A Newsletter from Ernst & Young

April 2008

**Disaster Recovery Services**

**Research Paper**

**NITRO - Fuelling Innovation**

**September 2015**

Contents

[Executive summary 3](#_Toc420069244)

[Introduction 3](#_Toc420069245)

[Features - DRaaS 3](#_Toc420069246)

[Business Benefits - DRaaS 4](#_Toc420069247)

[Major Vendors 4](#_Toc420069248)

[Recommendations 4](#_Toc420069249)

[Approach 5](#_Toc420069250)

[Analysis 6](#_Toc420069251)

[Disaster Recovery 6](#_Toc420069252)

[Key Benefits – Disaster Recovery 6](#_Toc420069253)

[Common Causes of Disaster 6](#_Toc420069254)

[Key Terms – Disaster Recovery 7](#_Toc420069255)

[Best Practices for IT Disaster Recovery 7](#_Toc420069256)

[Disaster Recovery Service Models 8](#_Toc420069257)

[Disaster Recovery as a Service (DRaaS) 12](#_Toc420069258)

[Appendix and references 22](#_Toc420069259)

# Executive summary

**01**

## Introduction

Disaster Recovery (DR) and Business Continuity Planning (BCP) are integral parts of the overall risk management of an organization. Since all the risks cannot be avoided, it is vital for every successful organization to have a well-defined and properly tested DR plan. The efficiency of a DR strategy depends on how fast and effectively can the operations be recovered on the DR site and failed back once the primary site returns to normal.

DR Services refer to a set of services that offer business continuity by enabling data backup, recovery, and retrieval. It helps enterprises to quickly recover business critical applications during natural disasters such as floods, tornados, hurricanes, or even a sudden and unforeseen system failure. There are different approaches to DR implementation and the prominence of cloud computing enhances the traditional ways of DR to have a more robust DR solution in the cloud.

Disaster Recovery as a Service (DRaaS) model leverages cloud technologies to facilitate agile recovery and achieve business resilience during declared disasters or other catastrophic events. DRaaS is the replication and hosting of physical or virtual servers by a third party to provide failover in the event of a disaster.

## Features - DRaaS

**Pay as you Go –** Pay for infrastructure only in the event of a disaster when the workloads need to be brought online during failover.

**Flexible Scalability –** Adding applications or VMs to the DR plan is simple and require no hardware changes.

**Automation -** Automated failover, failback, and DR testing are executed with just a few clicks.

**Assisted DR Implementation, Testing and Recovery –** DRaaS implementation with minimal in-house expertise.

**Workload Mobility –** Option to choose recovery of the entire infrastructure or just one VM or application.

**Better RTO and RPO –** Improved RTO and RPO at low cost when compared to traditional DR services.

**Support for Physical and Virtual Servers –** Supports recovery of both physical and virtual servers

**Simple Deployment and Management –** Removes the complexity involved in traditional DR services.

**Array Agnostic** – Eliminates the need for matching storage arrays and reduces storage cost.

**Leverage Expertise –** Third party DRaaS provider brings expertise in DR service management.

## Business Benefits - DRaaS

DRaaS helps business to achieve flexible and highly attainable DR solutions. Major benefits include reduced complexity and cost, minimized risk, flexible scalability, improved RTO and RPO, less manual intervention, automation reduced requirement for in-house IT expertise etc.

## Major Vendors

The major vendors in DRaaS landscape include SunGard, IBM, NTT Communications, Axcient, AWS etc.

# Recommendations

**02**

Disaster Recovery is an inevitable part of every organization to help the business continue with least interruption and to retain customers and brand value. DRaaS, the new delivery model for DR that leverages cloud technology facilitates agile recovery and achieve business resilience during disasters. This helps to achieve a service – oriented DR approach.

The findings and recommendations based on the initial research are described in this section. Applications that require a better DR than in-house DR are good candidates for cloud DR. Backup based DRaaS solutions are good options for small data centers.

It is important to gain experience with cloud based computing, storage, backup and DR for less critical applications before switching to DRaaS for data center level DR. While EY is embracing cloud based infrastructure and services, DRaaS can be considered as a genuine alternative to traditional DR approaches. Proven recovery capability, solution manageability, DR testing, migration capability and platform support should be the key factors when considering vendor evaluation.

Another key aspect is to ensure getting appropriate support from the provider for transition and DR testing. The cost involved in all the realms including DR testing needs to be considered.

Based on the initial research, recommended vendors for analyzing in detail in the next phases are SunGard, IMB, NTT Communications, Amazon, Microsoft et al.

# Approach

**03**

This research is intended to understand the various Disaster Recovery services available and how best it can be utilized for EY infrastructure. The research focuses on Disaster Recovery as a Service practice which makes use of cloud computing features. Vendor landscape is analyzed to discover the options offered by various Disaster Recovery solutions available in the market.

The research will be progressed to next stages, once the research paper is approved. This research was completely based on the information available on the internet. Discussion with various vendors and further experimentation with products would be required to reach a conclusion on the feasibility of enterprise wide adoption

Scope of Research

* What is Disaster Recovery and its relevance in IT
* Best practices for IT Disaster Recovery
* Disaster Recovery service models
* Cloud based DR services
* Disaster Recovery as a Service (DRaaS)
* Pros and Cons of DRaaS
* Factors affecting DRaaS adoption
* Critical capabilities of DRaaS vendors
* DRaaS Use Cases
* Key Considerations while selecting DRaaS vendor
* Vendor Landscape

# Analysis

**04**

## Disaster Recovery

When an unforeseen event takes place and brings the day-to-day operations to a halt, it is vital for every organization to recover as early as possible to continue providing services to the clients. Business Continuity and Disaster Recovery plans are imperative to reduce the impact of risks and to keep the organization brand name intact.

Disaster Recovery (DR) involves a set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human induced disaster. Disaster is an event that makes the continuation of normal functions impossible. While business continuity sets out controls to keep all aspects of business functioning when a disaster hits, Disaster Recovery primarily focuses on IT and its systems that support business functions in the case of a disaster.

### Key Benefits – Disaster Recovery

Customer

Satisfaction

Retain

Brand Value

Demand for

Zero Down Time

### Common Causes of Disaster

Fire & Accidents

Natural Disasters

Power Outages

Viruses

Sabotage

Server Failure

### Key Terms – Disaster Recovery

RPO

RTO

Recovery Point Objective -

The acceptable amount of data loss measured in time.

Recovery Time Objective -

The time it takes after a disruption to restore a business process to its defined service level

### Best Practices for IT Disaster Recovery

IT services need to be classified in to a handful number of classes of tiers based on the criticality. Some IT services will need to be recovered faster than others. Standardizing the mechanisms used in each tier to recover from faults and failures is a key DR process best practice.

Classification of Services

System availability, recovery speed and recovery assurance are inversely related to a system's complexity. More complex systems and recovery processes have more things that can break.

Decrease Complexity

Preventive mechanisms should be in place to avoid down time for common disruptions such as hardware, network and software failures. IT resiliency should be improved by building applications, storage and IT infrastructure resilient to disasters.

Increase Resiliency

### Disaster Recovery Service Models

The solutions available for IT Disaster Recovery can be categorized based on multiple factors. The various service models in DR can be broadly classified as below. Some vendors offer solutions of multiple service models.

DR Services

Iron Mountain

Commvault

Netapp

Evault

Rsync

Traditional DR

Cloud based DR

Offsite Backup

Colocation

Offsite Dedicated

Cloud Backup / Online Storage

DR Cloud Private / Public

DRaaS

Rackspace

Netmagic

Verizon -Terremark

NTT

Proprietary Solutions

Amazon

IBM

Microsoft

Axcient

Evault

Sungard

VMware

IBM

Sungard

IBM

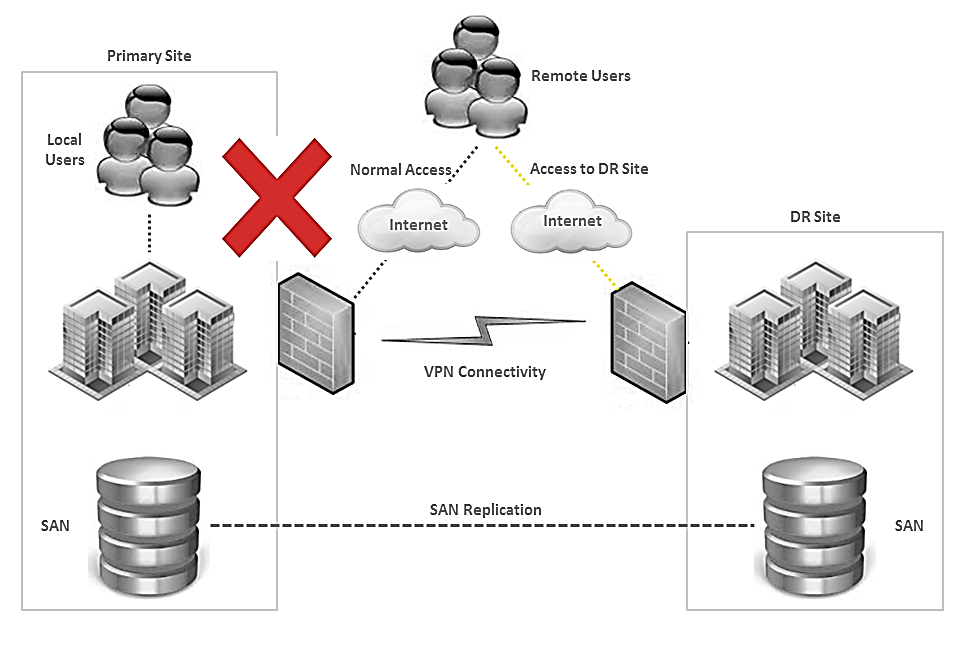
NTT

Microsoft

Amazon

#### Traditional DR

Traditional Disaster Recovery solutions involve the use of offsite data centers that replicate an organization’s critical IT infrastructure. Not all applications may be a part of the traditional DR plan. The DR site would be geographically away from the primary site to ensure recovery in the event of natural disasters like flood or earthquake.



##### Offsite Backup

This involves taking the backup of critical data on to backup tapes and sending them to a secure tape storage location or enabling the backup of local data on to a remote storage share with the help of backup software. The backup data can be used for server / data recovery in the event of a disaster at the primary site.

Major Vendors

* Iron Mountain
* Commvault
* Netapp
* Evault
* Rsync

##### Colocation

Colocation data centers are an alternative to setting up organization’s own DR site in a remote location or outsourcing the Disaster Recovery to a Disaster Recovery service provider. Colocation facilities offer a data center in which organizations can set up own network, servers and storage.

Colocation DR Selection Criteria:

* Power and Communication Redundancy
* Distance from Primary Site
* Technology Requirements
* Remote Management
* People Availability, Skills and Transportation Issues
* Physical Infrastructure and Security
* Regional Jurisdiction Regulations
* Cost Considerations

Major Vendors

* Rackspace
* Netmagic
* Verizon -Terremark
* NTT

##### Offsite-Dedicated

This is the proprietary DR solution for the organization where the secondary infrastructure is built in the DR location. The DR location would be a place owned by the organization which is dedicated for the Disaster Recovery purpose.

#### Cloud based DR

Cloud based DR indicates the scenario where the Disaster Recovery site or the backed data resides on the cloud. Cloud is essentially beneficial when it is used for DR considering the key features of cloud computing like flexible scalability, pay-as-you-go model etc. Cloud based DR site can used for recovery when the primary site goes down

##### Cloud Backup / Online Storage

Cloud backup refers to backing up data on to the storage on cloud. The data stored on cloud can be used for recovery in the event of a disaster. Many of the cloud storage solutions use high performance object based storage for fast backup and easy recovery.

Major Vendors

* Amazon
* IBM
* Microsoft
* Axcient
* Evault

##### DR Cloud Private / Public

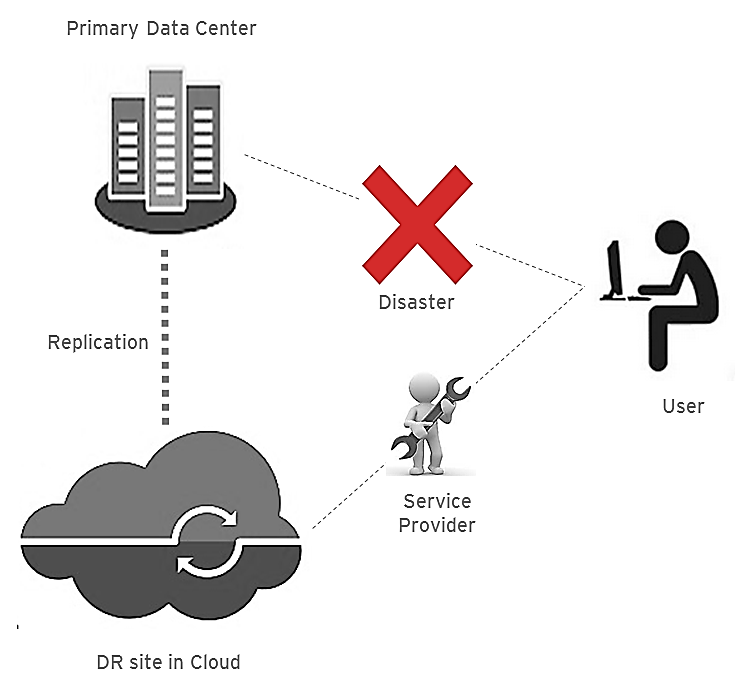
This solution makes use of private or public cloud implementation for Disaster Recovery. DR site can be hosted on a private cloud solution implemented at remote premises of the organization or it can be on a public cloud solution.

Major Vendors

* VMware
* Microsoft
* Amazon

### Disaster Recovery as a Service (DRaaS)

Disaster Recovery as a Service (DRaaS) is the replication and hosting of physical or virtual servers by a third-party to provide failover in the event of a disaster. Third-party vendor provides failover to a cloud computing environment, either through a contract or pay-per-use basis.



DRaaS addresses well-recognized pain points in IT Disaster Recovery management, including the need for frequent recovery-readiness testing and the cost of dedicated recovery floor space and facilities.

Major Vendors

* Sungard
* IBM
* NTT
* MS Azure
* AWS

#### Key Benefits - DRaaS



Cost saving can be achieved through avoiding large capital investment and the reduced time for recovery

Cost Effective Approach



Selective recovery of application workloads.

More Attainable DR



Provides much faster recovery when compared to other DR mechanisms

Speed of Recovery



Cloud DR Tests are more automated and require less manual intervention

DR Tests require Less Intervention



Cloud resources can quickly be added with fine granularity

Flexible Scalability

#### Factors Influencing DRaaS Adoption

* Quality of internet connectivity – Available WAN bandwidth for DR replication is a crucial factor in the success of DRaaS
* Regional cloud DR providers – DR service provider should have data centers far enough away to avoid the local disaster threats, but not so far away as to have an optimum WAN throughput
* Security concerns – This is a key consideration as per the organizational policy on security standards
* Organizational readiness – Cloud adoption readiness of the organization directly influences the choice of DRaaS

#### DRaaS and WAN Bandwidth

Sufficient bandwidth is a critical factor in the feasibility of cloud DR. This includes initial transmission of dataset and replication of data changes to the cloud.

There are two mechanisms for data replication

* Primary Data Replication – Requires significantly larger WAN throughput. It usually transmits the entirety of each of all changes. If the RPO is less than one day, then primary data replication (synchronous) would be required. This requires the DR site to be within 100 kilometers of the principle data center location, measured using the network cabling route. Synchronous replication is supported by very few software-based data replication solutions and must depend on storage hardware based replication. Only the traditional DR service providers and large Telcos generally support this.
* Backup Data Replication - Takes advantage of data deduplication before the periodic replication of backup data is transmitted to a remote site. It transmits only the final update in addition to deduplicating the data. Total daily data change volume can be reduced by the backup data deduplication and compression. Backup data replication only works if the RPO is greater than the backup frequency plus the backup data replication time delay.

#### Cloud DR Security

Cloud adoption for DR depends on the organizational policy on cloud security and the way in which the concerns are addressed. One of the mechanisms used by DRaaS vendors is data encryption. DRaaS vendors offer ways to encrypt data before it is transmitted to the cloud site and have data at rest in the cloud remains encrypted as well. The encryption keys can be held locally as well.

Below factors need to be considered while evaluating cloud security at the vendor level

* Customer specific firewalls
* Configurable VPNs
* Logging practices
* Network I/O authentication practices
* Security standards compliance practices

#### Critical Requirements of DRaaS

* **.**
* Physical and virtual system data protection and recovery capabilities
* DR testing and DR declaration support
* Pricing policies
* Value-added services (such as network optimization and DR test assistance)
* Speed with which it enables IT service recovery
* Manageability (including monitoring, reporting and networking options)
* Resiliency (including multisite capabilities, backups and the vendor's own DR maturity)
* Security and compliance (including data privacy measures and standards conformance)
* RPOs and RTOs
* Mechanism for data transmission to the cloud
* Easy-to-access-and-use tools for system monitoring and tracking and for performing failover and failback functions
* Should enable to thoroughly test Disaster Recovery capabilities to ensure readiness and reliability
* Smooth migration from, and coexistence with, traditional Disaster Recovery infrastructure and systems
* Offers support for mixed and virtualized server environments

**DRaaS – Critical Requirements**

#### Pros and Cons of DRaaS

**DRaaS - Pros**

* Offsite vendor will be less likely to suffer the direct and immediate effects in the event of a disaster
* Disaster Recovery is possible even in the case of, a total or near-total shutdown of the affected organization.
* Reduced need for expertise to provision, configure and test an effective disaster recovery plan.
* Organization doesn't have to invest in and maintain their own off-site DR environment.
* DRaaS contracts can be flexible as the business needs change.
* Offer value for an entire production infrastructure, all the servers and all the storage
* Minimize or even completely eliminate the requirement for organization capital in order to implement a DR solution
* Gives organizations the option to manage disaster recovery planning and processes internally or outsource it completely if they do not have the resources and expertise in-house
* Enables organizations to be more business IT resilient. Offers users the option to proactively failover to the cloud during the planned outage.
* Pay as you go option - organizations pay only for the services they need
* Easily scalable
* Eliminate the need for infrastructure that sits idle

**DRaaS - Cons**

* Organization must trust that the DRaaS service provider can implement the plan in the event of a disaster and meet the defined recovery time and recovery point objectives
* Not all clouds are created equal – some are considerably less secure, reliable and dynamic than others
* Security is another aspect to consider – Both data and physical security can be a challenge in DRaaS
* Not all DRaaS providers support unlimited managed failovers
* DRaaS may not be the best solution for recovering large data center operations
* Additional cost can be involved in DR testing
* Highly dependent on the available bandwidth and can burden the normal business traffic
* Cloud DR operations management requires additional training on new tools
* Things to manage while changing the vendor can be an overhead

#### DRaaS – Comparison with Traditional DR

|  |  |
| --- | --- |
| **Tradtional DR** | **DRaaS** |
| Secondary DR site with large investments in additional data center space, connectivity and servers | Pay only for what is stored and what is used – data storage and replication costs. Pay for servers on an infrastructure-as-a-service basis only in the event of a disaster when the virtual machines need to be brought online during failover. |
| Additional operational costs in terms of power, cooling, site maintenance etc. | No operational costs involved in term of hardware maintenance |
| The checklist of processes involved in making DR site live involves a time lag | Cloud DR sites are automated and can be made live within seconds or minutes |
| Relative risk of loss of data and business continuity | Minimizes data loss and improves business continuity |
| If connectivity between the primary site and the DR site fails, manual operations are required to start operations at the DR site | Cloud DR site can be triggered through a normal laptop or mobile device with a wireless internet connection even if the as designed connectivity fails |
| In-house automation | Cloud operations and DR process are highly automated |
| Idle redundant infrastructure | No idle infrastructure |
| Highly complex | Less complex |
| Scalability is difficult to achieve | Easily scalable and flexible |
| RPO and RTO achievable is not good as DRaaS | Better RPO and RTO |
| Security is ensured since the infrastructure is owned by the organization | Involves Cloud security challenges |
| Can’t start small | Can be started in small scale |
| DR testing and recovery process requires specialized staff skills | Well assisted DR tests and actual recovery process |
| Risk involved in hardware failure at the DR site | No risk of hardware failure at DR site |
| Complex process involved in getting started | Easy to get started |
| No self-service features available | Leverages the self-service capability of cloud model |

#### DRaaS Use Cases

##### **Application Group DR**

Complex applications which require a quick DR can make use of cloud DR

Disadvantages

Advantages

* Running a few IT services or applications in a DRaaS environment creates additional network, security, operations, management and sometimes regulatory challenges
* Separating some applications from other IT infrastructure DR can complicate DR
* Offer more agility and can be implemented relatively quickly
* Enables a DR capability with almost no in-house DR infrastructure or upfront costs
* Enables an organization to leverage cloud DR on a trial basis when larger-scale cloud DR might otherwise be problematic
* VM technology and VM replication enable DRaaS providers to offer very quick IT service recovery

##### **Small Data Centers**

For small data centers, DRaaS is hassle free when compared to the steps involved in recovering the data from off-site backup tapes

Advantages

Disadvantages

* Data backups and replication to cloud storage can require and consume significant WAN bandwidth
* Cloud DR operations and management integration take additional resources and often require learning new tools and user interfaces
* Addressing the relevant security and compliance concerns that exist with cloud DR may require extra staff resources
* Switching DRaaS vendors will require almost as much effort as picking the first DRaaS vendor
* Enables DR without additional data center facilities, storage or system hardware capital expenses
* Provides more DR configuration agility
* Enable simpler and more frequent data protection than the tape based backups often otherwise used for off-site data storage and DR for small data centers
* Enable faster recovery than the tape-based backups and restores
* Enables DR testing to be performed quickly and inexpensively

##### **Mid-Size Data Centers**

Not for all mid-size data centers, DRaaS is considered as mature enough to be adopted

Advantages

Disadvantages

* No hardware capital expenses
* More agility
* Faster recovery than tape-based backups and restores
* Enables more flexible DR environments than organizations normally can obtain with other DR approaches
* With VM technology. VMs can be restarted in the cloud within minutes of a disaster
* Additional resources are needed for DRaaS and operations integration
* Vendor failures may cause more frequent DRaaS migrations
* Assessing and addressing the relevant security and compliance concerns with cloud DR requires extra staff resources
* Data replication to the cloud consumes significant WAN bandwidth
* Cloud DR vendors charge for cloud storage use by the gigabyte per month which added up to the annual cost

##### **Large Data Centers**

All the challenges should be addressed before adopting DRaaS for large data centers and special care should be taken in the vendor selection

* No hardware capital expenses
* More agility
* Faster recovery than tape-based backups and restores
* Enables more flexible DR environments than organizations normally can obtain with other DR approaches
* With VM technology. VMs can be restarted in the cloud within minutes of a disaster

Disadvantages

Advantages

* Additional resources are needed for DRaaS and operations integration
* Data replication to the cloud consumes significant WAN bandwidth and can burden the user traffic
* Because of the typical storage and security configurations required, DRaaS for such large environments costs more
* RPO/RTO tiers may not be equivalent to in-house RPO/RTOs

#### Key Considerations in DRaaS Vendor Selection

* Support all the organization applications or just some of them
* Provider experience in managing actual DR declarations
* Vendor support for different production computing platforms
* VM profiles available and associated costs
* Vendor flexibility in managing VM allocations
* Data Synchronization aspects
* Data protection after failover
* Services included in RaaS cost and optional services available
* Penalty involved in not meeting SLAs
* DR testing time and cost factors

**Evaluate Cloud DR Service selection criteria**

* Ensure successful DR failover and failback processes
* Define RTOs and RPOs
* Vendor experience in handling extended disruptions
* Vendor consistency in meeting SLAs
* DR Infrastructure coverage
* Support for testing of DR plans, cost involved and automated testing
* Regular testing of DR Plan

**Recovery Assurance**

* Try Cloud DR on low risk IT services first
* Develop POC for DRaaS
* Test preferred RaaS solutions
* Evaluate cost savings and trade-offs

**Try before finalizing the options**

**Be Aware of Scalability Challenges**

* Wan bandwidth limitations during busy periods
* Implement data deduplication and compression techniques
* Implement detailed RaaS provider exit strategy, in case of change of provider or strategy

#### DRaaS Vendor Landscape

Major Vendors

* Sungard
* IBM
* NTT Communications
* Axcient
* AWS
* MS Azure

# Appendix and references

**05**

Detailed document on DRaaS vendor landscape is attached in the summary presentation for the research

[www.gartner.com](http://www.gartner.com)

[www.networkworld.com](http://www.networkworld.com)

[www.infoworld.com](http://www.infoworld.com)

[www.computerworld.com](http://www.computerworld.com/)

[www.techtarget.com](http://www.techtarget.com)

[www.forrester.com](http://www.forrester.com)

www.redmondmag.com

http://www.datacenterknowledge.com

<http://www.sungardas.com>

[www.axcient.com](http://www.axcient.com)

[www.ibm.com](http://www.ibm.com)

[www.azure.microsoft.com](http://www.azure.microsoft.com)

[www.aws.amazon.com](http://www.aws.amazon.com)

[www.nttict.com](http://www.nttict.com)

www.sungard.com

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2015 EYGM Limited.

All Rights Reserved.

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com

EY | Assurance | Tax | Transactions | Advisory