IBM Global Technology Services
June 2009

Expanding and enhancing risk evaluation strategies for better data protection.

Contents

Executive overview

Traditionally, organizations have evaluated the need for business continuity programs by trying to determine how adverse events could impact processes and create financial exposure. This approach has not changed; it still has merit today. But today, this method provides only the most basic steps. Now, organizations must expand the traditional approach to create a program that includes continuous enhancements to their continuity capabilities. Central to this approach is the need to evaluate how business and technical options can be leveraged to improve information availability and drive greater resiliency across business and IT functions.

Stepping beyond traditional resiliency evaluation techniques is necessary for a key reason—there is more at risk today than ever before. An organization now must be able to provide continuous service and support to its customers, suppliers, stockholders and stakeholders if it is to remain in business. And the risks that can interrupt business are increasing in number and frequency. Awareness of the likelihood of a business outage — and the damage that an outage can bring—has been greatly elevated as a result of widely publicized disasters such as hurricanes, power outages and terrorist attacks.

One source of protection is technical—the manner in which technological capabilities are used to enhance the resiliency of business processes and IT resources. Technology today provides an increased focus on infrastructure design, with a concentration on the companies' needs to maximize continuous availability of information—while enhancing their capacity to respond to events that could disrupt business operations.

Highlights

However, any change to an organization's underlying support infrastructure requires substantial time and investment spent evaluating the technology and logistics of recovery. Organizations must determine the impact such a change could have on their overall risk profile, the ongoing need for information availability, the demand to meet growing regulatory requirements, and the imperative to integrate and align business requirements with IT capabilities.

In determining these potential impacts and evaluating a strategy for recovery, organizations must ask critical questions:

- *What are the guiding principles involved in determining a recovery design?*
- *What options are available for implementing a recovery solution?*
- *What variables should be considered when evaluating alternatives?*

Developing a business continuity and recovery plan requires a top-down view of business needs and IT capabilities.

Determining the key factors in a recovery design

Developing a continuity and recovery plan requires an integrated, holistic view of an organization's business needs and IT capabilities—with an eye toward determining the critical success factors needed to design and develop the solution. Such a view should be developed from a top-down business perspective. It should examine not only the IT function, but also:

- *Business requirements—including a risk analysis and a business impact analysis*
- *The integration of business requirements into the technology roadmap—including whether leading-edge or established technologies are the best fit for meeting an organization's needs*
- *Geographic considerations—including the impact that an urban or rural location may have on an organization's vulnerability to risks and ability to recover*

Highlights

- *The regulatory environment—including demands for a quick recovery that may be required by a highly regulated industry or the amount of guidance available from regulatory agencies*
- *Industry posture and position—including leadership status and competitive positioning that the organizations must maintain in the face of a disruptive event*

In taking this holistic view and developing an integrated recovery design, organizations should also examine a number of detailed requirements that may affect its recovery design.

Financial concerns

To help ensure that the long-term cost of recovery is accurately depicted, an examination of the financial basis for changing the recovery strategy should consider all relevant elements. Many organizations, for example, identify initial costs only at a high level without considering the underlying costs of implementation and ongoing management. Such an oversight can result in a solution that is unexpectedly expensive and challenging to deliver.

The financial case for a recovery strategy must include implementation and ongoing management costs.

The financial case for change must consider ancillary factors that may affect the decision process. These can include the cost of an outage, the lost opportunity associated with misdirecting recovery investments to protect noncore business rather than to safeguard more critical revenue-generating functions, and the potential impact of using valuable resources for recovery that otherwise could be used to enable future infrastructure growth.

Highlights

A hybrid insourcing/outsourcing recovery model may be the most effective way to mitigate disaster risk.

Increased risk profiles

Any plan for enhancing or modifying recovery initiatives must examine specific risks to the business. But given the frequency and range of events that have caused disruptions recently—hurricanes, tornadoes, tsunamis, fires, floods, terrorist attacks, blackouts and computer malfunctions among them—the question may more properly address *when*, rather than *whether* or *what*, disruptions will occur. A risk plan must be designed to protect against any outage that could compromise business results. It must focus more on defining a resilient strategy to protect the environment from failure—instead of trying to predict which type of event may occur.

Options for guaranteed access

During a recovery event—whether an organization is conducting an exercise or responding to an actual outage—the recovery solution must allow continuous access to facilities and resources, whether primary or backup. It is important to decide early in the evaluation process how access will be provided. The two most popular models—insourcing or using an outside vendor—present their own unique challenges.

Insourcing requires duplicate resources that an organization must fund, maintain and manage at all times. The outside vendor model, which uses resources that are shared among a number of companies, poses concerns regarding the vendor's ability to handle multiple clients in the event of a regional disruption.

Both models face performance and security challenges. Today's demanding risk mitigation strategies increase the requirements for recovery program testing and require more effective guarantees of success, in the case of a disruption. Therefore, a third solution that should also be

Highlights

examined is a hybrid recovery solution. Hybrid solutions leverage both insourced and vendor infrastructures to create perhaps the most effective alternative to mitigating risk and ensuring continued operations.

To justify the cost of a mixed recovery option, organizations must identify and prioritize the workloads of the hybrid solution. This cost justification should entail a detailed analysis of business recovery requirements. The results of this analysis can contribute to determining the ultimate recovery design, its location and its optimal configuration.

Recovery time and recovery point objectives

Today's competitive business environment demands that organizations can rapidly recover from a disruption and, at the same time, ensure the integrity of recovered data. A complete recovery solution must meet increasingly stringent recovery time objectives (RTO) and recovery point objectives (RPO).

Successfully meeting time and point recovery objectives means dedicating infrastructure monitoring and management resources.

Successfully meeting these objectives requires that organizations dedicate an increased amount of infrastructure to monitoring and managing the recovery. A robust recovery infrastructure utilizes electronic media for data transfer between the production operations and recovery sites, while providing dedicated assets that are always available to resume processing for critical business functions.

Several options for providing this infrastructure should be evaluated, including an internal approach, a vendor approach and a hybrid approach. The evaluation should identify critical business process requirements and design solution alternatives—uncovering advantages and disadvantages to each approach. Organizations should

Highlights

examine these pros and cons in the context of the overarching recovery design in order to help ensure the solution's ability to meet business and IT requirements.

Industry-specific compliance guidelines and best practices can help strengthen resiliency.

Regulatory considerations

While not all industries impose established regulatory controls that govern recovery capabilities, many offer compliance guidelines that can help organizations ensure their viability. Some industries such as finance, the public sector and healthcare offer specific guidance in structuring individual recovery strategies, which organizations can integrate with other strategies to strengthen their resiliency. Companies in industries for which no specific direction is offered can benefit from reviewing best practices that have evolved to enhance recovery programs.

A detailed inspection of enterprise site options should be made to determine the best location for a recovery solution.

Examining the site options for implementing a solution

Once an organization has reached a better understanding of the key drivers of its recovery strategy, it should conduct a detailed inspection of site options. This inspection should be designed to determine the location where it would make the most sense to implement a recovery solution.

The inspection should include a review of internal facilities, such as a dedicated second data center or shared processing facilities, a vendor location providing dedicated or shared resources, and a hybrid vendor/internal solution in which some capabilities are provided in house and other capabilities are provided externally.

Highlights

Each recovery solution model has its own set of challenges that must be addressed to support success.

Internal

Many organizations implement internal recovery solutions for highly critical workloads. These solutions require a fully redundant design that can provide complete operational capability; they typically include processors, storage, channels, switching, data management and fully redundant, stand-alone networks. Such internal solutions are usually driven by the need for infrastructures that support availability and recovery within a geographic region. However, the organization must also provide some form of recovery capabilities to protect the business in the case of regional outages. These could involve out-of-region data storage, additional recovery infrastructure, and availability of skilled personnel to assist in the recovery from a wide-scale outage.

Vendor

Vendor solutions focus on providing a streamlined infrastructure and enhanced data availability in order to directly challenge the cost models currently being used by many organizations to justify internal solutions. Vendors are expected to continue to define options that augment internal solutions for fully implemented, in-region recovery. However, the vendor model faces the growing need for flexibility of test time, the need for guaranteed access to resources and data in a disruptive event, and increased cost pressures facing IT overall.

Hybrid

The greatest opportunity to define a fully functional recovery capability may lie in leveraging both internal and vendor resources—facilities, infrastructures and skills, for example—to protect data and operations from a regional event and drive recovery. The aim of this approach is to determine and prioritize business functions—starting at the process level,

Highlights

Each recovery option requires thorough business, IT and financial analysis in order to be judged quantitatively.

including examination of application tiers, and concluding with the supporting IT infrastructure. This prioritized strategy is crucial in determining the correct mix of people, processes and technology and the optimal mix of internal and vendor resources for the recovery solution.

Considering business and technical variables in the evaluation of recovery options

In determining the variables to use in an evaluation of recovery options, it is important to consider both business and technology factors. Organizations must evaluate the technology to be deployed, the manner in which the technology can support business drivers and regulatory compliance, and how well the technology can enable increased availability to ensure that the solution is designed for business results.

For each factor, the effort should analyze more detailed elements, including business system design, identification of technology components required for the solution, requirements for RTOs and RPOs, options for backup media format—usually tape or mirrored storage—and geographical concerns, such as whether the recovery operations will occur in or out of the organization's home region.

The result of this effort should be a matrix that provides the technical approach, a financial perspective, levels of operational complexity, recovery time and recovery point objectives, an overall risk assessment and a staffing plan. Once defined and assessed, this information can be ranked against the various recovery alternatives.

Highlights

Technology options, each with its own costs and benefits, should be thoroughly analyzed and reviewed.

Technical approach

A range of technology options should be considered in selecting a recovery solution. Considerations should include the type of recovery (including manual tape, electronic data transfer or disk mirroring), the recovery site (for example, internal, vendor or hybrid), and the type of support that will facilitate operations of the recovery site (for example, internal resources, vendor resources or hybrid resource pools).

Each technology option may provide variations of recovery types, sites and support features—each with its own associated benefits and costs. For example, one alternative might include a manual tape design at a vendor site using vendor resources. Another alternative might include an internal tape located at an internal site supported by internal resources. Further analysis of site options should be undertaken once the recovery alternatives have been evaluated and reviewed.

Consider both direct and indirect costs when analyzing the financial implications of a recovery solution.

Financial perspective

The initial financial analysis must be built on the understanding that the cost of the recovery solution must relate to its ability to support business requirements. Costs should be broken into two categories:

- *Direct costs—include expenses related to facilities, technology, networks, headcount, hardware or software maintenance and software licensing.*
- *Indirect costs—include costs incurred by gaining access to appropriately skilled resources, performing technology refreshes designed to ensure compatibility with changing production environments, devoting space to recovery facilities rather than to revenue-generating activities, and allocating funds to recovery that otherwise could be used for business purposes.*

Highlights

Protecting the integrity of the recovery environment requires established staffing, workload and availability agreements.

Operational complexity

An evaluation of the complexity that the recovery system may introduce into the existing environment should include:

- *Monitoring and managing of the environment*
- *Assurance of complete redundancy and diversity for the supporting infrastructure and networks*
- *Consideration of cross-technology integration*
- *Data synchronization within platforms and across platforms*
- *Consideration of the growing need to provide dedicated skills and resources to support day-to-day operations, recovery testing and management of a disruptive event*
- *Awareness of the level of complexity that may be caused by the need to test recovery operations without impacting the production environment*

If the proposed recovery environment will be used for functions other than recovery—test and development, peak load production or data mining, for example—agreements that protect the recovery configuration and strategy must be developed. These agreements may include:

- *How nonrecovery workloads will be migrated during recovery events*
- *How the integrity of the recovery environment will be maintained*
- *How the availability, capacity, growth, performance and technology refresh of the recovery configuration will be protected*
- *How detailed system testing will be maintained as a priority*
- *How staff assigned to normal IT functions will be utilized during recovery events such as preparation, testing and cleanup*

Highlights

Analysis of recovery time and recovery point objectives must go beyond financial considerations.

Many times, the recovery environment defined at the beginning of the design and implementation stage may be compromised later, as business and IT functions take over the infrastructure for other uses. This often occurs as a means of justifying the expense of the recovery design with respect to the overall IT budget.

Recovery time and recovery point objectives

In an analysis of the need for enhanced RTOs and RPOs, key factors must be examined in order to help ensure an equitable comparison of cost structures and capabilities for internal, vendor and hybrid solutions —and to justify the preferred solution. These costs and capabilities can then be compared and ranked according to their ability to deliver the required results.

In addition to the financial perspective described above, key areas of focus should include analyses of:

- *Critical business functions and subsequent mapping to applications and technology*
- *Physical proximity of facilities–examining tradeoffs in technology that may be required by distance and data loss that may be introduced by latency*
- *Resources and skills required to monitor and manage data transfer*
- *Ability to scale the solution to support complete production operations*
- *Need to refresh technology when upgrades are made to the production environment*
- *Availability of personnel to reconfigure the environment and resume IT operations when a disruptive event occurs*

Highlights

Overall risk assessment

As the types and frequency of events that may compromise an infrastructure continue to increase, so must the strategies that protect the business. Increased risk will drive the need for more dedicated infrastructures, duplicate online data and fully redundant networks.

Continual analysis of the recovery strategy and spending will help keep costs in line.

In order to help bring costs in line with the perceived business benefits of an enterprise recovery program, it is necessary to continually evaluate the existing recovery strategy and review spending, and return on investment and recovery capability. Ongoing evaluations must take into account the ability of the recovery strategy to ensure continuous business processing. And assessments should be tailored and repeated as business needs change.

Staffing

Designing, implementing, managing and testing a recovery solution require adequate resources with unique technology and business process skills. It is, therefore, paramount that headcount planning be an integral part of the recovery solution analysis. A duplication of existing skills may even be required to build and manage the desired environment.

Staffing and skills can be a point of failure.

It is also important to remember that technical skills can be a single point of failure in an organization's ability to test availability and recover from a disruptive event. Resources are often assumed to be allocated in the business case—but their omission can result in unreasonable expectations and workloads for the existing staff. The result can be an environment made unrecoverable by daily business support requirements. If adequate staff is not provided, normal functions such as IT production operations, systems maintenance, application development, testing and quality assurance can leave even the best-planned recovery program poorly maintained, ill-prepared or even forgotten.

Highlights

Recovery solution analysis must be quantifiable in order to compare the relative value of each option.

Analyzing the alternatives

Once an organization has identified the key factors for determining its optimal recovery design, reviewed the options for implementing a solution, and considered the variables for evaluating those solution options, it should conduct a detailed analysis in order to evaluate the alternatives and refine a recommended solution.

An example of how this may be accomplished is represented in the diagram below. This chart demonstrates an approach to quantifying recovery options using discrete criteria and a review of the variables—technology approach, cost, complexity, recovery time, recovery point, staffing and risk. The evaluation of each criterion may be assigned a numerical value, and those numbers may be totaled in order to rank the criterion's overall strength.

Recovery options	Tech approach	Cost	Complexity	Recovery time	Recovery point	Staffing	Risk
Vendor shared	Tape recovery	low	high	high	high	medium	medium
Vendor dedicated	Mirrored disk	medium	low	medium	medium	low	medium
Internal	Duplicate inf.	high	high	medium/low	medium/low	high	low
Internal	Workload shed	medium	high	medium/low	medium/low	high	medium
Internal	Active/active	high	medium	low	low	high	low
Hybrid Int/Vend	Mirrored/tape	medium	medium	medium	medium	medium	medium
Recovery outsource	Redundant ops	medium	low	low	low	low	low

Legend: High = 10, Med = 7, Med/Low = 4, Low = 1

Each variable should be reviewed against each recovery option to determine the relative value it brings to the overall solution. A set of metrics or success criteria may be developed to evaluate options and help ensure equity across alternatives. Each approach should give adequate consideration to the organization's unique underlying drivers for business recovery.

Highlights

A detailed analysis of requirements, options and variables, coupled with ongoing measurement, helps ensure success.

Conclusion

The bottom line is that the decision should not be driven by any single factor. An organization's move to change its recovery strategy may be driven by the availability of a second site, the end of a current vendor recovery contract, a perception that the rest of the industry is pursuing a certain course of action, or the belief that the value of one strategy from a certain source far outweighs the value alternatives.

Regardless of the reason, however, determining the best approach to changing a recovery strategy requires the inclusion of specific features—a detailed analysis of business and technical requirements, an understanding of the options that are available, and a deep inspection of the many variables that will support the ultimate strategy. Lastly, based on the business requirements for the recovery program, grading and success criteria must be established and implemented. Such a system of ongoing measurement and enhancement can help ensure that the new recovery program unfailingly meets the organization's identified business needs.

For more information

Visit **ibm.com**/services/continuity to learn more about continuity and recovery, or contact your IBM representative or Business Partner.

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

Produced in the United States of America
June 2009

BUW03012-USEN-00