IDC Middle East, Africa, and Turkey, Al Thuraya Tower 1, Level 15, Dubai Media City, P.O. Box 500615, Dubai, United Arab Emirates (UAE).
Tel: +971 4 391 2741 Fax: +971 4 391 1922

WHITE PAPER

Preparing for Disaster Recovery in Qatar

Sponsored by: MEEZA

Saurabh Verma
March 2014

IDC OPINION

Recent IDC research on business continuity and disaster recovery (BC/DR) services shows increased demand and uptake of these services among organizations in the Gulf Cooperation Council (GCC) and Qatar. Risk management and sustainability have been cited by organizations as the most important drivers for spending on disaster recovery (DR). When probed further on the risks associated with downtime, organizations stated that these cover a wide range; customer attrition, revenue loss, loss of reputation, and lawsuits, to name a few. The recent cyberattacks on certain high-profile organizations in the GCC region have spurred several organizations to reassess their BC/DR measures. Now, much greater involvement and collaboration are occurring between CIOs, senior executives, and boards to develop and implement DR strategies. In some industries, such as banking and financial services, specific regulations (overseen by central banks, where banks are concerned) mandate strong DR setup. Although no stringent regulations exist in the oil and gas industry, organizations are proactively implementing DR to mitigate risk and use the capability to showcase their global competitiveness.

IDC research shows that large and mature organizations across verticals in Qatar and the GCC are mostly proactive, and, by and large, are addressing BC/DR requirements by setting up in-house DR infrastructure. However, the research also showed an increasing appetite for outsourced and managed BC/DR services. The growing availability of these service offerings from providers, coupled with improved service delivery standards, have contributed to increased confidence, and thereby, adoption. Similarly, the hosted DR model is seeing greater demand as the value becomes apparent – such as access to the latest technologies, improved connectivity, guaranteed uptime, and service level agreements (SLAs) at lower capital expenditure.

In today's dynamic marketplace, organizations want to ensure that their businesses are up and running 24/7, and do not stop operations even in the event of a disaster. Therefore DR is now understandably becoming an integral and critical part of an organization's Business Continuity Plan (BCP).

IDC believes that:

- BC/DR will continue to be among the top priorities for CIOs in the coming years. IDC research indicates that 72% of the CIOs surveyed had planned BC/DR investments in 2012, compared to 48% in 2011.
- The increased adoption of outsourced models (i.e., hosted DR and managed DR) will drive the adoption of managed BC/DR services in the GCC and Qatar.
- The United Arab Emirates (UAE), Saudi Arabia, and Qatar are the largest IT markets in the region. Backed by the growing adoption of outsourcing services,

IDC predicts that spending on managed DR services will increase significantly (CAGR greater than 19%) for the combined UAE, Saudi Arabia, and Qatar market over the next five years. IDC predicts that outsourcing services and DR services will grow more than 20% in Qatar in the next three years.

- GCC organizations are likely to leapfrog generations of technology and bypass some of the DR obstacles faced by organizations in more mature markets resulting from legacy infrastructure.

- IDC believes that DR services in the GCC will evolve as large organizations and IT services firms come together to offer hosted and managed DR services. Faster time to market and cost pressures will further boost the adoption of fully outsourced DR, where both infrastructure and management will be owned by the services provider.

This IDC White Paper examines DR as part of the overall BCP, and analyzes prevalent DR models as to their merits and demerits.

METHODOLOGY

In preparation for this white paper, IDC utilized its continuous research on outsourcing, managed, and datacenter delivered services in the GCC and Qatar. Specifically, this document references IDC studies on managed BC/DR services. Additionally, this white paper references IDC's annual survey of CIOs in the Middle East. This survey focuses on understanding organizations' technology investment priorities and focus areas.

IDC also conducted in-depth interviews with regional IT service providers and user organizations in Qatar, the UAE, and Saudi Arabia, across verticals including banking, transportation, financial services, oil and gas, and manufacturing. The objective of the user interviews was to understand the existing BC/DR strategies and infrastructure in organizations, and their future plans. On the service providers' side, IDC interviewed large systems integrators, datacenter service providers, and managed BC/DR service providers. The objective of these interviews was to understand the challenges and drivers causing user interest in BC/DR. These discussions also sought to gauge customer maturity with regard to BCP implementation and assess how BC/DR is becoming an integral part of the BCP.

IN THIS WHITE PAPER

This IDC white paper explores various aspects of BC and DR, including customer maturity in terms of planning and risk management, key drivers for BC/DR services, the major challenges faced by organizations, and the options available to user organizations. Subsequently, we differentiate between BC and DR, and how they become part of an organization's wider BC plan. We then look at some of the key challenges that organizations face today with regard to BC and how DR services can help resolve them. Finally, we describe MEEZA's suite of BC/DR service offerings and their ability to address the needs of this market.

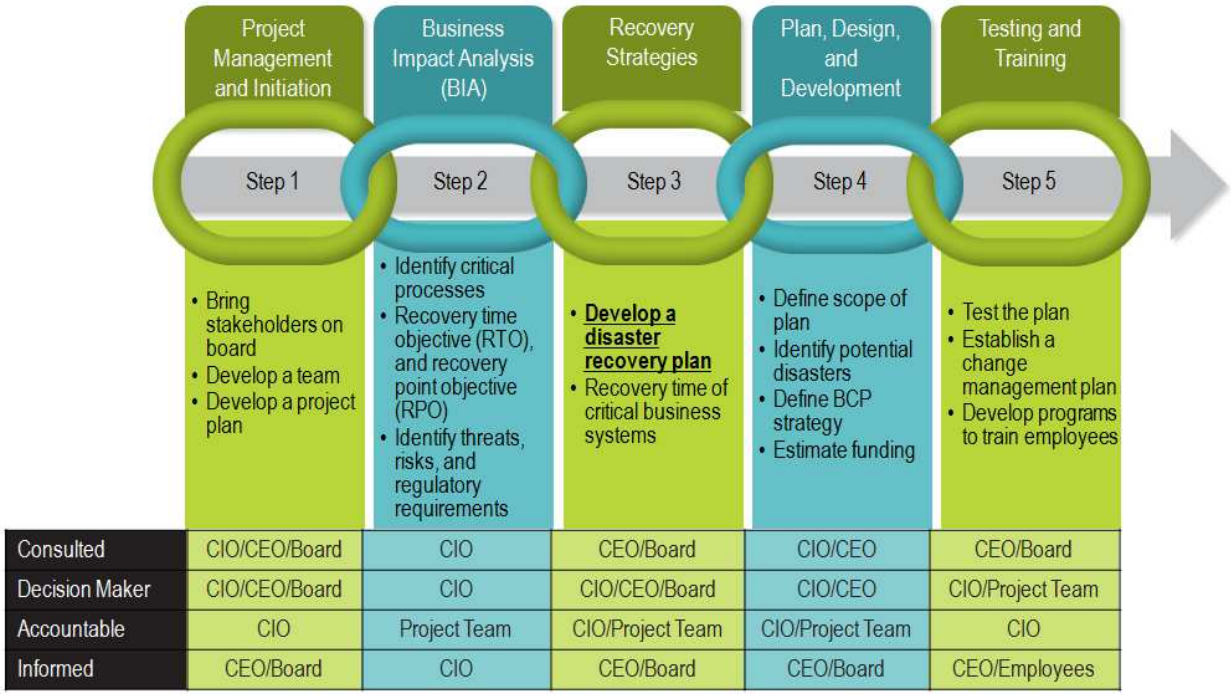
SITUATION OVERVIEW

Because disasters may strike at any time, businesses today are required to be constantly prepared for the worst-case scenario and strive to maintain uninterrupted business operation during times of crisis. The impact of a disaster can extend from a few hours to several days of outage, and it can directly affect employee productivity; brand image among customers, suppliers, partners, and the media; the quality of products and services provided; and sales and profitability (direct and indirect losses, cash flow, compensatory payments, and loss of revenue).

In recent years, disruptions have been frequent for businesses across the world. These disruptions have come in different forms, such as natural disasters, vandalism, terrorism, data loss and security breaches, systems and equipment failures, and power and communication line outages. The key question that organizations need to ask themselves is, "How prepared are we to maintain business operations in the event of a disaster?" The follow-up question to this should be, "How can we be prepared when we do not know what we should prepare ourselves against?" A comprehensive BCP has the capability to address both of these questions to a large extent. Such a plan, with strong DR measures, can go a long way toward ensuring that organizations continue business as usual, even if a disaster does occur. Figure 1 below shows the five steps to be taken in a BCP, as well as the stakeholders that should be involved and informed in each step.

FIGURE 1

The five (5) steps of a Business Continuity Plan and the Stakeholders to be involved and informed in each step



Consulted	CIO/CEO/Board	CIO	CEO/Board	CIO/CEO	CEO/Board
Decision Maker	CIO/CEO/Board	CIO	CIO/CEO/Board	CIO/CEO	CIO/Project Team
Accountable	CIO	Project Team	CIO/Project Team	CIO/Project Team	CIO
Informed	CEO/Board	CIO	CEO/Board	CEO/Board	CEO/Employees

Source: IDC, 2013

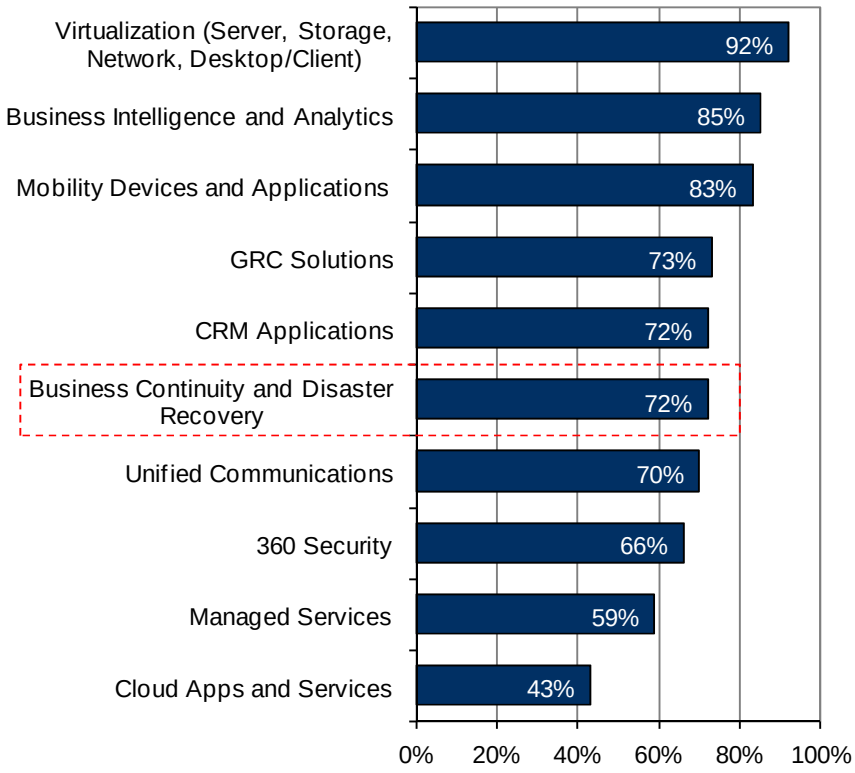
The first step is to bring the stakeholders on board to initiate planning. A Business Impact Analysis (BIA) creates the foundation for all subsequent steps; it is the most critical step, because it helps organizations identify their critical business processes and understand how various threats may impact them. Based on the BIA, the third step is the creation of a DR plan that takes into consideration the permissible downtime and recovery time of mission-critical systems. The final two steps center on defining and creating a BCP strategy, documenting it, testing the plan, managing change, and training employees. The DR plan and its implementation are highly critical to the success of BCP strategy.

Globally, the last decade has seen a considerable transformation in the way organizations build the necessary infrastructure for BC. More importantly, significant emphasis has also been placed on maintaining and regularly updating the BCP, as well as training employees. IDC research has shown increased interest and rigor from GCC organizations in this area. Some of the core drivers behind this change are natural disasters, regional political unrest, and global politics. Other factors, including increased media coverage, the increasing international exposure of regional organizations, and the increasing availability of DR services providers, have also accelerated the DR movement. Traditionally, mature verticals (banking and financial services, oil and gas, and aviation/transportation) have been most proactive in adopting DR. Banks, specifically, are mandated by their respective central regulatory bodies to have DR sites; as a result, they have traditionally been at the forefront of adoption. In general, DR has emerged in recent years as one of the top priorities of C-level executives in the region.

IDC research has shown significantly increased interest among CIOs in the region to make BC/DR investments. IDC findings highlight that 72% of the Middle Eastern CIOs surveyed intended to make BC/DR investments last year, compared to 48% the year before.

FIGURE 2

IT Investments Planned in 2012



Source: IDC, 2013

IDC believes that developing a BCP is largely a planning and consulting exercise, from understanding the relevant business processes and identifying those that are critical, to formulating a DR plan and implementing maintenance and training processes. Organizations must be careful in assessing their ability to undertake such an exhaustive and critical exercise on their own. If small skills gaps exist, or doubts arise over internal IT capabilities, organizations should ideally engage a consulting or IT services firm that can bring skills, expertise, and hands-on experience in BCP.

Differences Between Business Continuity and Disaster Recovery

BC/DR is evolving, particularly via the introduction of new technologies (e.g., virtualization, remote VPN) and new delivery options (e.g., cloud/utility services). The concept of Business Continuity Management (BCM) is expanding from its traditional model of stove-piped services (e.g., hot site, cold site, and data recovery) to a much broader definition. The widely accepted BS 25999 business continuity management standard was created to establish a uniform benchmark in good practice, and satisfy the needs of stakeholders (i.e., customers, clients, government, regulators, and business partners). The BS 25999 standard has formed the basis of many other BCM standards since its formation, including the newly introduced ISO 22301 and ISO

22313. The terms BC and DR are often used interchangeably, but they are different in terms of both policy and technology.

Business Continuity

In simple terms, BC is defined by the ability to maintain operations in the event of any disruption. BC acts as a means of providing any stakeholder (e.g., employee, partner, supply chain) with the appropriate resources for ensuring workplace productivity that includes access to business resources and applications that operate at or near 24/7.

BC differs from DR in that its focus is on people and the continuation of business processes, rather than just the availability of IT systems. BC formulates proactive measures to ensure business continuity as well as plans to manage the response to, and recovery from, a disruption. This plan would include mandates and detailed steps for the command team to coordinate and oversee the response, as well as sub-plans for the business units.

Disaster Recovery

DR includes a number of service elements that keep a business running in the event of a major incident or disaster. For the purposes of this white paper, DR is defined as a coordinated activity of recovering IT systems following the complete or partial loss of a site due to a disaster. The infrastructure used for DR can include virtualization, server and network hardware, networking, datacenter facilities, replication, backup to disk, backup to tape, and tape vaulting. While BC is measured in seconds, DR is measured in hours or days. However, depending on the technology deployed, recovery can be achieved far more quickly.

Drivers for Investing in Disaster Recovery

Two sets of broad drivers, direct and indirect, are causing businesses to ensure DR. The direct drivers relate to mandates and regulations imposed by various regulatory authorities. The indirect drivers stem from other external factors, including natural and man-made disasters, and directives from clients and business partners. The following are some of the drivers in the GCC for investing in DR:

- **Risk Management and Sustainability:** The core driver for organizations to invest in DR is risk management. Disasters can take any form and size, and awareness continues to increase among regional organizations. Natural calamities, as well as recent cyberattacks and security breaches in energy, media, and government organizations, are some of the most significant events that have led many organizations to reassess their DR plans. Interest is certainly greater in hedging against the risk of a potential disaster, not only among large organizations, but within the small and medium-sized business (SMB) segment as well. The volume of data and number of customers are directly proportional to the extent of any monetary and data loss a disaster can create for an organization. Any organization that deals with a large volume of data and large numbers of customers must have a strong and reliable DR strategy in place.

"For us and our industry peers, risk mitigation is the most critical driver for disaster recovery. An hour of downtime has serious implications on our business operations, employee productivity, and, most importantly, revenues." – major manufacturing organization, UAE

- **Compliance, Regulations, and Corporate Governance:** The banking industry is highly regulated. While global regulations such as Basel II and III are more guidelines related to governance, they do have specific mandates on data availability, driving banks to invest in storage, archiving, and data retrieval. Banks worldwide are required to comply with these regulations. Furthermore, the various country-specific central banks or regulatory bodies in the region have mandated DR sites. This is one of the major drivers, from a compliance perspective. In other verticals, including telecommunications and oil and gas, DR is driven by corporate governance, scale of business operations, bulk of customer information, and high data volume.

"In addition to operational continuity, compliance is the major driver for all the banks in the country. We have strict mandates from our central bank to have a DR site within the country. The central bank periodically audits our DR setup, and there are severe monetary penalties in case of failures" – major bank, Qatar

- **Loss of Reputation and Legal Liabilities:** The effects of a disaster are not limited to operational disruptions, since a domino effect can occur, extending to several other aspects of the business. A few minutes or hours of shutdown will prevent customer access (and, possibly, impact the customers' operations too), which may easily result in non-compliance with SLAs and trigger potential lawsuits and legal liabilities. Even a single such instance can tarnish an organization's reputation. The findings of this IDC research show that many more organizations are coming forward and evaluating DR solutions.

"We are a well-reputed organization in a highly competitive industry. Apart from revenue leakage and customer churn, our reputation is at stake; this is why BC/DR is a high-priority area for us. We have scheduled simulations and drills to ensure that our systems are functioning well around the clock." – major bank, Saudi Arabia

- **Executive Leadership:** Today's CIOs have arguably greater responsibilities and more accountability than their predecessors. Along with other C-level executives, they are responsible for ensuring that the organization is better prepared to continue operations in the event of a disaster. CIOs in the region are building strong business cases to acquire funds to implement BC/DR. Taking into account budgets, time constraints, current infrastructure and other factors, organizations are deciding on the most suitable DR model for them (i.e., dedicated DR, managed DR, or hosted DR).

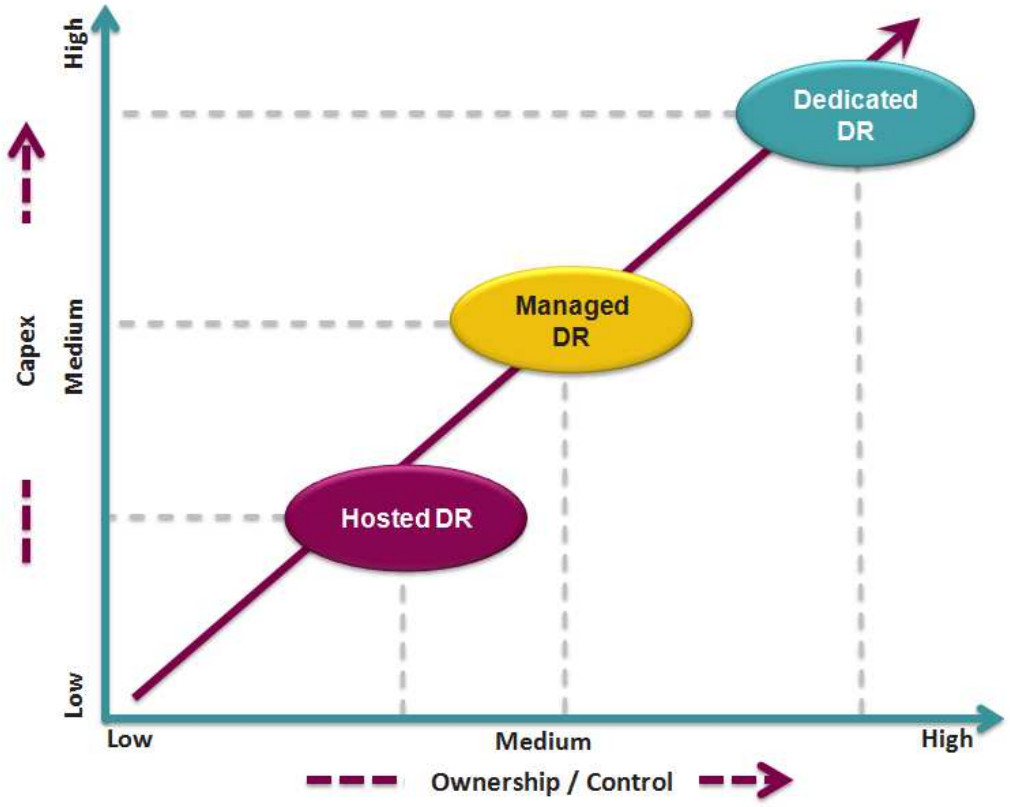
"DR is not an IT discussion anymore. Our top business leaders, as well as the executives on board, were actively involved when we were formulating our BCP and disaster recovery strategy." – major manufacturing organization, Qatar

Prevalent Disaster Recovery Models

Organizations have multiple options to address when it comes to DR. However, each model has its pros and cons. The decision to choose one of these models comes down to a combination of factors, including risk appetite, IT infrastructure, choice of applications and data to be put in the DR site, in-house IT operations capabilities, budget, and organization/industry policies on control over data. The figure below displays the three most prevalent DR models available, and the level of capabilities, expenditure, and ownership/control associated with each.

FIGURE 3

Prevalent Disaster Recovery Models



Source: IDC, 2013

- **Dedicated Disaster Recovery:** A dedicated DR site is one in which the operations and maintenance are run entirely by the organization to which it belongs. A dedicated DR site enables complete control over the data that is being replicated and archived, the frequency of replication, data security, storage, applications, and other important IT and network connectivity aspects.

  A dedicated DR model requires organizations to invest heavily in setting up an exclusive datacenter, which means releasing a request for proposal (RFP) from IT services providers, followed by vendor evaluation, negotiation, then the project

launch. This entire process can take a couple of months or more, depending on the organization. Some organizations stated that they had encountered long procurement processes and slow customs clearance for IT equipment. The other option is to perform the implementation in house. Once the DR is up and running and an infrastructure upgrade is required, IT teams often face the same obstacles again. The other key challenge in a dedicated DR model is keeping up with the latest technology and industry best practices, which are arguably provided more easily in an outsourced model.

- **Managed Disaster Recovery:** In the managed DR model, an organization commissions an external provider to operate and maintain its DR site. The datacenter or the DR site is still owned by the organization, but the day-to-day operations and maintenance are outsourced to an IT services provider. This model still offers a high level of control and ownership for the organization, while freeing it from maintaining personnel on its payroll and the hassle of operating the DR site.

  The time taken to establish a datacenter is typically the same for dedicated and managed DRs. Organizations that have outsourced the operations of their DR sites face challenges, at times, with the quality of service delivery. This could be due, in part, to inconsistent delivery standards and SLAs. Customers may not always be very clear about their expectations, and services providers are not always proactive in educating customers on what can and cannot be delivered. This sometimes causes unexpected surprises during service delivery.

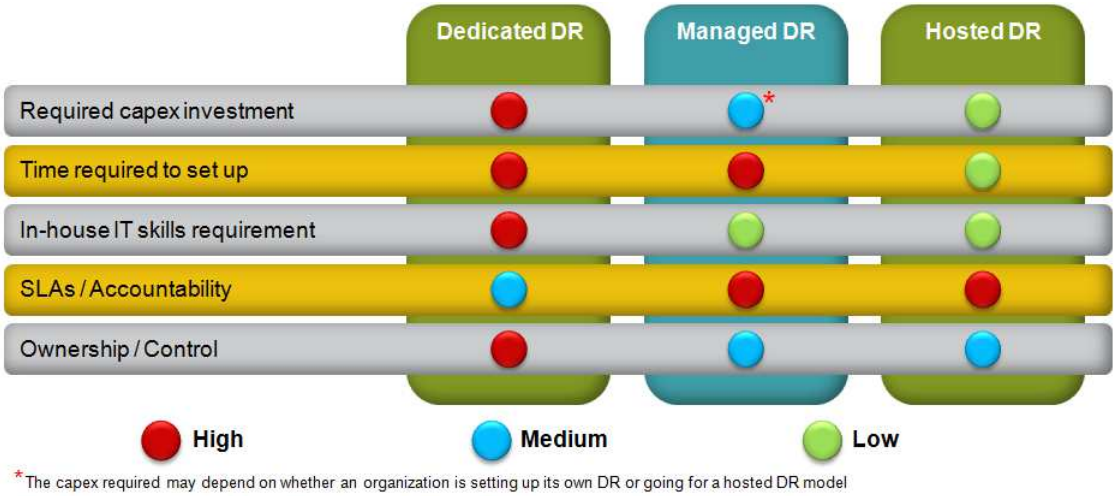
- **Hosted Disaster Recovery:** In the hosted DR model, a datacenter owned by the services provider hosts an organization's business-critical applications and/or data. The organization has the option to manage its own infrastructure, or to outsource the management to the services provider. In the simplest terms, it is a co-location setup that is used for DR purposes. The infrastructure and applications are owned by the organization, but the real estate, network connectivity, and power are provided by the services provider. The services come with a guaranteed uptime and structured SLAs.

  The time spent in getting the DR up and running is greatly reduced in a hosted DR model when compared to the other two models. Reasonable value exists in hosted DR in the form of faster time to go live, higher flexibility to scale up and down, access to the latest technology, and industry best practices. However, challenges pertaining to inconsistent service delivery standards and lack of mature and stringent SLAs prevail. Concerns also persist around relinquishing control of outsourced IT operations.

The figure below provides a comparison of the key attributes of the three discussed models.

FIGURE 4

Comparison of Prevalent Disaster Recovery Models



Source: IDC, 2013

All the above-mentioned DR models have their own value propositions. The dedicated DR model provides a sense of strong control and ownership of the infrastructure, applications, and data that are hosted by the DR site. The managed DR model provides infrastructure ownership with slightly less control over the operations and maintenance of the site, while the hosted DR model offers a mix of both, where the organization still owns the IT infrastructure and operations (one can outsource the operations as well) and the rest (i.e., real estate, power, cooling, and connectivity) is provided by the service provider.

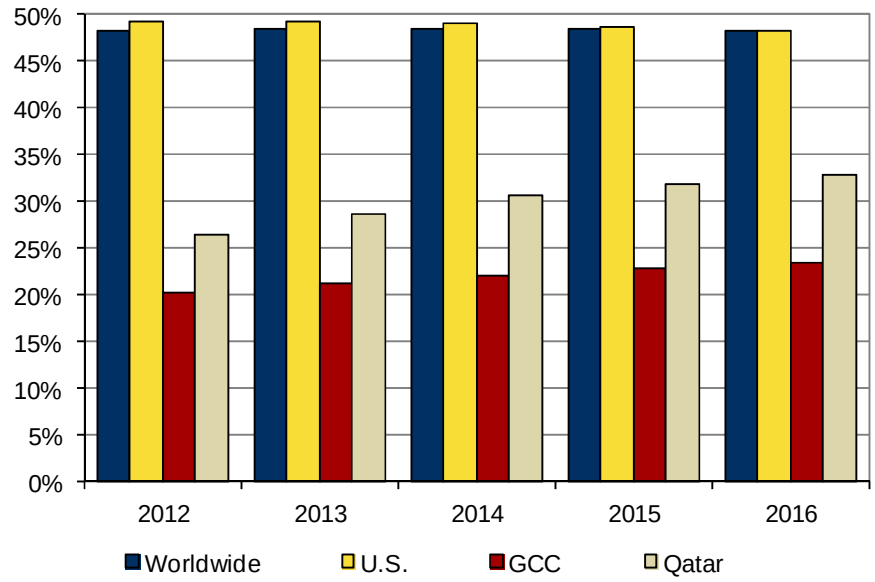
Implications for Managed BC/DR Services

It is a widely accepted fact that the adoption of outsourcing services increases as the market and customers mature; Western markets, including the U.S. and Europe, are an example. IDC believes that factors such as process improvement, best practices, higher efficiencies, agile processes, cost reduction, and faster response time will drive the adoption of outsourcing services in the GCC. Qatari organizations are also expected to embrace outsourcing at a faster rate than organizations in the overall GCC.

The image below compares the constantly increasing share of outsourcing services in total IT services across different markets. As demonstrated, the proportion of outsourcing services to total IT services in Qatar is expected to continue to increase until 2016. The overall GCC market is also expected to follow this trend.

FIGURE 5

Proportion of Outsourcing Services to Total IT Services, 2012–2016

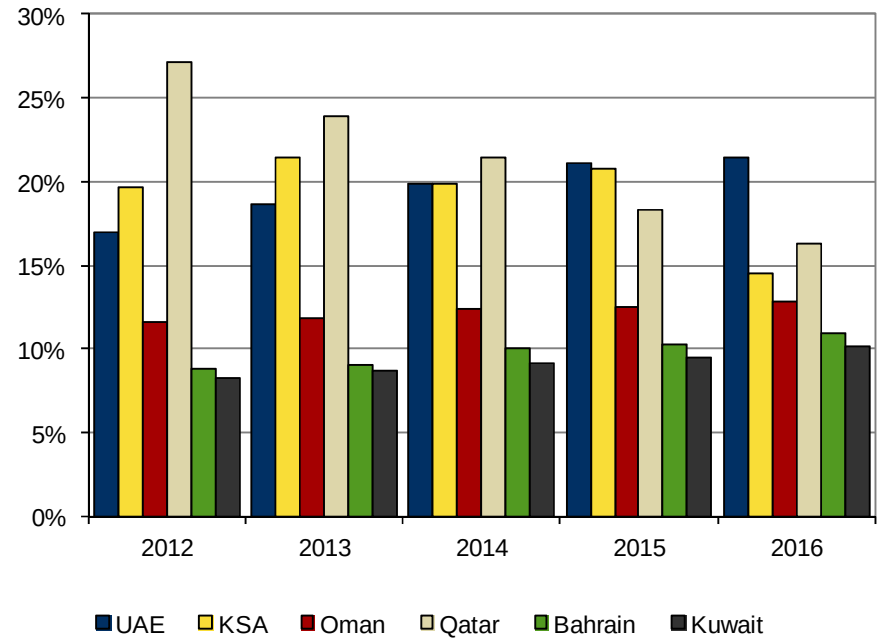


Source: IDC, 2013

On the back of the benefits discussed in the previous sections, managed BC/DR service is forecast to witness the fastest growth rate in the GCC.

FIGURE 6

Year-on-Year Growth of Managed BC/DR Services, 2012–2016



Source: IDC, 2013

ESSENTIAL GUIDANCE

No set formula exists for selecting a DR model, and an organization has to take various factors into consideration when formulating a BCP and DR strategy.

- First and foremost, get management buy-in and identify the stakeholders to become involved in the process of developing BCP and DR strategy.
- Identify and prioritize applications and infrastructure that are required to be in a DR environment.
- Evaluate DR models according to various attributes, including compliance and regulations, risk tolerance, budget availability, acceptable time to complete the project, outsourceability of applications and infrastructure, location of the DR site, and cost of ownership for the next 3–5 years.
- Incorporate stakeholder recommendations and obtain buy-in to finalize the most suitable DR model for your organization.
- Evaluate service providers according to their IT infrastructure, datacenter tier level, customer references, service delivery standards, pricing offered, site location, SLAs, and process and technology certifications

- Push for precise, well-defined, and measurable SLAs when contracting with a hosted and/or a managed DR services provider.

"We hosted our ERP application with our application vendor, at one of their datacenters. We weighed the option of setting up our own DR, but the time involved and the associated costs were too much, and impractical for our business. We are highly satisfied with our decision, as we have not had any downtime at all since we started hosting with our application vendor." – major manufacturing company, Qatar

IDC believes that service providers will continue to invest in providing BC/DR services. IDC also predicts that newer business models will emerge, such as collaboration between large customer organizations and IT services providers to offer hosted DR and managed DR services. These services will typically be branded under the customer organization's name, but the management and delivery will be performed by the IT services provider. These developments are expected to create more options for customers to choose from and improved service delivery standards.

The region's businesses are now moving away from keeping everything in house and are rapidly adopting the outsourcing models. IDC predicts that managed DR services spending will grow at a CAGR of 19.7%, 19.2%, and 24% for the UAE, Saudi Arabia, and Qatar markets, respectively, over the next five years.

MEEZA SOLUTIONS

MEEZA, a Qatar Foundation joint venture, is a provider of managed IT services in the Middle East and covers a wide array of vertical markets, including finance, government, telecommunications, oil and gas, healthcare, education, and manufacturing, with an end-to-end solution delivery approach. In addition, MEEZA is becoming a recognized Systems Integrator and continues to establish its expertise on Smart Cities.

MEEZA believes that its value proposition is built on taking over the day-to-day IT operations of an organization, thus allowing it to focus on its core business and leave the management of IT-related tasks to a competent managed IT services provider. MEEZA's managed services portfolio have the capability to address the changing needs of customers at the infrastructure and application layers.

MEEZA has Tier III certified datacenters located in Qatar; these are known as "M-VAULT" 1, 2, and 3. M-VAULT 1 was launched in 2008, followed by M-VAULT 3 in 2012; M-VAULT 2 was launched in Q1 2014. M-VAULT 2, located more than 30 kilometers from Doha, is one of the main pillars of MEEZA's DR solutions offering.

MEEZA has invested in IT governance to ensure consistency across its solutions portfolio and go-to-market model in terms of processes, value proposition, and quality and risk management. MEEZA has additionally adopted a number of industry standards that are vital, particularly for services providers that offer mission-critical solutions with less tolerance for data latency and service downtime. These standards include LEED Gold and Platinum certifications, and ISO 20000-1:2011. MEEZA is the first IT services and solutions provider in Qatar to be awarded ISO 27001:2005 and ISO 9001:2008 certifications. MEEZA believes that its proactive approach to certification, along with its built-in competencies, help the service provider to differentiate itself through its secure IT environment, adherence to uptime (99.98%), and consulting capabilities.

MEEZA offers a variety of services using its current datacenter. It continues to expand its services portfolio from hosting infrastructure and hosted application services to BC and DR services. It acts in a consulting capacity when addressing customers' BC and DR challenges. MEEZA's BC/DR offering is structured around four main pillars: identification of risks and business impacts, development of a BC/DR strategy and plan, implementation of a tailored BC/DR solution, and maintenance of the service through regular audits and BC/DR plan reviews.

MEEZA aims to expand its market coverage outside Qatar by making its managed services portfolio available throughout the Middle East.

CHALLENGES/OPPORTUNITIES

With different DR models in play, the challenges faced by customers also vary. Most of the dedicated DR customer organizations mentioned challenges concerning procurement, operations, and upgrades. Managed DR and hosted DR customers, meanwhile, face hurdles related to service delivery standards and SLAs.

While convincing potential clients of the value of managed and hosted DR models, service providers often face challenges in addressing customer concerns over the loss of control. This can be addressed better by bringing in more transparency on the existing datacenter setup, certifications, infrastructure, pricing, committed delivery standards, availability of skills, and IT security. More importantly, services providers should also strive to guarantee comprehensive, well-defined, precise, and measurable SLAs.

CONCLUSION

Disasters are inevitable, and organizations are recommended to have sound DR strategies in place to prepare for them. IT managers and CIOs who do not plan for disruptions put their organizations at unpredictable operational and financial risk. The increasing importance of BC/DR in IT decision makers' plans is reflected in IDC's 2012 Middle East CIO survey, in which 72% of the CIOs interviewed stated that they had planned BC/DR. It is important that CIOs lead DR discussions with their management teams and stakeholders and get their buy-in.

IT managers are evaluating different models of BC/DR models, including dedicated, managed, and hosted DR, on the basis of the investments and level of control. According to IDC research, managed and hosted DR are expected to gain traction in organizations. IDC believes that organizations are starting to realize the benefits of outsourcing, such as lower CAPEX, access to skills and the latest technology, industry best practices, and hassle-free operational management. Indeed, managed BC/DR services are expected to grow at a CAGR of 19% in the GCC and Qatar for the 2012–2016 period.

In summary, IDC recommends that organizations consider multiple factors, including initial investment, desired level of control over IT infrastructure, regulations and compliance, and internal IT skills availability when formulating a DR strategy and choosing a DR model.