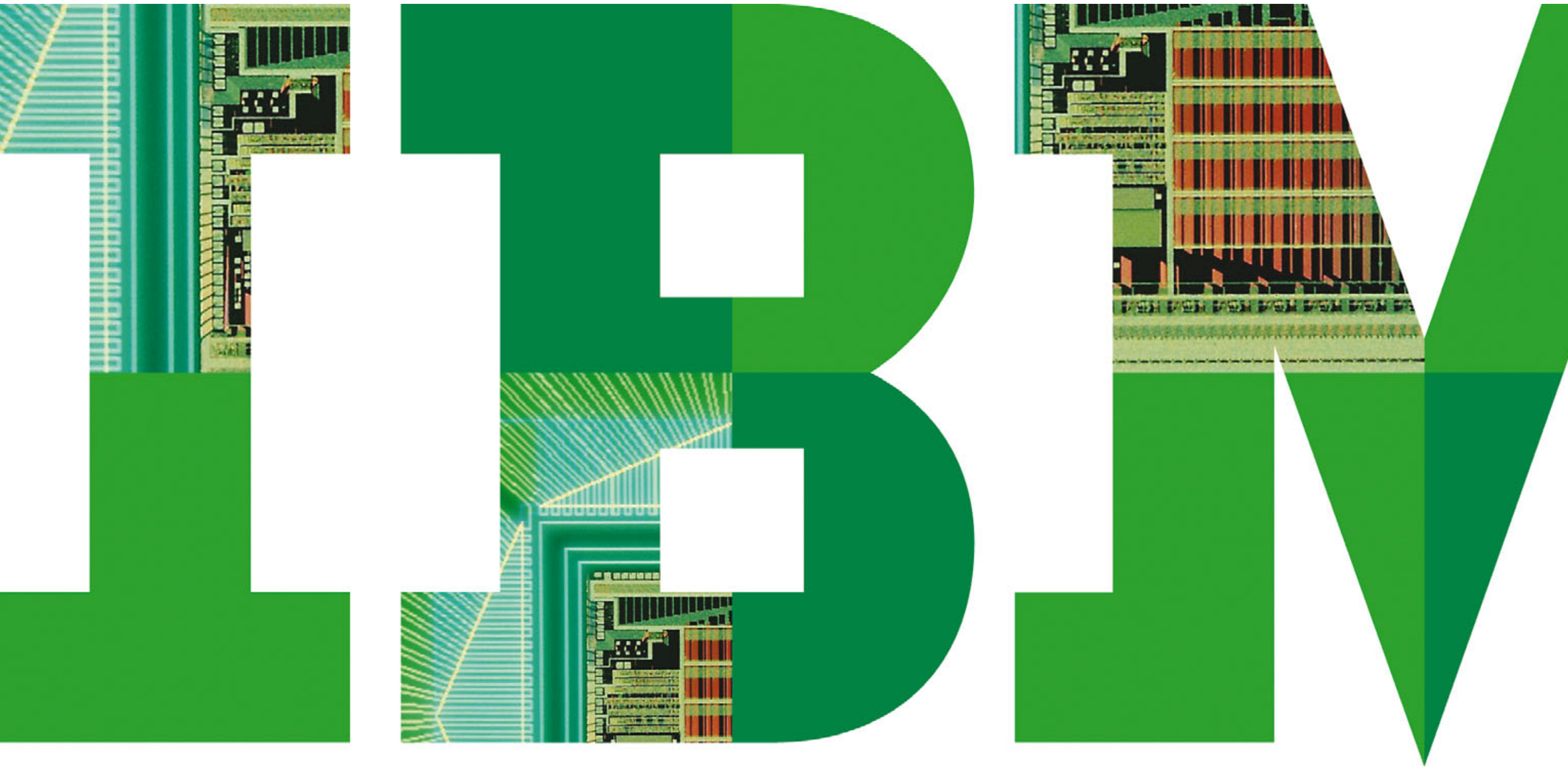
IBM Global Technology Services

Thought Leadership White Paper

August 2011

Developing an effective resiliency capability within a cloud design

Considerations for protecting the business and meeting processing needs



Contents

Executive summary

Cloud computing has the potential to change how organizations define, manage and deliver information technology (IT). It can help reduce the need to integrate new technologies in order to keep pace with growing server capacity demands, greater storage requirements and increasingly complex networks.

The capacity of cloud computing can be dynamically scalable to meet peak processing needs and to reduce consumption during off-peak times, thus enabling organizations to use technology more cost effectively. With either an existing Internet Protocol (IP) network or a series of dedicated high-speed lines, cloud computing can provide rapid access to resources and help drive efficiency, standardization and best practices while allowing the business to retain its customization and control capabilities. Such an elastic and scalable approach makes it possible to benefit from emerging technologies more quickly because the cloud provider is responsible for the design and integration of these new technologies. As a result, the organization gains greater information-processing capabilities to support its growing IT needs and can reallocate time, resources and money to more business-focused opportunities.

Cloud computing is evolving, so not all workloads are immediate candidates for cloud deployment. Your organization may still require a combination of traditional processing and extended, remotely delivered services. However, for many workloads, simply plugging into the cloud can provide access to an almost endless amount of virtualized resources to meet your information processing needs.

This white paper examines important considerations for effective resiliency program management within a cloud design. One crucial factor is how the new cloud-based design will impact your organization’s existing ability to protect underlying IT systems and critical applications, as well as the associated information and data requirements that support the business. Additionally, it is important to ensure that the cloud-based functionality allows for continuous processing across your organization to sustain business success.

Assessing resiliency requirements

The migration from a traditional processing capability with a somewhat static design to a more fluid, cloud-based initiative undoubtedly increases the level of resiliency needed to sustain business operations. To address these resiliency needs, your organization should first evaluate:

- Which workloads will be acceptable for processing outside of the traditional data center
- Whether cloud connection will be through the internal private network or through the public Internet
- The benefits and tradeoffs of using a public versus a private cloud
- Whether the cloud will include storage or computing services
- How distance might restrict how far the organization can place cloud content

To help ensure comprehensive business protection at the enterprise level, it is important to define an integrated approach to resiliency.

The next step is to conduct an assessment to help ensure zero impact to your business operations during the transition to cloud. This assessment also provides insight into how the existing architecture will impact your current design and helps to determine the potential impact, if any, as the delivery model changes. Critical areas to assess are:

- **Business functions.** Defining and mapping business functions helps to ensure that modifications will not impact your existing system access, application dependencies and cross-site communications that are critical to optimal performance.
- **Performance objectives.** You will need to revalidate service level agreements (SLAs), recovery time objectives (RTOs), recovery point objectives (RPOs) and security parameters for all critical and noncritical workloads that are candidates for cloud services.
- **System capacities.** To sustain complete business operations, you must have the necessary system capacities in place at all times (such as scalability, performance and throughput), and these should address both short- and long-term outages.
- **Information accuracy and integrity.** Ensuring consistent business operations is critical at all times, but it becomes increasingly important as your organization introduces flexibility into the overall environment. The ability to quickly move workloads through automated processes puts a greater focus on how information is handled relative to data currency, synchronization, availability and secured access.
- **Validation of the capability.** This is an ongoing concern because the rapid change associated with the combination of physical and virtual resources results in more frequent modifications to the environment that are also more fluid in design.

To help ensure comprehensive business protection at the enterprise level, it is important to define an integrated approach to resiliency. Avoiding multiple or conflicting approaches resulting from piecemeal strategies is particularly critical if you are considering a combination of traditional and cloud capabilities.

In most instances, you will need to revalidate and redefine each of the critical assessment areas to maintain resiliency across your organization. Identified changes should be validated immediately upon introducing the modifications into the overall environment to prevent or reduce the impact that an adverse event might have on business results. This is where a well-defined resiliency strategy proves vital.

Developing a cloud-based strategy

An important first step in establishing a resiliency strategy within a cloud design is developing a detailed breakdown of the mandatory components of an effective program. Thoroughly reviewing your current resiliency program allows you to determine how you will need to modify existing capabilities to adapt to changes in the production environment when moving to a cloud-based design. Figure 1 depicts the components of a resiliency program.

Once you have established the crucial resiliency components of the program, you must then consider how to incorporate recovery into your design. Critical questions to ask include:

- What are the cross-platform requirements and challenges?
- How will backups be processed, and where will they be stored?
- From a data standpoint, what are the recovery objectives (RTOs and RPOs)?
- How will recovery processing be performed?
- How will these cloud components be integrated into the overall resiliency program?
- How will the design be validated? (How frequently will it be tested? At what scale?)

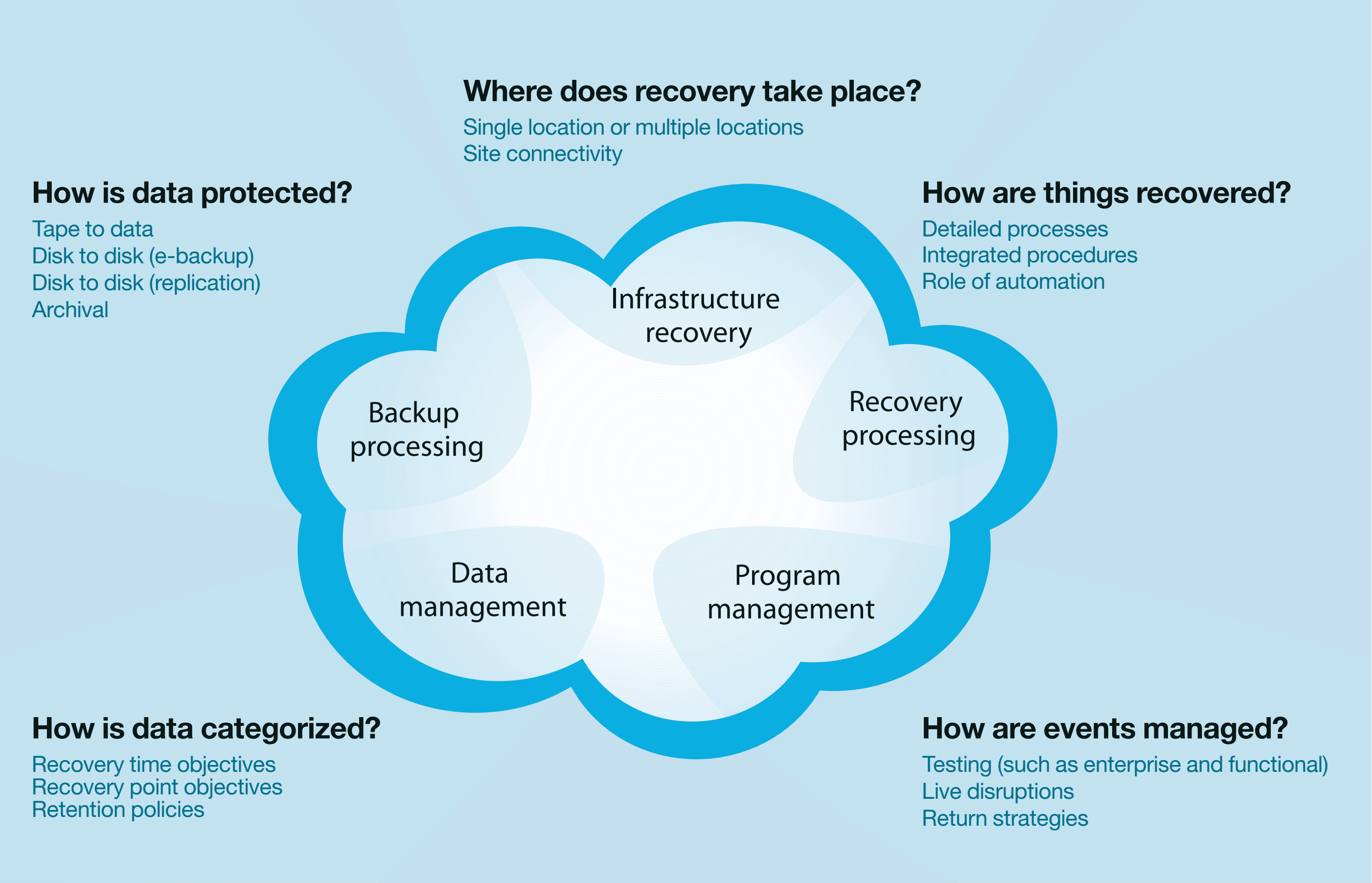


Figure 1: Components of a resiliency program

In-depth resiliency analysis

When detailing the design of a cloud-based resiliency program, you will need to look at several variables that are critical for processing end-to-end business transactions. First, you must consider how to position key applications and supporting information. Additionally, you must determine your server capacity and throughput needs, as well as identify distance limitations for data synchronization and transfer. Another key variable is how you will address cross integration of heterogeneous platforms to ensure seamless processing. Finally, you will need to be certain that the new program will not impact your existing service levels. A detailed analysis that looks into the following areas can help address these issues.

Defining the infrastructure for cloud must take into account the numerous challenges associated with cross-platform integration.

Business functions

A thorough evaluation of all of the business functions is the first step in determining which workloads may be candidates for cloud computing. An analysis of the detailed process flows ensures that you have identified each process relative to the inputs, outputs and dependencies (both internal and external) needed to meet your business objectives.

Service level objectives

One of the most critical success factors in the deployment of any cloud implementation is keeping the existing service level objectives intact. You must manage the requirements for continuous and high-availability SLAs, as well as business resumption metrics for RTOs and RPOs, in accordance with existing agreements so that your business remains protected from any adverse event that could interrupt production operations. These metrics should be reviewed and validated during both the business functional assessment and detailed technology blueprint analysis to ensure a consistent cloud design going forward.

Technology blueprint

The next step is to define and analyze the technology blueprint for all of the system, data and application components that correspond to the associated business processes. This analysis provides information about the options that will be in place to effectively position the supporting infrastructure for both in-house and remote cloud processing. The organization must take into account adequate processing capacity, positioning of systems and data, and the integration of multiplatform technologies when redesigning the current production environment.

Documented connectivity requirements

Once you have defined the combined infrastructure—local production and remote cloud—you must identify the detailed networking requisites. Data transfer abilities need to focus on application latency considerations along with bandwidth sizing for both peak and off-peak processing. System and application connectivity considerations should include remote operations and end-user access for both internal and external entities, as well as monitoring and management functions in support of operational status and reporting capabilities.

Parameters and metrics for validation

Validation of the newly defined resiliency capability requires that detailed objectives are identified by a combined effort involving the business functional areas and the IT community. Testing scenarios must focus on achieving business results that are delivered according to documented parameters, with specific metrics used to evaluate the accuracy of the resilience capability during period exercise events.

Recommended design principles

Implementing identified design criteria not only facilitates an effective design, but can also ensure that an ongoing resiliency capability will remain in place to protect the business as the cloud capability takes form and continues to evolve. Standardization and consistency are critical to verifying that business protection, data integrity and overall enterprise-level protection strategies are in place to support the underlying IT resources of the future integrated cloud design.

Defined workload dependencies

A criticality analysis is often a direct output of a business impact analysis and will reveal the detailed dependencies from a systems, application and data perspective. This helps determine how work is flowing throughout your organization. Without these linkages, it is essentially impossible to determine the impact of an outage as it relates to the combined environment of a virtual, cloud-based infrastructure.

Mapped access to systems and data

Leveraging the infrastructure blueprint is a crucial component for architecting a clear view of the operational requirements needed to execute business transactions. This analysis will serve as a cornerstone for the eventual architecture that you will implement, ensuring performance and consistency across the applications environments to drive seamless business operations. Technology decisions will be based upon this analysis, providing the detailed resource requirements from a capacity and functionality perspective.

Verified connectivity to all virtual processing sites

Connectivity will play a critical role in the outcome of your cloud processing environment. In addition to the day-to-day operational characteristics, it is important to design a network that is flexible with full redundancy and dual pathing to avoid any single points of failure that may compromise production operations. From a resiliency standpoint, the same holds true for the additional requirement of connecting any-to-any from all production sites to all recovery sites at any given point in time.

Defined information accuracy and integrity (RTO/RPO)

Yesterday's challenges of cross-platform recovery, whereby systems and data are dissimilar and synchronization is a major concern, may be exacerbated when attempting to recover multiple systems across multiple locations within a cloud design construct. More specifically, if business functions are split across sites using a combination of traditional processing and cloud design, determining the common synchronization point may be much more difficult. You will need to coordinate backups over distance, whereas in the past, these same backups were done within the same site with the same operations staff. Documenting recovery objectives will become increasingly more important as the ability to restore systems and data becomes more fragmented.

Scoped performance and throughput

Any component of the environment that is recovered during an event must maintain the equivalent production environment characteristics needed to sustain business resumption. This includes maintaining all aspects of processor and storage performance, decreasing all application latency and providing optimal end-user access speed to avoid impacting the ability to deliver agreed-upon service level objectives. Each of these processes is critical to resuming operations as quickly as possible and reducing the growing backlog that you will encounter during any prolonged service interruption.

Defined and documented business resiliency objectives

Defining discrete testing and validation objectives will help your organization meet its resiliency requirements. A detailed business impact analysis, accompanied by a formal risk profile, will reveal those areas that you will need to exercise periodically to ensure that you have achieved complete business resiliency.

Conclusion

Your cloud implementation must allow for continuous processing of transactions that enable business success, regardless of where your systems, applications or data reside. Business resiliency should be an inherent attribute within the fabric of the cloud design and, as such, needs to be part of your critical design efforts.

It is important to gain a detailed understanding of how cloud computing will be delivered and to review how you established the current resiliency strategy to protect your business. Many questions must be answered relative to how the new design will modify the existing strategy, taking into consideration several key recovery disciplines.

This knowledge serves as the baseline for further assessment of how changes to the production environment will impact the ability to continue delivering optimal service in support of business needs. From an implementation standpoint, identifying a structured set of design principles can help guide this effort. Focusing on standardization and consistency not only establishes the initial effort, but also serves as a framework for future cloud enhancements.

For more information

To learn more about effective resiliency within a cloud computing environment, please contact your IBM marketing representative, or visit our website: **ibm.com**/services/continuity

Additionally, IBM Global Financing can help you acquire the IT solutions that your business needs in the most cost-effective and strategic way possible. We'll partner with credit qualified clients to customize an IT financing solution to suit your business goals, enable effective cash management, and improve your total cost of ownership. IBM Global Financing is your smartest choice to fund critical IT investments and propel your business forward. For more information, visit: **ibm.com**/financing

IBM Global Services
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
August 2011