Resiliency:

Resiliency is the ability of a server, network, storage system, or an entire data center, to recover quickly and continue operating even when there has been an equipment failure, power outage or other disruption.

Data center resiliency is often achieved through the use of redundant components, subsystems, systems or facilities. When one element fails or experiences a disruption, the redundant element takes over seamlessly and continues to support computing services to the user base. Ideally, users of a resilient system never know that a disruption has even occurred.

RESILIENCY MODELING AND ANALYSIS (RMA)

There are four phases of RMA

1) Pre-Work: Creates a diagram to capture resources, dependencies and component interactions. By identifying the dependencies in the system, we can detect the failure points. These failure points then can be secured more.
2) Discover: Identifies failures and resilience gaps
3) Rate: Perform Impact Analysis
4) Act: Produces work items to improve resilience

Cloud Provisioning:

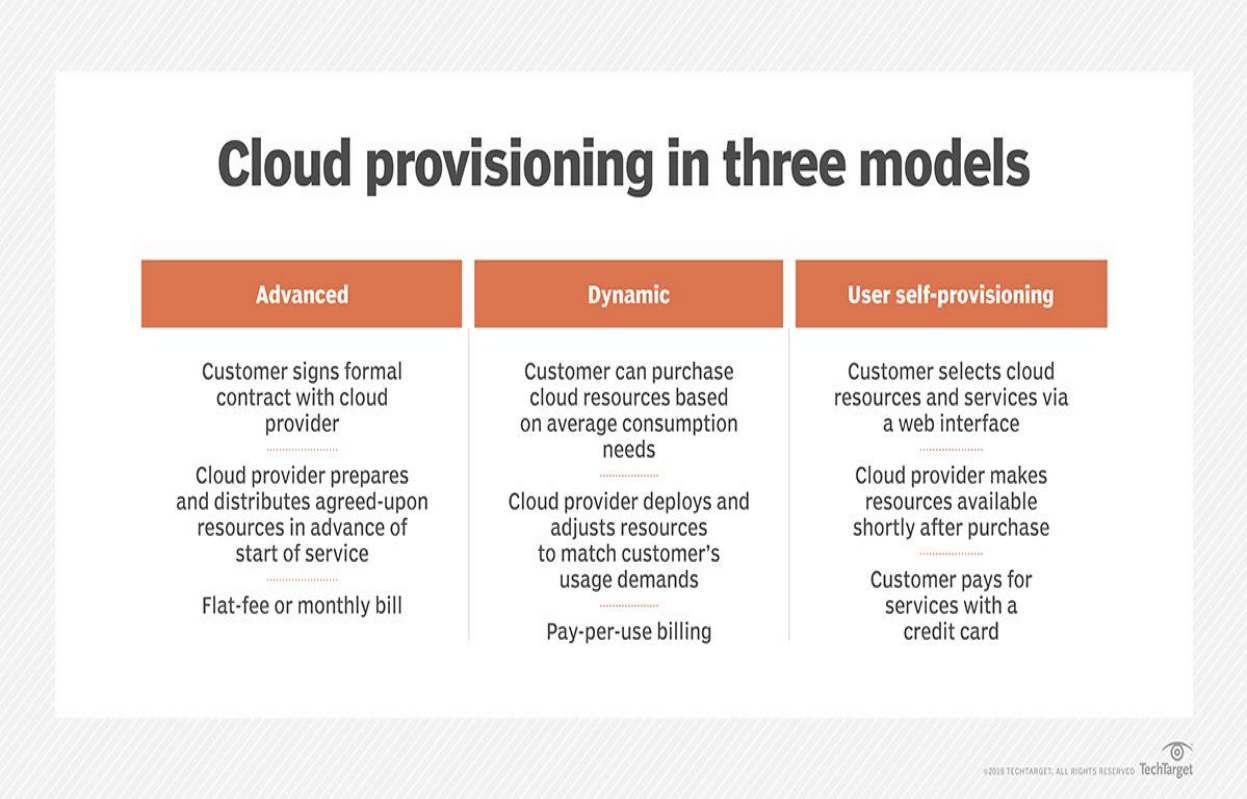
Cloud provisioning primarily defines how, what and when an organization will provision cloud services. These services can be internal, public or hybrid cloud products and solutions. There are three different delivery models:

Dynamic/On-Demand Provisioning: The customer or requesting application is provided with resources on run time.

User Provisioning: The user/customer adds a cloud device or device themselves.

Post-Sales/Advanced Provisioning: The customer is provided with the resource upon contract/service signup.

From a provider's standpoint, cloud provisioning can include the supply and assignment of required cloud resources to the customer. For example, the creation of virtual machines, the allocation of storage capacity and/or granting access to cloud software.



High Availability

High availability (HA) is the ability of a system or system component to be continuously operational for a desirably long length of time.

Availability can be measured relative to "100% operational" or "never failing." In information technology (IT), a widely-held but difficult-to-achieve standard of availability for a system or product is known as "**five 9s**" (99.999 percent) availability.

Availability experts emphasize that, for any system to be highly available, the parts of a system should be well-designed and thoroughly tested before they are used. Since a computer system or a network consists of many parts in which all parts usually need to be present in order for the whole to be operational, much planning for high availability centers around backup and failover processing and data storage and access.

How availability is measured

Typically, an availability percentage is calculated as follows:

*Availability = (minutes in a month - minutes of downtime) * 100/minutes in a month*

A service provider will typically provide availability metrics in their service level agreements (SLAs). Since system maintenance and planned downtime are a part of life, an HA system or system component is not expected to be available 100% of the time.

If the service level agreement for availability is 99.999%, the end user can expect the service to be unavailable for the following amounts of time:

Time Period	Time system is unavailable
Daily	0.9 seconds
Weekly	6.0 seconds
Monthly	26.3 seconds
Yearly	5 minutes and 15.6 seconds

To provide context, if a company adheres to the “three 9s” standard (99.9%), that means there will be about 8 hours and 45 minutes of system downtime during the course of one year. A "two 9s" standard for high availability is even more dramatic; 99% HA equals a little over three days of downtime in a year.

How to achieve high availability

A highly available system should be able to quickly recover from any sort of failure state to minimize interruptions for the end user. Best practices for achieving high availability include:

- Eliminate single points of failure, or any node that would impact the system as a whole if it becomes dysfunctional.
- Ensure that all systems and data are backed up for simple recovery.
- Use load balancing to distribute application and network traffic across servers or other hardware. A popular example of a load balancer is HAProxy.
- Continuously monitor the health of backend servers.
- Distribute resources geographically in case of power outages or natural disasters.
- Implement reliable crossover or failover In terms of storage, a redundant array of independent disks (RAID) or storage area network (SAN) are common approaches.
- Set up a system that detects failures as soon as they occur.
- Design system parts for high availability and test their functionality before implementation.

The role of backup and recovery in HA

Backups and failover processes are crucial components to accomplishing high availability. This can be attributed to the fact that some computer systems or networks consist of individual components, either hardware or software, that must be fully operational in order for the entire system to be available.

Backup components should be built into the infrastructure of the system. For example, if a server fails, an organization should be able to switch to a backup server. To obtain redundancy in a component, IT organizations should follow an N+1, N+2, 2N, 2N+1 strategy. These strategies ensure mission-critical software and hardware are given at least one component as a backup.

Ensuring there are data backups will help ensure high availability in the case of data loss, corruption or storage failures. A datacenter should be able to quickly recover from data loss for any reason to maintain high availability. An IT organization should enact automatic disaster recovery plans such as hosting data backups on redundant servers for data resilience.

Cloud based Disaster Recovery

Data is the most valuable asset of modern-day organizations. Its loss can result in irreversible damage to your business, including the loss of productivity, revenue, reputation, and even customers. It is hard to predict when a disaster will occur and how serious its impact will be. However, what you can control is the way you respond to a disaster and how successfully your organization will recover from it.

Backup and Disaster Recovery in Cloud Computing

Cloud computing is the on-demand delivery of computing services over the internet (more often referred to as 'the cloud') which operates on a pay-as-you-go basis. Cloud computing vendors generally provide access to the following services:

- Infrastructure as a service (IaaS) allows you to rent IT infrastructure, including servers, storages and network component, from the cloud vendor.
- Platform as a service (PaaS) allows you to rent a computing platform from the cloud provider for developing, testing, and configuring software applications.
- Software as a service (SaaS) allows you to access software applications which are hosted on the cloud.

As you can see, each cloud computing service is designed to help you achieve different business needs. More so, cloud computing can considerably improve data the security and high availability of your virtualized workloads. Let's discuss how you can approach disaster recovery in the cloud computing environment.

Cloud disaster recovery vs. traditional disaster recovery

Cloud disaster recovery is a cloud computing service which allows for storing and recovering system data on a remote cloud-based platform. To better understand what disaster recovery in cloud computing entails, let's compare it to traditional disaster recovery.

The essential element of traditional disaster recovery is a secondary data center, which can store all redundant copies of critical data, and to which you can fail over production workloads. A traditional on-premises DR site generally includes the following:

- A dedicated facility for housing the IT infrastructure, including maintenance employees and computing equipment.
- Sufficient server capacity to ensure a high level of operational performance and allow the data center to scale up or scale out depending on your business needs.
- Internet connectivity with sufficient bandwidth to enable remote access to the secondary data center.
- Network infrastructure, including firewalls, routers, and switches, to ensure a reliable connection between the primary and secondary data centers, as well as provide data availability.

However, traditional disaster recovery can often be too complex to manage and monitor. Moreover, support and maintenance of a physical DR site can be extremely expensive and time-consuming. When working with an on-premises data center, you can expand your server capacity only by purchasing additional computing equipment, which can require a lot of money, time, and effort.

Disaster recovery in cloud computing can effectively deal with most issues of traditional disaster recovery. The benefits include the following:

- You don't need to build a secondary physical site, and buy additional hardware and software to support critical operations. With disaster recovery in cloud computing, you get access to cloud storage, which can be used as a secondary DR site.
- Depending on your current business demands, you can easily scale up or down by adding required cloud computing resources.

- With its affordable pay-as-you go pricing model, you are required to pay only for the cloud computing services you actually use.
- Disaster recovery in cloud computing can be performed in a matter of minutes from anywhere. The only thing you need is a device that is connected to the internet.
- You can store your backed up data across multiple geographical locations, thus eliminating a single point of failure. You can always have a backup copy, even if one of the cloud data centers fails.
- State-of-the-art network infrastructure ensures that any issues or errors can be quickly identified and taken care of by a cloud provider. Moreover, the cloud provider ensures 24/7 support and maintenance of your cloud storage, including hardware and software upgrades.

Why Choose Disaster Recovery in Cloud Computing

The primary goal of disaster recovery is to minimize the overall impact of a disaster on business performance. Disaster recovery in cloud computing can do just that. In case of disaster, critical workloads can be failed over to a DR site in order to resume business operations. As soon as your production data center gets restored, you can fail back from the cloud and restore your infrastructure and its components to their original state. As a result, business downtime is reduced and service disruption is minimized.

Due to its cost-efficiency, scalability, and reliability, disaster recovery in cloud computing has become the most lucrative option for small and medium-sized businesses (SMBs). Generally, SMBs don’t have a sufficient budget or resources to build and maintain their own DR site. Cloud providers offer you access to cloud storage, which can become a cost-effective and long-lasting solution to data protection as well as disaster recovery.

How to Design a Cloud-Based Disaster Recovery Plan

After considering the benefits of cloud computing in disaster recovery, it is time to design a comprehensive DR plan. In fact, you can read one of our blog posts which walks you through the entire process of a creating a DR plan. Below, we are going to discuss how to create a DR plan which works in the cloud environment.

As a rule, an effective cloud-based DR plan should include the following steps:

1. Perform a risk assessment and business impact analysis.
2. Choose prevention, preparedness, response, and recovery measures.
3. Test and update your cloud-based DR plan.

Perform a risk assessment and business impact analysis

The first step in a disaster recovery planning in cloud computing is to assess your current IT infrastructure, as well as identify potential threats and risk factors that your organization is most exposed to.

A risk assessment helps you discover vulnerabilities of your IT infrastructure and identify which business functions and components are most critical. At the same time, a business impact analysis allows you to estimate how unexpected service disruption might affect your business.

Based on these estimations, you can also calculate the financial and non-financial costs associated with a DR event, particularly Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

The RTO is the maximum amount of time that IT infrastructure can be down before any serious damage is done to your business.

The RPO is the maximum amount of data which can be lost as a result of service disruption.

Understanding the RTO and RPO can help you decide which data and applications to protect, how many resources to invest in achieving DR objectives, and which DR strategies to implement in your cloud-based DR plan.

Implement prevention, preparedness, response, and recovery measures

The next step is to decide which prevention, preparedness, response, and recovery (PPRR) measures should be implemented in disaster recovery of the cloud computing environment. In a nutshell, PPRR measures can accomplish the following:

- **Prevention** allows you to reduce possible threats and eliminate system vulnerabilities in order to prevent a disaster from occurring in the first place.

- **Preparedness** entails creating the outline of a DR plan which states what to do during an actual DR event. Remember to document every step of the process to ensure that the DR plan is properly executed during a disaster.
- **Response** describes which DR strategies should be implemented when a disaster strikes in order to address an incident and mitigate its impact.
- **Recovery** determines what should be done to successfully recover your infrastructure in case of a disaster and how to minimize the damage.

After you have determined which approach to disaster recovery to implement, you should choose a data protection solution capable of putting your DR plan into action and achieving DR objectives. Choose the solution which meets your business needs and complies with your infrastructure requirements. For this purpose, consider the following criteria:

- Available services
- Hardware capacity
- Bandwidth
- Data security
- Ease of use
- Service scalability
- Cost
- Reputation

Test and update your cloud-based DR plan

After you have created and documented the DR plan, you should run regular tests to see if your plan actually works. You can test whether business-critical data and applications can be recovered within the expected time frame.

Testing a cloud-based DR plan can help you identify any issues and inconsistencies in your current approach to disaster recovery in cloud computing. After the test run, you can decide what your DR plan lacks and how it should be updated in order to achieve the required results and eliminate existing issues.

Disaster Recovery Checklist

Every time a disaster strikes, it can cause serious damage to your organization if appropriate actions are not immediately implemented. A responsible business owner understands that disaster recovery planning is a complex process that should be approached in a responsible manner. Thus, you should use a disaster recovery checklist which outlines the steps you need to take in order to successfully deal with the crisis.

The ultimate disaster recovery plan checklist should include the following:

1. Conduct risk assessment and business impact analysis
2. Determine recovery objectives
3. Assign roles and responsibilities within a DR team
4. Create a DR site
5. Prepare for failback
6. Store critical documents in a remote location
7. Establish equipment needs
8. Enable communication channels
9. Detail disaster response procedures
10. Report the incident to stakeholders
11. Test and update a DR plan
12. Decide on the right DR strategy

High availability versus disaster recovery

The terms high availability and disaster recovery are often used interchangeably. However, they are two distinct concepts:

- High availability (HA) describes the ability of an application to withstand all planned and unplanned outages (a planned outage could be performing a system upgrade) and to provide continuous processing for business-critical applications.

- Disaster recovery (DR) involves a set of policies, tools, and procedures for returning a system, an application, or an entire data center to full operation after a catastrophic interruption. It includes procedures for copying and storing an installed system's essential data in a secure location, and for recovering that data to restore normalcy of operation.

High availability is about avoiding single points of failure and ensuring that the application will continue to process requests. Disaster recovery is about policies and procedures for restoring a system or application to its normal operating condition after the system or application suffered a catastrophic failure or loss of availability of the entire data center.

Cloud governance

When you run a business in the cloud, there are a few rules you have to comply with. Generally, these rules relate to personal privacy and data security, and they can vary according to the industry you operate in. Typically the rules are no different from those you have to comply with when you run a business on on-premises IT infrastructure. It’s only the landscape that is different.

The different landscape is the reason you need to know what cloud governance is. This is because, when you run a business on an on-premises IT infrastructure, you know what your capital costs are and have a fairly good idea about your month-to-month operational costs. You also know departments will be running the software, applications, and programs that have been approved for them.

In the cloud, different departments can develop their own systems and deploy assets with the click of a mouse. You may no longer have to worry about capital costs, but your operational costs can get quickly out of hand without controls in place. Furthermore, the software, applications, and programs deployed by one department may not be able to communicate with those deployed by another department.

A lack of controls not only creates issues with costs and efficiency, but can also raise security concerns. Whereas cloud services themselves are secure, assets that are deployed with poor access controls or configuration vulnerabilities are an

invitation to a hacker to infiltrate your network. Previously—with an on-premises IT infrastructure—your business network was protected from many security concerns by a firewall. There are no firewalls in the cloud. This is why you need cloud governance.

Cloud governance is basically a set of rules

To eliminate issues with costs and efficiency, you need to create a set of rules. These rules of cloud governance should consist of budgets for how much departments can spend, guidelines about what software, applications and programs departments can use, and policies for cloud security. Naturally the rules can be flexible, but there needs to be an approval process in place to prevent too much flexibility.

Then compliance with the rules needs to be monitored. This can be achieved via many different types of cloud management software; although, if you operate in a multi-cloud or hybrid cloud environment (or plan to), it is better to use a third party cloud management solution—rather than software supplied by cloud service providers—in order to give you total visibility of all your business's cloud activity.

As you monitor compliance with the rules, you may notice areas that could be tweaked to improve cost-efficiency or performance. It may also be the case that, as you expand your cloud-based operations, you need to make changes to the rules you have created in order to accommodate new products and services, or to remain competitive within your industry. Processes need to be in place for this too.

Cloud governance is a set of rules you create, monitor, and amend as necessary in order to control costs, improve efficiency, and eliminate security risks. There may be other areas of your cloud operations that require governance, but these will become apparent when you first start pulling together the components that will eventually form your rules of governance.

Before you start creating rules of governance

Before you start creating rules of governance, you need to know what assets are already deployed in the cloud, how they work together, and what security risks exist. The best way of doing this is to use a **cloud management solution** that gives you total visibility over your cloud account(s) in order to compile an inventory of your assets, analyze their relationships, and identify security vulnerabilities.

You should then optimize your assets for costs and performance to get a starting point for future capacity planning and budgeting. This may involve exchanging one provider´s services for another provider´s service in order to take advantage of discounted pricing structures or more suitable services, but is something you should be able to manage easily with a suitable cloud management solution.

Once your assets are optimized, and you are armed with reports evaluating costs and performance by department, you can then collaborate with different departments in your business to create the rules of governance. As mentioned above, in addition to creating the rules, you have to have processes in place to accommodate flexibility and revisions, and policies in place to govern the security of your network.

Security policies are without doubt the most important element of cloud governance. Without effective policies in place—and effective monitoring of the policies—it is just a question of when, not if, your network will be infiltrated. Security policies not only need to be applied to assets deployed in the cloud, but also to areas such as access control, security groups, and encryption key management.

What is cloud governance automation software?

Cloud governance automation software is a useful element of some third party cloud management solutions that executes predetermined actions when a governance rule is violated.

Whereas some cloud governance solutions can help you audit and optimize your assets, and monitor compliance with the governance rules you apply, cloud governance automation software can be configured to notify you of a violation, request approval for an event beyond the parameters of your governance rules, or automatically terminate an asset. Here are some examples of how it works:

- Let’s say you have allocated a monthly budget to a department. You can create a policy to notify you (and/or the budget owner) when monthly costs to date are projected to exceed the budget so the overspend can be investigated.
- Or, you have stipulated the development team cannot launch non-production Virtual Machines with more than 4 cores without approval. As soon as an 8 core VM is launched, it is suspended until you approve the deployment.

- Or, if during the monitoring process of an AWS account, the software identifies an account with root account API access, the software can be configured to execute a Lambda function to revoke user access and notify you of the violation.

Effectively, cloud governance automation software removes much of the work involved in cloud governance, helps you create a more cost-effective and efficient environment, and alerts you to potential security issues before they develop into serious concerns. It is certainly worth investigating regardless of what size of operation you run in the cloud.