Disaster Recovery as a Service
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>3</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>3</td>
</tr>
<tr>
<td>Traditional disaster recovery—a choice between cost and speed</td>
<td>4</td>
</tr>
<tr>
<td>Disaster Recovery as a Service (DRaaS)</td>
<td>5</td>
</tr>
<tr>
<td>Best Practices in DRaaS</td>
<td>8</td>
</tr>
<tr>
<td>Challenges with DRaaS</td>
<td>9</td>
</tr>
<tr>
<td>DRaaS providers</td>
<td>10</td>
</tr>
<tr>
<td>Deloitte and disaster recovery</td>
<td>13</td>
</tr>
<tr>
<td>Observations</td>
<td>13</td>
</tr>
<tr>
<td>Key takeaways</td>
<td>13</td>
</tr>
<tr>
<td>References</td>
<td>14</td>
</tr>
<tr>
<td>Future with DRaaS</td>
<td>14</td>
</tr>
</tbody>
</table>
Abstract
Disaster Recovery (DR) is a solution that offers business continuity across a range of organizations and their applications by ensuring availability of IT infrastructure in case of any disaster resulting in disruption of Business Services. Historically, disaster recovery (DR) preparedness required substantial time and financial investment. For many, DR was out of reach, and for others, it was a burdensome task that often felt like an expensive insurance policy. Also as IT environments become more complex with greater mixes of operating systems, virtual platforms, applications, and storage growth as a result cascading impacts on DR are exponential. DR is still an all-or-nothing investment, and there were few options for moderately priced solutions that offered recovery times ranging from a few hours to a day.

Today, cloud-based DR is poised to shake up the legacy approaches and offer frustrated infrastructure and operations (I&O) professionals a great alternative. This paper will explore the use cases for DR in the cloud, the different models and providers today, and the benefits and risks of this approach and how should we pursue it.

Disaster Recovery
To understand what a Disaster means in very simple terms, we can look at a situation where a person performing an important online financial transaction suddenly experiences disruption in the banking services due to an IT downtime thereby resulting in failure of the transaction. In this situation the bank deems the failure of its online services as a disaster and recovering the online operations of the bank would constitute as Disaster Recovery which not only helps the bank maintain business continuity but also enables the customer/end user to have seamless usage of the services.

Over the past 20 to 30 years, businesses of all sizes have steadily grown more dependent on their expanding IT infrastructures to help them automate, manage, and analyze their business operations and strategy. Whether it’s online trading, insurance-document imaging, airline reservations, financial databases, Web sites, or other computing systems, the fortunes of business are inextricably linked to the continuous availability of these services and data.

<table>
<thead>
<tr>
<th></th>
<th>Normalized expected response</th>
<th>DRaaS users</th>
<th>In-House infrastructure users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average length of DR Events</td>
<td>2.3 hours</td>
<td>1.0 hours</td>
<td>2.6 hours</td>
</tr>
<tr>
<td>Average cost per hour of downtime</td>
<td>$138,000</td>
<td>$138,000</td>
<td>$138,000</td>
</tr>
<tr>
<td>Yearly average cost of downtime</td>
<td>$793,500</td>
<td>$207,000</td>
<td>$1,004,640</td>
</tr>
</tbody>
</table>

Unfortunately, IT infrastructures face varying risks of interruption. Most executives focus on natural disasters such as hurricanes, tornados, floods etc. But IT leaders recognize that a disaster can be any event that prevents a business from accessing the data and systems it needs to operate. That could encompass everything from regional power outages, to virus outbreaks, to employee sabotage, to external data fraud, to devastating terrorist attacks.
A recent study commissioned by CA Technologies and conducted in May 2010 by research firm Coleman Parkes shows that 95 percent of organizations experienced data loss in the last 12 months ending May 2011, with 74 percent pointing to IT systems failure as the biggest cause, while 42 percent pointed to external attacks and 37 percent to IT and human error.

The study polled 1,086 respondents from both small and midsize businesses (SMBs) and large organizations across eight countries in Asia: Singapore, Australia, China, India, Malaysia, South Korea, Thailand and Taiwan. The enterprises were from four vertical sectors: finance, public sector, retail and manufacturing.

It’s human nature to look at these risks and assign a very low probability to their occurrence in your business. But that simply isn’t the case: virtually every company faces the risk of IT interruptions that can grind business to a halt. A KPMG study (Fig. 2) conducted in the millennium showed the shifting nature of these interruptions with natural disasters comprising a shrinking portion of the total causes of IT interruptions and manmade disasters — human- and IT-related failures — representing an increasing share.

A traditional disaster recovery—a choice between cost and speed

DR success consideration depends on level of service required which could be measured by two key factors namely.

Recovery Time Objective (RTO): It is the measure of how quickly you need to have the application’s information back available after the downtime has occurred.

Recovery Point Objective (RPO): It describes the point in time to which data must be restored to successfully resume processing (often thought of as time between the last backup and when an event occurred).
RTO & RPO Objectives should be set for each application based on:

- The expected loss to the business with the objective
- The cost of achieving the objective

Gartner also reported that companies were deploying Raas in two ways. One of these uses server virtualization recovery features and SAN-based replication to deploy in-house disaster recovery capabilities for some applications, while the other involves the implementation of initial pilots for the use of cloud services as an alternative to more traditional disaster recovery resources.

Disaster Recovery as a Service (DRaaS)

Study indicates that virtualized cloud platforms are well suited to providing DR. Under normal operating conditions, a cloud-based DR Service may only need a small share of resources to synchronize state from the primary site to the cloud. But the full amount of resources required to run the application only needs to be provisioned (and paid for) if a disaster actually happens. The use of automated virtualization platforms for disaster recovery means that additional resources can be rapidly brought online once the disaster is detected.

It is observed that current DR Services come either at very high cost or with weak guarantees about the amount of data lost and time required restarting operation after a failure. However, with cloud computing and virtualization opening up a plethora of opportunities, business enterprises are discovering that a lot of applications can be availed as services, DR being no exception.

This has resulted in the emerging model of delivering Disaster Recovery as a Service (DRaaS) or DR as a cloud service or DR on demand. We have observed that DRaaS as a model is gaining popularity among enterprises mainly due to its pay-as-you-go pricing model that can lower costs, and use of automated virtual platforms that can minimize the recovery time after a failure.
Benefits offered by DRaaS over traditional disaster recovery models

- Multi-tenant portal enables the management of customer services through a single portal
- Seamlessly delivers a virtual machine for every physical or virtual server in your customers’ environment
- Delivers true application-consistent data availability across both virtual and physical machines
- Works with any and all applications to provide near low RPO and RTO
- Automatic alerting on replication and recovery status
- The backup data is kept in a geographically separate location
- The cost and difficulty of working with “recovered” data is eliminated
- Low overhead in deployment and use makes it a great fit for virtual machine environments that are a key supporting technology in cloud-based computing
- Flexible licensing model allows for a Pay as You Go

Normal operations without DRaaS

Using DRaaS
**DRaaS blueprint and architecture models**

Our research shows that there isn’t a single blueprint for DRaaS. Every organization is unique in the applications it runs, and the relevance of the applications to its business and the industry it is in. Therefore, DRaaS blueprint will be very distinct and unique for each organization.

Triage is the overarching principle used to create cloud-based DRaaS plans. The process of devising a DRaaS plan starts with identifying and prioritizing applications, services and data, and determining for each one the amount of downtime that’s acceptable before there’s a significant business impact. Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) will then determine the approach. Identifying critical resources and recovery methods is the most relevant aspect during this process, since an organization needs to ensure that all critical applications and data are included in the blueprint.

**DRaaS Models**

When a disaster strikes, it is clear that there are serious repercussions to the business. In addition, there could be temporary or even permanent loss of critical data. Offline, comprehensive and regular data back-ups are usually the first step in an IT continuity plan, but in today’s 24x7 business world, protecting against data loss is not good enough.

We believe that in addition to data loss, disasters may also lead to the permanent loss of physical infrastructure including IT infrastructure. This loss may result in the inability to fulfill existing or new orders. In most cases the loss of key IT applications or services can have as negative an impact on the business as the loss of data. In fact, according to the National Archives & Records Administration in Washington, 93 percent of companies that lost their data center for 10 days or more due to a disaster, filed for bankruptcy within one year of the disaster. To be fully protected, organizations must not only have a plan to quickly restore their data but also the underlying server capacity and the business services those servers support.

**Managed applications and managed DR**

An increasingly popular option is to put both primary production and disaster recovery instances into the cloud and have both handled by a managed service provider. By doing this enterprises can get all the benefits of cloud computing – from usage-based cost to eliminating on-premises infrastructure.

However, the choice of service provider and the process of negotiating appropriate service level agreements (SLAs) are of utmost importance. By handing over control to the service provider, we, as an enterprise need to ensure whether the service provider is able to deliver uninterrupted service within the defined SLAs for both primary and DR instances.

**Back up to and restore from the cloud**

It is observed that applications and data remain on-premises in this approach, with data being backed up into the cloud and restored onto on-premises hardware when a disaster occurs. In other words, the backup in the cloud becomes a substitute for tape-based off-site backups.

**Back up to and restore to the cloud**

In this approach, data is not restored back to on-premises infrastructure; instead it is restored to virtual machines in the cloud. This requires both cloud storage and cloud compute resources. The restore can be done when a disaster is declared or on a continuous basis (pre-staged). Pre-staging DR VMs and keeping them relatively up-to-date through scheduled restores is crucial in cases where aggressive RTOs need to be met.

**Replication to virtual machines in the cloud**

For applications that require aggressive recovery time (RTO) and recovery point objectives (RPOs), as well as application awareness, replication is the data movement option of choice. Replication to cloud virtual machines can be used to protect both cloud and on-premises production instances.

In other words, replication is suitable for both cloud-VM-to-cloud-VM and on-premises-to-cloud-VM data protection.
Before selecting a vendor to provide DRaaS, we should look out for the following on an organization:

- Lead time to allocate the minimum required resources, should DRaaS be invoked
- Lead time to scale up resources to the defined (or full) level
- Duration for which such resources will be retained on a dedicated basis for the company
- Additional fees for occupancy beyond the pre-defined period
- Additional facilities such as conference rooms and video conferencing
- Capability to provide additional hardware as and when needed
- Parameters related to work area recovery can also be included if such services are used
- Tiered service levels
- Global reach and local presence
- Support for mixed and virtualized server environments

<table>
<thead>
<tr>
<th>Managed primary and DR instances</th>
<th>Cloud based backup and restore</th>
<th>Replication in the cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instances</td>
<td>Email in the cloud</td>
<td>On premises into the cloud</td>
</tr>
<tr>
<td></td>
<td>• On premises into the cloud</td>
<td>Cloud to cloud</td>
</tr>
<tr>
<td>Merits</td>
<td>• Fully managed DR</td>
<td>Best recovery time objectives (RTOs) and recovery point objectives (RPOs)</td>
</tr>
<tr>
<td></td>
<td>• 100% usage based</td>
<td>• More likely to support application — consistent recovery</td>
</tr>
<tr>
<td></td>
<td>• Least complex</td>
<td></td>
</tr>
<tr>
<td>Caution</td>
<td>Service level agreements define access to production and DR instances</td>
<td>Less favorable RTOs and RPOs than replication</td>
</tr>
<tr>
<td>Implemented via...</td>
<td>N/A</td>
<td>Backup applications and appliances</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Key Considerations while selecting a Service for DR**

Before selecting a vendor to provide DRaaS, we should look out for the following on an organization:

- Lead time to allocate the minimum required resources, should DRaaS be invoked
- Lead time to scale up resources to the defined (or full) level
- Duration for which such resources will be retained on a dedicated basis for the company
- Additional fees for occupancy beyond the pre-defined period
- Additional facilities such as conference rooms and video conferencing
- Capability to provide additional hardware as and when needed
- Parameters related to work area recovery can also be included if such services are used
- Tiered service levels
- Global reach and local presence
- Support for mixed and virtualized server environments

**Best Practices in DRaaS**

**Start with the priority applications**

Not every application in the organization’s portfolio will be an ideal fit for DRaaS. We should start with applications that have a strong track record of performance in your virtual environment but aren’t supporting most critical systems. Starting with systems that are business critical rather than mission critical gives us the leeway to try different approaches and vendors. Once we are comfortable and have proven its effectiveness with testing, we can then move on to more critical applications.

**Understand SLAs and be realistic**

A standard best practice for DRaaS is found to first understand the service-level agreements of our solution so that we don’t receive any unwelcome surprises when it comes to service levels. With that said, often DRaaS providers are generally not flexible when it comes to SLAs, especially when we’re not offering to utilize those VMs outside of a disaster and testing. Similarly, many DRaaS providers will not guarantee RTOs and RPOs but promise to make best efforts to meet them. Only few will be willing to take financial responsibility if we are unable to recover.

**Right size the recovery resources**

To really take advantage of the cloud economic model, we must scrutinize the amount of resources needed during recovery and try to keep this minimal, take advantage of elastic scaling only if needed. For example, a large database may not need to come back with full capacity at the recovery site; during a disaster, most business units can afford to — and are prepared to — operate at reduced speed or capacity.
Challenges with DRaaS
It’s still early in the game, and DRaaS is by no means a proven use case at 11% overall adoption. Despite the strong economic and flexibility benefits of DRaaS, many enterprises are hesitant to adopt for these reasons:

- Complexity of Deployment
- Security and compliance are difficult to achieve in the cloud
- Providers are often unwilling to negotiate SLA penalties
- Not all cloud providers can support adequate site separation
- Some apps don’t work in cloud environments
- Recovery resources are oversubscribed

Security and compliance are difficult to achieve in the cloud
Security concerns regarding compliance and data protection is still the top barrier to public cloud adoption. Often what the enterprise requires and what the provider offers don’t match up — and that’s not always clear.

It’s up to the enterprise to fully understand the offering and make up the difference between the two. Enterprises need to take the same additional security features as they would if these applications were permanently running in the cloud.

Providers are often unwilling to negotiate SLA penalties
Despite charging customers based on RPO and RTO, there are typically no financial repercussions for missing these SLAs. We observed that for many enterprises, this simply isn’t good enough for DRaaS.

Not all cloud providers can support adequate site separation
For DRaaS, location is of utmost importance. If we’re planning to use this site in the case of a region wide disaster, it’s important that our recovery site is not in the same affected region. There’s no hard-and-fast rule for site separation, but it’s important to locate the production and recovery sites far enough apart so they are not subject to the majority of the same risks, but not so far apart that latency and bandwidth become barriers. Most DRaaS providers don’t have significant geographic presence and/or redundancy within each represented country. Whether a provider meets business requirements can be hit or miss.

Some apps don’t work in cloud environments
Simply put, there are applications, observed, that are not a good fit for a cloud environment — and unfortunately, it’s often these legacy and high transaction applications that are the most critical. Typically, applications that run on x86 platforms and can easily fit into VMs will be solid candidates for DRaaS. Because of this, there will be few companies that use the cloud for all of their recovery needs; DRaaS will be one tool in the tool kit alongside more traditional recovery methods.

Recovery resources are oversubscribed
DRaaS providers typically, have been found to oversubscribe resources, banking on the fact that all customers won’t need to use resources at the exact same time. On the one hand, enterprises need to know that if there’s a region wide disaster, they’ll still be able to recover; but on the other hand, DRaaS providers can’t reserve resources for the just-in-case scenario, keeping these resources unused and revenue-less in the meantime. Some providers guarantee that some minimum level of resources will be available at the time of declaration, but other providers offer no guarantees that resources will be available when needed. Current DRaaS providers offer certain levels of capacity guarantees only at an extra cost.
<table>
<thead>
<tr>
<th>Provider/Vendors</th>
<th>Solutions Provided</th>
<th>Service Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon</td>
<td>DRaaS</td>
<td>Amazon Virtual Private Cloud (Amazon VPC) lets you provision a private, isolated section of the Amazon Web Services cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address range, creation of subnets, and configuration of routes tables and network gateways. This would enable you to create a VPN connection between your corporate datacenter and your VPC and leverage the AWS cloud as an extension of your corporate datacenter.</td>
</tr>
<tr>
<td>CA Technologies</td>
<td>DRaaS</td>
<td>In early 2012, CA Technologies announced CA ARCserve D2D On Demand hybrid data protection and recovery based on Microsoft Azure. This solution gives ARCserve Backup customers the ability to back up data to the Azure cloud and also to recover those backups in the cloud. CA also offers ARCserve Instant Recovery On Demand, which is based on Geminare's Cloud Recovery.</td>
</tr>
<tr>
<td>Carpathia Hosting</td>
<td>DRaaS</td>
<td>Carpathia Hosting is a provider of managed hosting, cloud, colocation, and other data center services. Using this solution, customers can replicate data to one of Carpathia’s data centers from either on-premises production or another cloud environment. There, VMs can be grouped into application consistency groups to ensure that recovery is successful. Carpathia offers managed recovery solutions or customers can opt to manage their own recovery.</td>
</tr>
<tr>
<td>Doyenz</td>
<td>DRaaS</td>
<td>Doyenz is a cloud provider focused specifically on BC/DR solutions. Doyenz’s rCloud offering uses either ESX virtual machine snapshots or backups by StorageCraft ShadowProtect software to replicate data to one of Doyenz’s data centers in the U.S. or UK. Backups of virtual or physical machines can be spun up into VMs in roughly 15 minutes. In early 2012, Doyenz and Symantec partnered to offer Backup Exec Cloud DR option, allowing current Backup Exec customers to recover via backups in the Doyenz cloud. Doyenz is headquartered in Bellevue, Wash., and has approximately 3,500 customers using the service today.</td>
</tr>
<tr>
<td>EVault</td>
<td>DRaaS</td>
<td>EVault’s Remote Disaster Recovery solution is based on the company’s flagship cloud backup vaulting service. It’s a fully managed DRaaS service with DR planning, testing, and guided recoveries included. Backups can be spun up into VMs in the cloud with an RTO of 4 to 48 hours. Users pay a base rate based on capacity plus an additional flat fee per server when a disaster is declared. Actual prices are dependent on the type and amount of servers, data, and VPN connections, as well as the length of the contract.</td>
</tr>
<tr>
<td>Provider/Vendors</td>
<td>Solutions Provided</td>
<td>Service Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>FusionStorm</td>
<td>DRaaS</td>
<td>FusionStorm was one of the four launch partners of VMware for Site Recovery Manager (SRM) 5.0 — the first version to enable providers to offer SRM-as-a-service. The solution involves deploying SRM agents onto VMware hosts that need protection. Data is replicated to the cloud using vSphere replication, and SRM is used for the failover automation.</td>
</tr>
<tr>
<td>Hosting.com</td>
<td>DRaaS</td>
<td>Hosting.com offers several different flavors of cloud-based recovery, including Cloud Replication, powered by VMware SRM 5.0 offering VMware replication and failover; Server Replication, powered by Geminare, which provides cloud-based recovery for physical and virtual machines; and SAN2SAN Replication, based on EMC RecoverPoint and VMware SRM 5.0.</td>
</tr>
<tr>
<td>iland</td>
<td>DRaaS</td>
<td>iland, another launch partner for VMware’s SRM 5.0 cloud recovery, has been offering cloud-based DR for several years. Its Continuity Cloud offering allows customers to choose from a range of different technology platforms, including Acronis, Dell Equallogic, Veeam, VMware SRM, and Vision DoubleTake to replicate systems to the iland cloud. Once in the cloud, iland offers both managed and unmanaged recovery options.</td>
</tr>
<tr>
<td>IT-Lifeline</td>
<td>DRaaS</td>
<td>IT-Lifeline is a BC/DR service provider based in Washington state. Its cloud DR solution, BlackCloud and BlackCloud Edge, is built on AWS and based on CommVault Simpana 9 software. It allows customers to failover production servers to either IT-Lifeline’s data center, or to leverage Amazon Web Services for recovery. BackCloud Edge delivers compliance with SAS70 Type II, ISO 27001 Certification, Payment Card Industry Data Security (PCI DSS) Level 1 Service Provider, and FedRAMP (FISMA).</td>
</tr>
<tr>
<td>Microsoft Windows Azure</td>
<td>DRaaS</td>
<td>Microsoft Windows Azure is one of the leading cloud service providers. In January 2012, Microsoft announced an alliance with Geminare. Geminare’s recovery-as-a-service (RaaS) solution will be delivered through the Azure platform. Additionally, its basic services can be leveraged by companies to build their own recovery cloud. Compute resources range from $30 to $720 per month per VM (with some storage included). SQL Azure databases range from $3.33 to $10 per GB per month. There are additional charges for bandwidth, service bus, CDN, access control, and caching on a usage basis.</td>
</tr>
<tr>
<td>VeriStor</td>
<td>DRaaS</td>
<td>VeriStor is a cloud service provider focused on enterprise and mid-market companies. VeriStor’s cloud continuity for VMware vSphere and cloud DR services are based on VMware SRM 5.0 — VeriStor is another of VMware’s launch partners. VeriStor also supports replication from HP, Dell, and other storage platforms to support DR-in-the-cloud services.</td>
</tr>
<tr>
<td>Provider/Vendors</td>
<td>Solutions Provided</td>
<td>Service Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allstream</td>
<td>DRaaS</td>
<td>Allstream is a B2B network provider based in Canada. Allstream’s managed cloud replication services are based on Geminare’s Cloud Recovery and provide customers with real-time server replication and automated failover and failback. Allstream also offers traditional IT systems recovery and workforce continuity solutions.</td>
</tr>
<tr>
<td>CenturyLink</td>
<td>DRaaS</td>
<td>In 2011, CenturyLink acquired Qwest and Savvis, which significantly expanded their disaster recovery services portfolio. CenturyLink Realtime application recovery (originally a Qwest offering) is based on Geminare’s Cloud Recovery. Savvis, a CenturyLink company, also offers managed and custom cloud-based disaster recovery services.</td>
</tr>
<tr>
<td>Terremark, a Verizon Company</td>
<td>DRaaS</td>
<td>Terremark, a Verizon company, offers fully managed virtualized disaster recovery (VDR) based on replication solutions from Veeam, Zerto, NetApp, and other array vendors. Data is replicated to the Terremark cloud where applications can be restored into shared or dedicated infrastructure. In addition to its cloud offering, it can support recovery for hybrid environments that require a mix of physical and virtual resources. VDR can also be deployed in an active-active configuration to support applications such as SQL, Exchange, DNS, ActiveDirectory, Oracle, and Lotus Notes. Customers can elect a committed or burst model depending on its own oversubscription tolerance.</td>
</tr>
</tbody>
</table>
Deloitte and disaster recovery

Deloitte’s SNL team has already prepared a POC for Disaster Recovery using Amazon Elastic Compute Cloud (Amazon EC2) web service for public and hybrid clouds. Oracle’s RDBMS, Secure Backup Cloud module along with other Monitoring tools were used. The team deployed Data Guard on AWS.

Below is a high level architecture of Data Guard on Cloud.

**Observations**

Disaster Recovery Infrastructure is expensive in terms of:

- hardware,
- software,
- network,
- facilities and
- resources

Proper planning is needed on below mentioned points:

- Budgeting
- Provisioning
- Implementation
- Training
- Maintenance

**Key takeaways**

- **Security:** Requirements will vary when deployed in the public or hybrid cloud compared to all in-house
- **Network:** Review your application network latency and bandwidth requirements
- **Monitoring:** We can monitor instances in the Amazon Virtual Private Cloud using our existing tools, however we were unable to use the tools on Amazon EC2 Cloud
- **Backups:** An instance in the VPC can be backed up either to S3 (with OSB Cloud Module) or to existing enterprise backup solution.
- **Standby Database:** Creation and switchover faster on EC2 to EC2 as compared to in-house to VPC
- **Configuration:** Configuring Data Guard on Amazon EC2 or Virtual Private Cloud is not any different from traditional in-house configuration
- **Firewall:** Applications or services running on non standard ports on Amazon EC2 will require additional ports to be opened on the corporate firewall.
Future with DRaaS
According to a recent IDC survey, data center managers expect to allocate nearly 50 percent of their budgets to running services in the cloud (public and private) by 2013. As this cloud revolution continues, it’s also becoming increasingly clear that more and more applications will be delivered “as a service.” Disaster recovery as a service (DRaaS) is particularly interesting as it helps IT address many of its biggest challenges. Because of this, DRaaS is a natural for cloud computing and is rapidly becoming the killer app for the cloud – with service providers, IT resellers and start-ups all jumping on board.

Research conducted by Technavio reveals, that the Global Disaster Recovery Services Market 2010-2014 will reach $22.6 billion in 2014. One of the key factors contributing to this market growth is the need for better data security. The Disaster Recovery Services Market has also been witnessing cloud based disaster recovery. However the complexity of deployment could be a challenge to the growth of this market. Deloitte’s capability with DRaaS.

Conclusion
DRaaS is an emerging solution for organizations that wish to control their own infrastructure but not maintain the disaster recovery systems themselves. With a DRaaS offering, an IT organization does not directly build a contingency site, but instead relies on a vendor to do so on a dedicated or utility computing infrastructure. The cloud’s advantages of elasticity and cost-reduction are significant benefits in a disaster recovery scenario, and service offerings allow organizations to outsource portions of contingency planning to vendors with expertise in the area. However, many of the complexities remain and it is essential to perform the due diligence to ensure that the contingency plan will work and provide a sufficient level of service if called upon. Deloitte’s PoC, stresses upon the fact that we can establish production like capabilities on disaster recovery and we can host long term environments on Amazon EC2 through DR process. According to us providing this a service could fetch us more business from end to end client.

References

http://www.mspmentor.net/2012/02/07/why-disaster-recovery-as-a-service/


http://aws.amazon.com/disaster-recovery/


http://aws.amazon.com/ec2/


Authors
The authors welcome your comments and questions.

Minal Deshpande
Deloitte Consulting SI
mdeshpande@deloitte.com

Kanchan Bansal
Deloitte Consulting SI
kbansal@deloitte.com

Bharat Jadwani
Deloitte Consulting SI
bjadwani@deloitte.com

Vishnu Vardhana Raju
Deloitte Consulting IM
vraju@deloitte.com

Pallavi Satpute
Deloitte Consulting SI
pasatpute@deloitte.com

Mamta Sharma
HR Talent Business Advisor
mamsharma@deloitte.com
Disaster Recovery (DR) is a solution that offers business continuity across a range of organizations and their applications by ensuring availability of IT infrastructure in case of any disaster resulting in disruption of Business Services.