this data is not allowed to go outside of the United States. It can also force encryption of certain types of data, and permit only specified users to access the data. It can provide compliance with the Payment Card Industry Data Security Standard (PCI DSS). True unified end-to-end security in the cloud will likely requires an ecosystem of partners.

### Application Security:

Application security is one of the critical success factors for a world-class SaaS company. This is where the security features and requirements are defined and application security test results are reviewed. Application security processes, secure coding guidelines, training, and testing scripts and tools are typically a collaborative effort between the security and the development teams. Although product engineering will likely focus on the application layer, the security design of the application itself, and the infrastructure layers interacting with the application, the security team should provide the security requirements for the product development engineers to implement. This should be a collaborative effort between the security and product development team. External penetration testers are used for application source code reviews, and attack and penetration tests provide an objective review of the security of the application as well as assurance to customers that attack and penetration tests are performed regularly. Fragmented and undefined collaboration on application security can result in lower-quality design, coding efforts, and testing results.

### Virtual Machine Security:

In the cloud environment, physical servers are consolidated to multiple virtual machine instances on virtualized servers. Not only can data center security teams replicate typical security controls for the data center at large to secure the virtual machines, they can also advise their customers on how to prepare these machines for migration to a cloud environment when appropriate.

Firewalls, intrusion detection and prevention, integrity monitoring, and log inspection can all be deployed as software on virtual machines to increase protection and maintain compliance integrity of servers and applications as virtual resources move from on-premises to public cloud environments. By deploying this traditional line of defense to the virtual machine itself, you can enable critical applications and data to be moved to the cloud securely. To facilitate the centralized management of a server firewall policy, the security software loaded onto a virtual machine should include a bidirectional stateful firewall that enables virtual machine isolation and location awareness, thereby enabling a tightened policy and the flexibility to move the virtual machine from on-premises to cloud resources. Integrity monitoring and log inspection software must be applied at the virtual machine level.

This approach to virtual machine security, which connects the machine back to the mother ship, has some advantages in that the security software can be put into a single software agent that provides for consistent control and management throughout the cloud while integrating seamlessly back into existing security infrastructure investments, providing economies of scale, deployment, and cost savings for both the service provider and the enterprise.

### Disaster recovery plan (DRP)

A disaster recovery plan (DRP) is a documented, structured approach with instructions for responding to unplanned incidents. This step-by-step plan consists of the precautions to minimize the effects of a disaster so the organization can continue to operate or quickly resume [mission-](http://searchitoperations.techtarget.com/definition/mission-critical-computing) [critical functions.](http://searchitoperations.techtarget.com/definition/mission-critical-computing) Typically, disaster recovery planning involves an analysis of [business](http://searchcio.techtarget.com/definition/business-process) [processes](http://searchcio.techtarget.com/definition/business-process) and continuity needs. Before generating a detailed plan, an organization often performs a business impact analysis ([BIA](http://searchstorage.techtarget.com/definition/business-impact-analysis)) and risk analysis ([RA](http://searchmidmarketsecurity.techtarget.com/definition/risk-analysis)), and it establishes the recovery time objective ([RTO](http://whatis.techtarget.com/definition/recovery-time-objective-RTO)) and recovery point objective ([RPO](http://whatis.techtarget.com/definition/recovery-point-objective-RPO)).

### Recovery strategies

A disaster recovery strategy should start at the business level and determine which applications are most important to running the organization. The RTO describes the target amount of time a business application can be down, typically measured in hours, minutes or seconds. The RPO describes the previous point in time when an application must be recovered. Recovery strategies define an organization's plans for responding to an incident, while disaster recovery plans describe how the organization should respond. In determining a recovery strategy, organizations should consider such issues as:

* + Budget
  + Resources -- people and physical facilities
  + Management's position on risks
  + Technology
  + Data
  + Suppliers

Management approval of recovery strategies is important. All strategies should align with the organization's goals. Once disaster recovery strategies have been developed and approved, they can be translated into disaster recovery plans.

### Disaster recovery planning steps

The disaster recovery plan process involves more than simply writing the document. In advance of the writing, a risk analysis and business impact analysis help determine where to focus resources in the disaster recovery planning process. The BIA identifies the impacts of disruptive events and is the starting point for identifying risk within the context of disaster recovery. It also generates the RTO and RPO. The RA identifies threats and [vulnerabilities](http://whatis.techtarget.com/definition/vulnerability) that could disrupt the operation of systems and processes highlighted in the BIA. The RA assesses the likelihood of a disruptive event and outlines its potential severity. A DR plan checklist includes the following steps, according to independent consultant and IT auditor.

* Establishing the scope of the activity;
* Gathering relevant network infrastructure documents;
* Identifying the most serious threats and vulnerabilities, and the most critical assets;
* Reviewing the history of unplanned incidents and outages, and how they were handled;
* Identifying the current DR strategies;
* Identifying the emergency response team;
* Having management review and approve the disaster recovery plan;
* Testing the plan;
* Updating the plan; and
* Implementing a DR plan audit.

Disaster recovery plans are living documents. Involving employees -- from management to entry-level -- helps to increase the value of the plan.

### Creating a disaster recovery plan

An organization can begin its DR plan with a summary of vital action steps and a list of important contacts, so the most essential information is quickly and easily accessible. The plan should define the roles and responsibilities of disaster recovery team members and outline the criteria to launch the plan into action. The plan then specifies, in detail, the incident response and recovery activities. Other important elements of a disaster recovery plan template include:

* + Statement of intent and DR policy statement;
  + Plan goals;
  + [Authentication](http://searchsecurity.techtarget.com/definition/authentication) tools, such as passwords;
  + Geographical risks and factors;
  + Tips for dealing with media;
  + Financial and legal information and action steps; and
  + Plan history.

### Scope and objectives of DR planning

A disaster recovery plan can range in scope from basic to comprehensive. Some DRPs can be upward of 100 pages long.

Disaster recovery budgets can vary greatly and fluctuate over time. Organizations can take advantage of free resources, such as online DR plan templates from SearchDisasterRecovery or the Federal Emergency Management Agency. Several organizations, such as the [Business](http://searchdisasterrecovery.techtarget.com/definition/Business-Continuity-Institute-BCI) [Continuity Institute](http://searchdisasterrecovery.techtarget.com/definition/Business-Continuity-Institute-BCI) and Disaster Recovery Institute International, also provide free information and online how-to articles.

A disaster recovery plan checklist of goals includes identifying critical IT systems and networks, prioritizing the RTO, and outlining the steps needed to restart, reconfigure and recover systems and networks. The plan should at least minimize any negative effect on business operations. Employees should know basic emergency steps in the event of an unforeseen incident.

Distance is an important, but often overlooked, element of the DR planning process. A disaster recovery site that is close to the primary data center may seem ideal -- in terms of cost, convenience, [bandwidth](http://searchenterprisewan.techtarget.com/definition/bandwidth) and testing -- but outages differ greatly in scope. A severe regional event can destroy the primary data center and its DR site if the two are located too close together.

### Specific types of disaster recovery plans

DR plans can be specifically tailored for a given environment.

* **Virtualized disaster recovery plan.** [Virtualization](http://searchservervirtualization.techtarget.com/definition/virtualization) provides opportunities to implement disaster recovery in a more efficient and simpler way. A virtualized environment can spin up new virtual machine ([VM](http://searchservervirtualization.techtarget.com/definition/virtual-machine)) instances within minutes and provide application recovery through [high availability.](http://searchdatacenter.techtarget.com/definition/high-availability) Testing can also be easier to achieve, but the plan must include the ability to validate that applications can be run in disaster recovery mode and returned to normal operations within the RPO and RTO.
* **Network disaster recovery plan.** Developing a plan for recovering a network gets more complicated as the complexity of the network increases. It is important to detail the step-by- step recovery procedure, test it properly and keep it updated. Data in this plan will be specific to the network, such as in its performance and networking staff.
* **Cloud disaster recovery plan.** Cloud-based disaster recovery can range from a file backup in the cloud to a complete [replication.](http://searchdisasterrecovery.techtarget.com/definition/data-replication) [Cloud DR](http://searchcloudstorage.techtarget.com/definition/cloud-disaster-recovery-cloud-DR) can be space-, time- and cost-efficient, but maintaining the disaster recovery plan requires proper management. The manager must know

the location of physical and [virtual servers.](http://searchnetworking.techtarget.com/definition/virtual-server) The plan must address security, which is a common issue in the cloud that can be alleviated through testing.

* **Data center disaster recovery plan.** This type of plan focuses exclusively on the data center facility and [infrastructure](http://searchdatacenter.techtarget.com/definition/infrastructure). An operational risk assessment is a key element in data center DR planning, and it analyzes key components such as building location, power systems and protection, security and office space. The plan must address a broad range of possible scenarios.

### Types of disasters

A disaster recovery plan protects an organization from both human-made and natural disasters. There is not one specific way to recover from all kinds of disasters, so a plan should tackle a range of possibilities. A natural disaster may seem unlikely, but if it can happen in the organization's location, the DR plan should address it. According to independent consultant Edward Haletky, potential disasters to plan for include:

* + Application failure
  + VM failure
  + Host failure
  + Rack failure
  + Communication failure
  + Data center disaster
  + Building disaster
  + Campus disaster
  + Citywide disaster
  + Regional disaster
  + National disaster
  + Multinational disaster

### Testing your disaster recovery plan

DR plans are substantiated through [testing,](http://searchwindevelopment.techtarget.com/definition/testing) which identifies deficiencies and provides opportunities to fix problems before a disaster occurs. Testing can offer proof that the plan is effective and hits

RPOs and RTOs. Since IT systems and technologies are constantly changing, DR testing also helps ensure a disaster recovery plan is up to date.

Reasons given for not testing DR plans include budget restrictions, resource constraints or a lack of management approval. Disaster recovery testing takes time, resources and planning. It can also be a risk if the test involves using live data.

DR testing can be simple to complex. In a plan review, a detailed discussion of the disaster recovery plan looks for missing elements and inconsistencies. In a tabletop test, participants walk through plan activities step by step to demonstrate whether disaster recovery team members know their duties in an emergency. A simulation test uses resources such as recovery sites and backup systems in what is essentially a full-scale test without an actual [failover](http://searchstorage.techtarget.com/definition/failover).

### Cloud disaster recovery (cloud DR)

Cloud disaster recovery (cloud DR) is a [backup](http://searchstorage.techtarget.com/definition/backup) and [restore](http://searchstorage.techtarget.com/definition/restore) strategy that involves storing and maintaining copies of electronic records in a [cloud computing](http://searchcloudcomputing.techtarget.com/definition/cloud-computing) environment as a security measure. The goal of cloud DR is to provide an organization with a way to recover data and/or implement [failover](http://searchstorage.techtarget.com/definition/failover) in the event of a man-made or natural catastrophe.

There are a number of benefits that make cloud disaster recovery appealing, including the variety of ways it can be implemented: in-house, partially in-house or purchased as a service. This flexibility allows smaller enterprises to implement robust [disaster recovery plans](http://searchenterprisewan.techtarget.com/definition/disaster-recovery-plan) that would otherwise have been impossible. Typically, cloud providers charge for storage on a [pay-per-use](http://searchcio.techtarget.com/definition/metered-services) [model](http://searchcio.techtarget.com/definition/metered-services), based on [capacity](http://searchstorage.techtarget.com/definition/storage-capacity-planning), bandwidth or [seat](http://searchexchange.techtarget.com/definition/seat). Because the provider is in charge of purchasing and maintaining its storage [infrastructure,](http://searchdatacenter.techtarget.com/definition/infrastructure) the customer doesn't have to spend money on additional hardware, network resources, data center space and the personnel required to support them.

In addition to cost, there are other important issues to consider before adopting cloud-based disaster recovery:

* Does the organization have the necessary [bandwidth](http://searchenterprisewan.techtarget.com/definition/bandwidth) and network resources to move data fast enough between the primary site and the cloud?
* Can the organization [encrypt data](http://searchstorage.techtarget.com/definition/storage-encryption) in flight as it leaves the data center?

### Failover, failback keys to cloud recovery

Effective cloud disaster recovery provides continuity for services and the ability to fail over to a second site if there is a hardware or software failure of IT systems. Workloads are then failed back to their original locations when the crisis is resolved. Failover and [failback](http://whatis.techtarget.com/definition/failback) can be automated. Organizations should run tests at regular intervals on isolated network segments that do not impact production data.

Organizations can choose to fail over data, entire applications or [virtual machine (VM)](http://searchservervirtualization.techtarget.com/definition/virtual-machine) images. When data is failed over, it is available from file services in the cloud. However, cloud recovery can take a long time if there is a great deal of data. Application-based data can be [replicated](http://searchsqlserver.techtarget.com/definition/replication) to another application running in the cloud. Or an entire VM image, including data, can be replicated to the cloud and powered up and accessed if there is an on-premises failover.

### Cloud service-level agreements

Service-level agreements ([SLAs](http://searchitchannel.techtarget.com/definition/service-level-agreement)) hold cloud providers accountable and establish recourses and penalties if providers don't live up to their promises about [cloud services.](http://searchcloudprovider.techtarget.com/definition/cloud-services)

LAs can call for the provider to reimburse customers with credits if there is a service outage or data cannot be recovered during a disaster. Customers can usually apply credits toward their cloud bill or a subscription to another service, but these credits seldom make up for the loss of business if cloud recovery is delayed. Customers should also study SLAs to help formulate an [exit](http://whatis.techtarget.com/definition/exit-strategy) [strategy](http://whatis.techtarget.com/definition/exit-strategy) for the service.

SLAs for cloud disaster recovery can include guarantees for [uptime,](http://searchcloudstorage.techtarget.com/definition/cloud-uptime) recovery time objectives ([RTOs](http://whatis.techtarget.com/definition/recovery-time-objective-RTO)) and [recovery point objectives](http://whatis.techtarget.com/definition/recovery-point-objective-RPO). For instance, an RTO can be from one hour up to 24 hours or even longer, depending on how important an application is to restore the business. The faster the guaranteed restore time, the more expensive the service costs.

### Cloud disaster recovery providers, vendors

Because the cloud removes the need to maintain a second site, DR is considered a prime use case for the cloud. Disaster recovery requires failing applications over to the cloud and failing back, so hundreds of vendors have sprung up to offer cloud DR services. The leading cloud [DR as a](http://whatis.techtarget.com/definition/disaster-recovery-as-a-service-DRaaS)

[service](http://whatis.techtarget.com/definition/disaster-recovery-as-a-service-DRaaS) vendors include Axcient, Bluelock, IBM Resiliency Services, iland, [Microsoft Azure Site](http://searchwindowsserver.techtarget.com/definition/Microsoft-Azure-Site-Recovery) [Recovery](http://searchwindowsserver.techtarget.com/definition/Microsoft-Azure-Site-Recovery) and SunGard Availability Services.

Traditional backup vendors, such as [Acronis,](http://searchdatabackup.techtarget.com/definition/Acronis) [Carbonite](http://searchdatabackup.techtarget.com/definition/Carbonite) (EVault), Datto and Unitrends, have expanded into DR services. [Amazon Web Services](http://whatis.techtarget.com/definition/Amazon-Web-Services-AWS) and [VMware vCloud Air](http://searchservervirtualization.techtarget.com/definition/VMware-vCloud-Air)Disaster Recovery have also expanded into cloud DR. Other vendors providing cloud DR products and services include Databarracks, Windstream, Zerto and Zetta.