Best Practices in Business Continuity Planning

U.S. Symposium/ITxpo 2001

Donna Scott
William Malik

7–10 May 2001
Colorado Convention Center
Denver, Colorado

56 Top Gallant Road
P. O. Box 10212
Stamford, CT 06904-2212

Conclusions

- An increase in e-commerce-related risk broadens the scope of business continuity planning.
- E-commerce drives increased requirements for continuous availability and shorter recovery times and points.
- E-commerce is transforming the market for business continuity services.

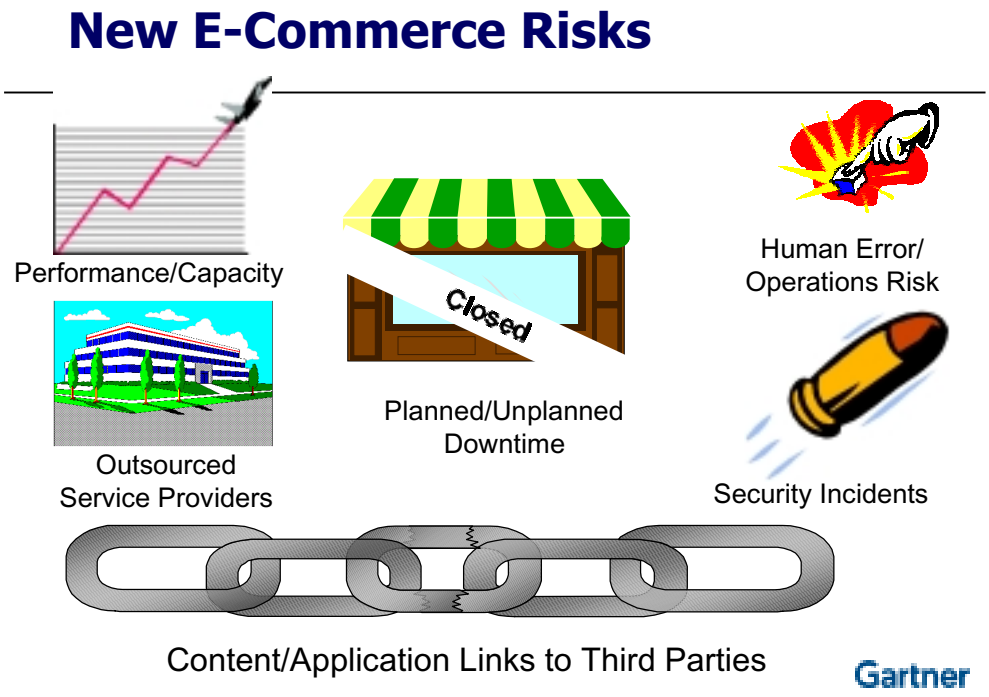
Gartner

Source: Gartner Research

Over the course of the 1990s, traditional IT disaster recovery evolved into a critical component of business continuity planning which has the larger goal of ensuring resumption and recovery of end-to-end enterprise business processes when disaster strikes. In the mid to late 1990s, as technology became integral to the business processes themselves, enterprises began to realize that traditional disaster recovery plans with 72 hour recovery periods were not good enough — in fact, for many, a 72-hour outage of critical business processes would seriously damage the enterprise and potentially affect its economic viability. As a result, enterprises instituted shorter recovery time and point objectives, often between four and 24 hours. The evolution toward e-business has resulted in yet another discontinuity affecting business continuity planning requirements. First, for many e-businesses, a four- to 24-hour site outage would cause irreparable damage to the enterprise; consequently, many enterprises are incorporating business continuity planning into their application and technology architecture designs — and building-in continuous 24x7 availability. Second, the risks are greater with e-business, so the BC plan must address new scenarios, and BC processes must integrate with a greater number of enterprises processes, including e-fulfillment, security, performance and problem management. This presentation focuses on best practices in business continuity planning, with an emphasis on new requirements driven by the criticality of e-business.

Donna Scott, William Malik
32G, SPG3, 5/01

Conclusion: An increase in e-commerce-related risk broadens the scope of business continuity planning.



Source: Gartner Research

Traditional business continuity plans cover scenarios for physical site outages, as well as for power failure, technology outage and natural disaster. With e-commerce, however, comes new requirements and risks. E-commerce initiatives tend to be business-critical, requiring 24x7 availability. As a result, recovery time objectives are much shorter — and sometimes nonexistent — thus requiring business continuity and disaster recovery to be considered at the time of application architecture and design. Typically, e-commerce sites are built across two or more physical sites, in either active/active or active/passive configurations. Active/passive configurations are typically built to recover from a physical site outage in 30 to 60 minutes. Because any amount (and cause) of downtime significantly impacts the business, the scope of scenario planning broadens for the BC manager/team to encompass new risks, including any incident that could invoke a recovery to another physical site, such as security incident/breach, outsourcer outage/breach, content/application link outage/breach, e-commerce site outage (planned or unplanned), performance degradation or insufficient capacity due to a newly initiated marketing program, and operations error/change resulting in downtime.

Action Item: Applications architecture/design must include new continuous availability requirements, including planning for physical site outages, regardless of cause.

Strategic Planning Assumption: By 2005, 70 percent of new application investment and 50 percent of new IT infrastructure investment will focus on e-business transformation (0.7 probability).

E-Commerce BC: New Rules/New Realities

- IT and business process management are integrated — they are no longer solo views
- Production costs increase — no separate budget for BCP
- Risk identification and management take on a matrix management focus, e.g., technology, financial, trading, operations
- Problems are public — IT and business problem management must be integrated; root cause analysis
- Only as strong as your weakest link — good application/bad operations
- Contingency plans become critical when automation isn't there — ***every*** component of the business process now must have a plan

Gartner

Source: Gartner Research

Conclusion: An increase in e-commerce-related risk broadens the scope of business continuity planning.

With 70 percent of new application investment and 50 percent of new infrastructure investment by 2005 (0.7 probability), e-business is rapidly transforming business processes. The result of the new risks and the integration of continuous availability into the business process impacts the business in new ways. The boundaries between business-as-usual and an emergency event that were so easily erected prior to e-commerce are no longer possible. There is no distinction between these two operating environments. The cost of operating the e-commerce application environment increases because the decision for business continuity needs is pushed up to the design phase of the project. The risk of e-commerce site downtime reduces the number of risks that can be accepted by business management; therefore, they must now be directly addressed with recovery solutions. The new risks being presented by e-commerce need to be reviewed by an integrated team including a full contingent of IT and business personnel. An e-commerce outage is now public knowledge; therefore, the reaction to the outage must be immediate and well-managed. Outages take on many faces — the application might hum, but the operating processes around the application environment might be the cause.

Strategic Planning Assumption: By 2004, more than 60 percent of large enterprises will have invested in BC planning for e-business processes, compared to less than 25 percent (of non-e-business processes) today (0.8 probability).

BC Components

	Disaster Recovery	Business Recovery	Business Resumption	Contingency Planning
Objective	Mission-critical applications	Mission-critical business processing (workspace	Business process workarounds	External event
Focus	Site or component outage (external)	Site outage (external)	Application outage (internal)	External behavior forcing change to internal
Deliverable	Disaster recovery plan	Business recovery plan	Alternate processing plan	Business contingency plan
Sample Event(s)	Fire at the data center; critical server failure	Electrical outage in the building	Credit authorization system down	Main supplier cannot ship due to its own problem
Sample Solution	Recovery site in a different location	Recovery site in a different power grid	Manual procedure	25% backup of vital products; backup supplier
CRISIS MANAGEMENT				

Source: Gartner Research

Conclusion: An increase in e-commerce-related risk broadens the scope of business continuity planning.

The shift from disaster recovery to business continuity is due to the fact that most, if not all, stages of the business life cycle are totally dependent on IT services. Along with dispersed ownership and management (internally and externally) of IT services, providing for BCP is a top-level concern for enterprises and is vital to maintaining financial confidence in and the reputation of the business.

E-commerce does not change the five components of BCP. It places more importance on the enterprise's contingency and crisis management plans, due to the public nature of outages and the increasing reliance on outside service providers for processing. The potential range of e-commerce failures must be determined from an organizational perspective and all interdependencies appropriately planned for. Each component of the business process must have a recovery plan. If the link to the credit-checking service (an outside service provider) is not available from your Web site, then alternate plans must be in place to immediately handle the purchase in progress.

Action Item: An end-to-end analysis of the information flow through internal- and external-processing environments is required to successfully provide for recovery options for all potential scenarios.

Strategic Planning Assumption: By 2004, the majority of spending on e-commerce recovery will become part of the production budget rather than a discrete business continuity expenditure (0.8 probability).

Project Life Cycle

Bus. Req.	System Arch.	System Design	Con-struct	Test	Imple-ment	Post Imple-ment
• Identify technology and ***business continuity*** risks from a business perspective - ***BIA/ Risk Analysis RTO/RPO*** • Ensure complete cost estimate • Ensure appro-priately protected end product	• Assess risks of new technology products • Identify security infrastructure reqs. • Identify sec. admin. reqs. • Establish security responsibilities and service-level regs. • ***Identify business continuity/DR strategies*** • Establish security test strategy	• Translate security architecture to detailed security infrastructure design • Develop security baselines for new technologies/ products • Develop detailed sec. admin. design • ***Develop detailed BCP/DR design/strategy*** • Develop draft SLAs • Develop security test plan	• Build/code security infrastructure env. and procs. • Build/code sec. admin. env ., roles/profiles and procs. • ***Build BCP/DR env., plans and procs.*** • Build/code security test plan, procs., scripts and test env.	• Train sec. admin., operations, business unit, etc. staff • Identify security non-compliance issues • Identify new security exposures • ***Test BCP/DR plans to ensure that RTO/RPO is attainable***	• Turn over secure application infrastructure to production • Implement sec. admin. roles/profiles • ***Implement business/ continuity DR env.***	• Identify changes to tested env. • Finalize sec. admin. env. and procs. • Finalize security infrastructure env. and procs. • ***Finalize BCP/DR env., plans and procs.*** • Assess SLA accuracy • Finalize risk acceptance with business • Ensure that info. sec. policies are current

Source: Gartner Research

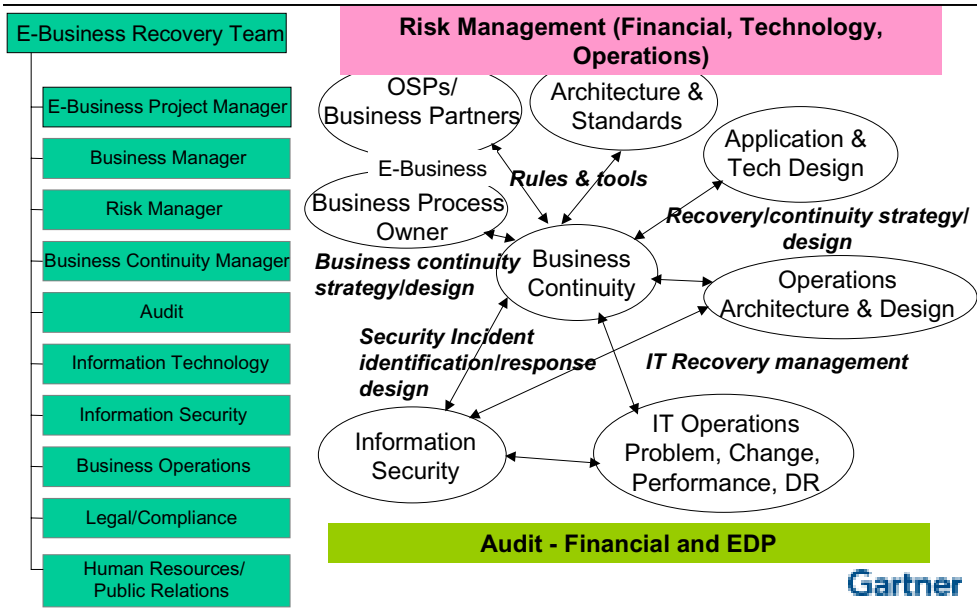
Conclusion: An increase in e-commerce-related risk broadens the scope of business continuity planning.

The foundation of BCP success is senior management sponsorship and participation. Direct financial impact will arise via lost sales, increased costs of working, material losses or other loss exposure. Indirect financial impacts (e.g., reduction in future earnings) may arise in the long term via loss of customer confidence or competitive advantage, or damage to the brand value. In the start-up phase of the BC program, the enterprise must establish a base view of its recovery needs by following traditional planning steps, which include: 1) ***business impact analysis (BIA)*** to identify what and how much the enterprise has at risk, as well as which business processes are most critical, thereby prioritizing risk management and recovery investments; 2) ***risk analysis*** identifies the vulnerability of the enterprise to different categories of risk and its probability; 3) the ***recovery strategy*** outlines in broad terms the approaches to risk mitigation, incident management and recovery from the incident; 4) ***detailed plans and procedures*** are then created by those responsible for the daily operation of the processes; 5) ***recovery process testing*** is the key to success; and 6) a ***continuous-monitoring process*** is implemented to keep the plan updated.

Action Item: Integrate business continuity planning into the enterprise project life cycle to ensure that recovery needs are identified in the initial phases of new projects, including "project creep" and major upgrades.

Strategic Planning Assumptions: By 2005, 70 percent of all product and service-based industries will be dominated by virtually integrated enterprises (0.7 probability). By 2004, 30 percent of the Global 2,000 will have risk management departments, which will integrate financial, operational and technology risk mitigation (0.7 probability).

E-Commerce BC — Integrated Processes



Source: Gartner Research

Conclusion: An increase in e-commerce-related risk broadens the scope of business continuity planning.

Key to an effective business continuity program is inter- and intraenterprise process engineering. The team required to plan and implement business continuity plans for e-commerce must be comprised of the e-commerce business units, IT and all outside service providers. The resulting plans must also be integrated because of the shorter recovery time frames and because any outage is now public. These changes from traditional BCP require a much higher level of communication built into the overall e-commerce management process on a day-to-day basis — between business units and between businesses — which itself poses challenges as to "how much do I tell my business partner." The role of the business continuity manager will change, as well as become a major part of the business operations staff.

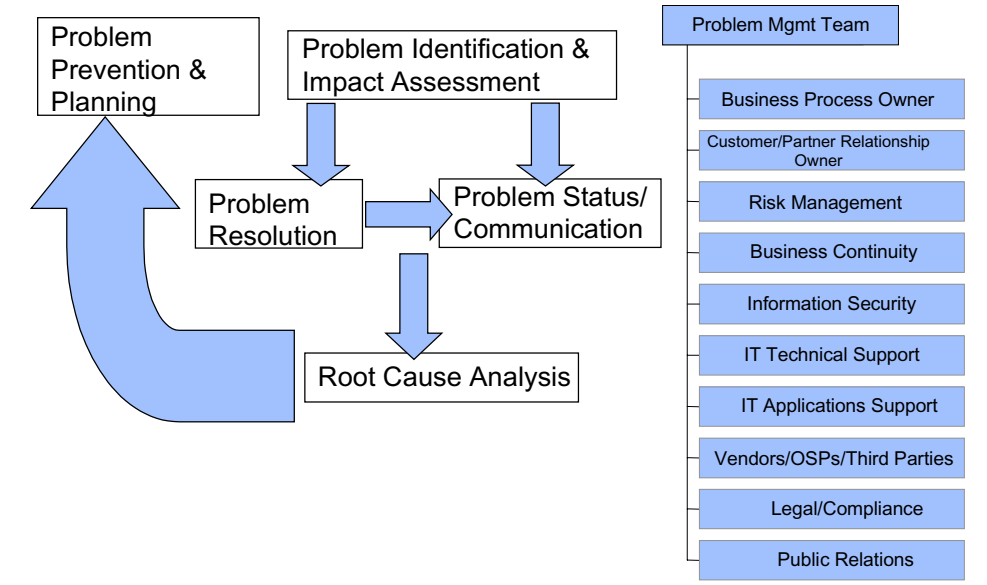
Deloitte & Touche offers one approach to integrating BCP into e-commerce as follows: subdivide the three e-commerce areas and apply the BCP process to each subdivided area:

1. Content: Data quality, content generation, sharing and liabilities
2. Buy-Sell: Logistics, distribution, credit and audit trails
3. End-to-End Technology: Architecture, systems, file structure and mapping

Strategic Planning Assumption: By 2004, 30 percent of the Global 2,000 will have information classification procedures implemented to ensure that the intellectual property of the enterprise is not disclosed to unauthorized parties (0.8 probability).

Imperative: Managing problems through resolution, root-cause analysis and prevention requires a cross-functional team from the business and IT.

Problem Management Life Cycle



Source: Gartner Research

Conclusion: An increase in e-commerce-related risk broadens the scope of business continuity planning.

Reacting to and managing an outage in e-commerce also requires an integrated process to determine the root cause of the outage. In addition to predefined plans for recovering from an outage, enterprises need to have a predefined problem management process that includes many of the same people as on the e-commerce recovery team. Again, communications are critical to a well-executed problem management process. Information sharing is required in the e-commerce business process; however, when resolving a problem, often more information than is usually disclosed to customers, partners or OSPs is required in order to resolve the problem. Extra precautions must be built into the predefined problem management process to ensure that the intellectual property of the enterprise is not disclosed throughout the problem management life cycle. Management must classify information that can and cannot be disclosed. Contracts must contain nondisclosure clauses and agreements on handling procedures must be developed for such instances.

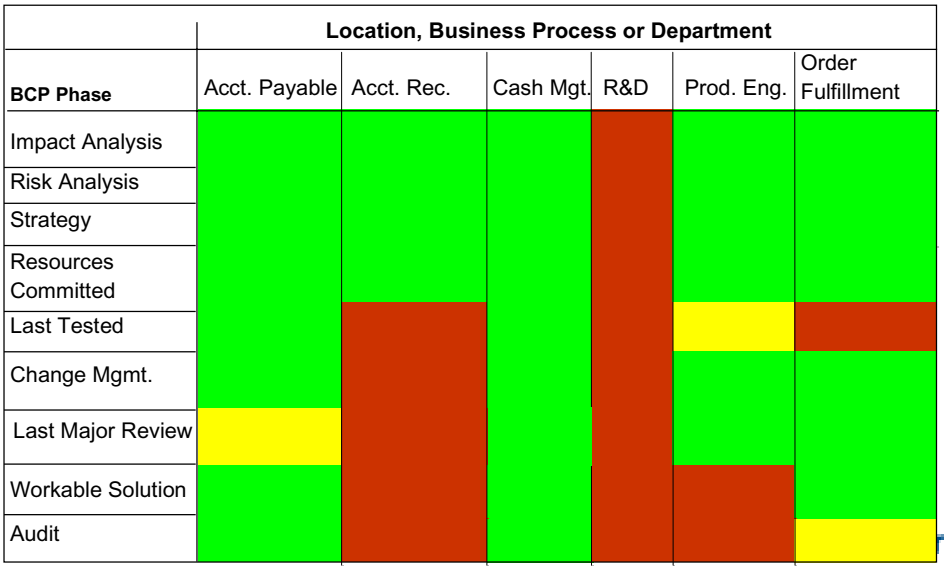
Action Item: Institute an information classification process to ensure that information critical to the enterprise is not disclosed during the problem management life cycle.

Even a failed disaster recovery test is useful.

E-business continuity plans require frequent testing to assure support of critical business requirements.

Too Much Testing and Reporting Is Never Enough

Management Reporting Is Critical

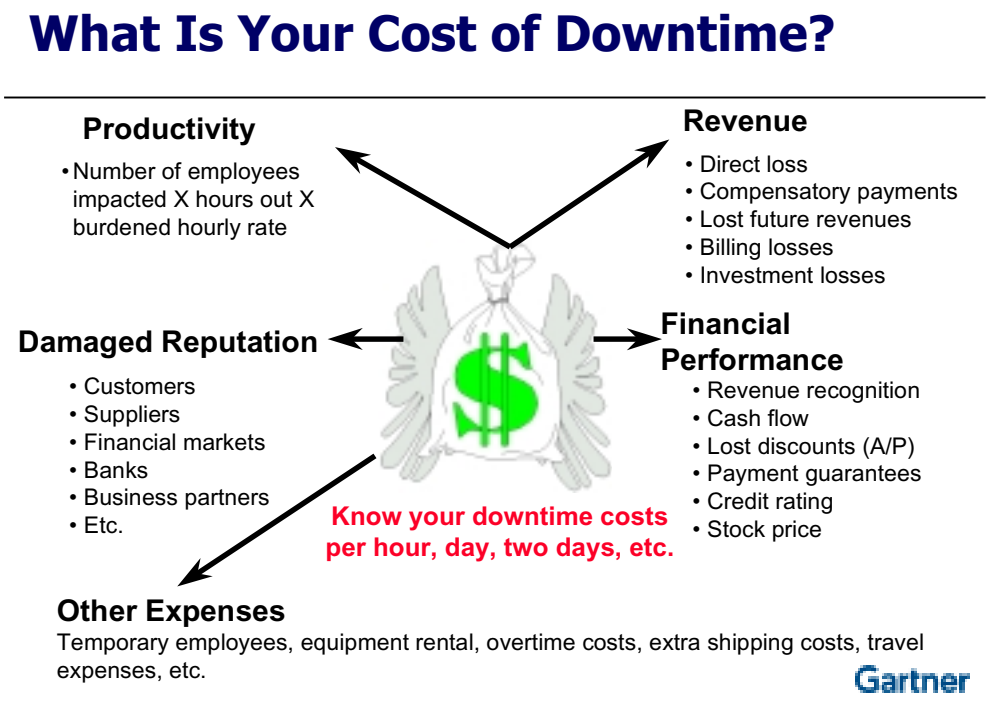


Source: Gartner Research

Conclusion: An increase in e-commerce-related risk broadens the scope of business continuity planning.

To ensure a credible degree of recovery preparedness, every plan must be regularly tested. Testing familiarizes BC team members with the experience of a sudden, unexpected interruption in business processing, exposing potential problems and unforeseen situations. A continuous cycle of testing and plan modification is key to recovery preparedness and maximizing the chances of successfully surviving a disaster. Testing e-commerce BC plans adds new requirements and pressures: Reliance on alternate processing procedures increases. Some plans might not be able to be tested, due to availability requirements, the complexity of the telecom connections and the range of business interdependencies, which results in the necessity of including more participants — inside and outside the enterprise —in the test. Reporting BCP status and progress is a key element of getting the plans created, but more important, in keeping them up-to-date. By using normal line management to ensure that functional and process management take responsibility for their own domains, each manager should sign the business continuity plan and be held accountable for its accuracy. *Action Item: Testing e-business recovery plans requires an integrated effort of all parties involved with the business transaction. The participation of all outside service providers is critical to the success of the recovery process. When it is impossible to live-test, conduct a tabletop testing to ensure that external dependencies are addressed. Contracts with outside service providers must address BC needs.*

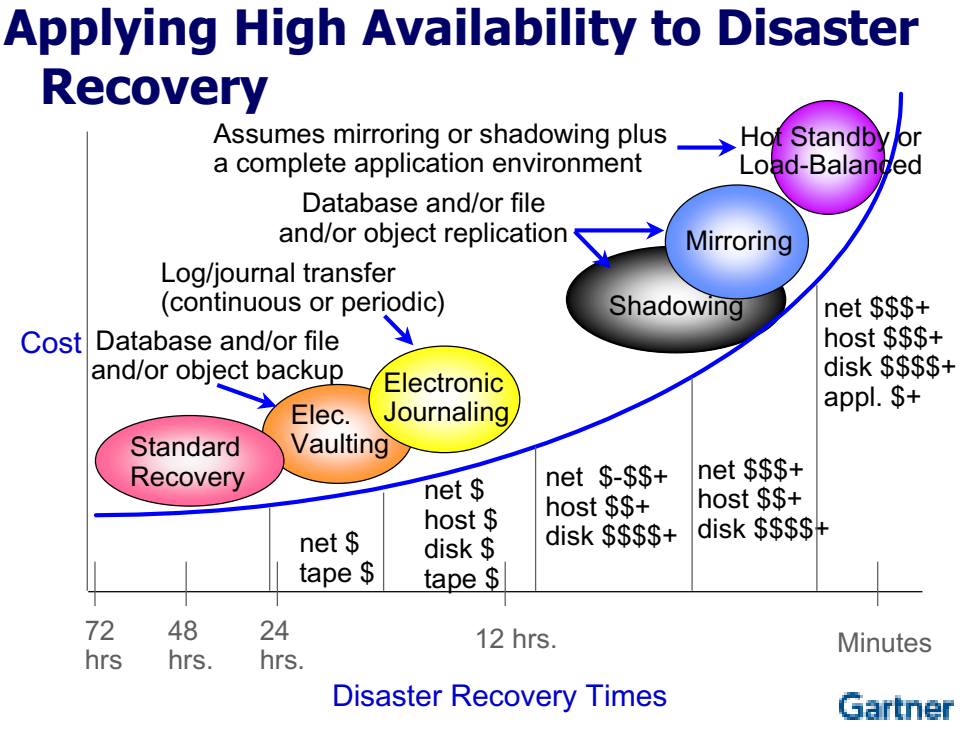
Conclusion: E-commerce drives increased requirements for continuous availability and shorter recovery times and points.



Source: Gartner Research

To determine appropriate availability investments, enterprises should first understand the consequences of downtime, which will aid in justifying investments for day-to-day operational availability and for business continuity. One of the first steps in developing a BC plan is performing a BIA, where critical business processes are identified and prioritized, and costs of downtime are evaluated over various time periods. The BIA is performed by a project team consisting of business unit, security and IS personnel. Key goals of the BIA are: 1) to agree on the cost of business downtime over varying time periods; 2) to identify business process availability and recovery time objectives; and 3) to identify business process recovery point objectives. The results of the BIA feed into the business recovery strategy and process. Enterprises that have never instituted a BIA into their application life-cycle processes typically initiate a project to develop a BIA for critical business processes, and use their findings to ensure that existing recovery strategies meet business process requirements. However, with e-business, it is critical that BC be built into the life cycle for new applications and business process enhancement projects so that availability and recovery requirements are built into the architecture and design. In fact, with e-business, many traditional BC costs (e.g., for duplicate equipment located in a secondary facility) are built into the application architecture, and are not included in the BC or disaster recovery budgets.

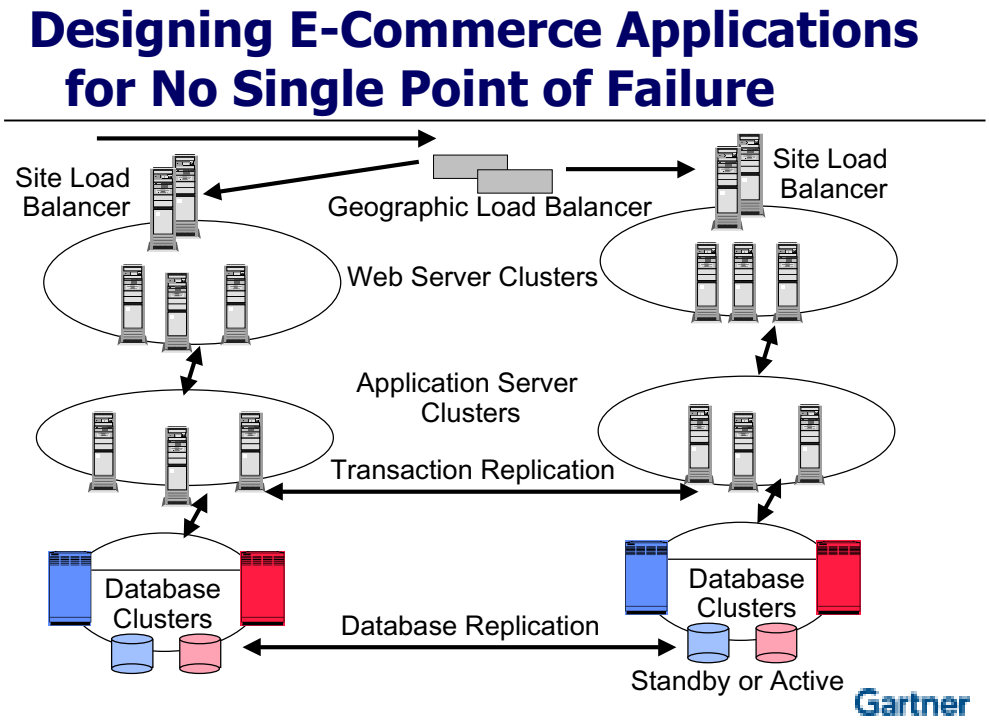
Tactical Guideline: Recovery strategies must match e-business requirements and risk scenarios.



Source: Gartner Research

Conclusion: E-commerce drives increased requirements for continuous availability and shorter recovery times and points. Traditional BC plans provide 24- to 72-hour application and business process recoverability. With technology more intrinsic to business processes and costs of outages escalating, many enterprises are seeking shorter recovery times for critical applications. Use of high-availability techniques is escalating, especially for ERP and e-business applications, enabling enterprises to achieve recovery time objectives (RTOs) and recovery point objectives (RPOs) in a matter of minutes rather than days. With e-business, hot standby often is not good enough, and many design application architectures across two or more active physical sites. This way, even if one physical data center experiences an outage, the others continue processing the requests. Load balancing across two or more physical sites is especially common for non-transactional applications. Often transactional applications are located in a single physical site, with hot standby at another site. This configuration reduces the complexity and chances for conflict resolution. For both hot standby and load-balanced sites, data is replicated between physical sites, typically via either mirroring or shadowing (at the transaction level or the data level). Shadowing builds a replica of databases or file systems by continuously capturing changes and applying them at the recovery site. Mirroring builds a replica of databases or file systems, by applying changes at the alternate location in lockstep with the primary site. *Action Item: Evaluate Web site and all integrated content/applications availability and recovery strategies to ensure they meet business requirements.*

Strategic Planning Assumption: Through 2004, more than 60 percent of the top 100 e-commerce "sites" will operate two or more load-balanced physical sites or have a hot standby environment (0.8 probability).



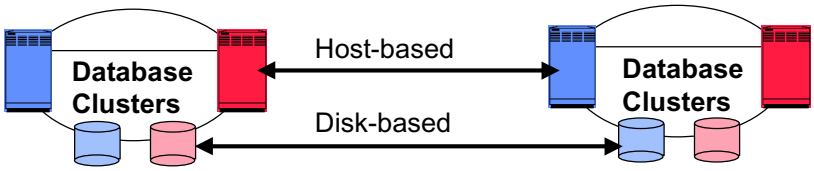
Source: Gartner Research

Conclusion: E-commerce drives increased requirements for continuous availability and shorter recovery times and points.

To mitigate the risks of a single site outage, multisite architectures are used. Often, a new e-business site starts with a single site architecture and migrates to multiple sites as it and its risks grow. Having multiple sites, however, complicates application architecture design (e.g., considerations of load balancing, database partitioning, database replication and site synchronization must be designed into the architecture). For nontransaction processing (non-TP) applications, multiple sites run concurrently, connecting users to the closest or the least-used site. To reduce complexity, most TP applications replicate databases to an alternate site, but the alternate databases are idle unless disaster occurs, whereupon a switch to the alternate site is accomplished in minutes (typically 15 to 30 minutes). Some enterprises prefer to partition databases and split the TP load between sites, and consolidate data later for decision support and reporting. This option reduces the impact of any site outage, affecting only a portion of the user base. Other enterprises prefer even more complex architectures with bidirectional replication (often accomplished through transaction replication) between sites to maintain a single database image. *Action Item: Enterprises should plan for multiple sites up front when designing the application architecture to increase the flexibility of options and better meet multisite needs.*

Strategic Planning Assumptions: The threat of lost economic viability in the event of a disaster will drive penetration of data replication technologies for e-commerce from less than 25 percent today to 75 percent by 2005 (0.8 probability). Lack of available and economical bandwidth will prevent widespread deployment of data replication technology through 2005 (0.2 probability).

Data Replication for Continuous Availability



Replication Methods	Examples
Disk-to-disk mirroring	EMC SRDF, Compaq DRM, IBM PPRC & XRC, HDS HARC & HRC
Log-based DBMS Replication	Quest Shareplex, Oracle Standby Database, ENET RRDF, SQL Server 2000
Server-based block or file replication	Legato Octopus, NSI Doubletake, Veritas SRVM
Application-based replication	Typically implemented with message-queuing middleware

Gartner

Source: Gartner Research

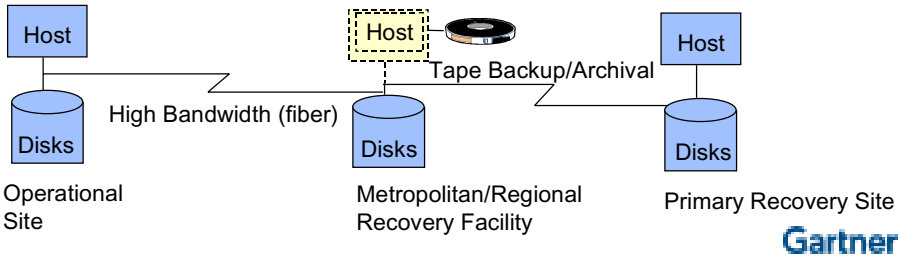
Conclusion: E-commerce drives increased requirements for continuous availability and shorter recovery times and points.

Data replication solutions are specific to a database, file system, OS, disk subsystem or application; thus, enterprises often must use multiple solutions to protect their critical data. The most common approach to mirroring for DR is disk-to-disk remote copy. Remote copy is relatively easy to set up, well proven and has low day-to-day administration. The cons are the costs and the potential impact on production applications (when in synchronous mode). Further, databases are not accessible at the secondary site for inquiry purposes. Database replication enables replication between sites (which can be bi-directional). For some applications, this works well, but for others, there is too great a chance for conflict resolution (updates made on both sites on the same record that must be resolved). In addition, for DR purposes, database replication is typically far too complex. Log-based DBMS replication products have less management overhead, work well for DR and enable a copy of the database in an alternative location for use for inquiry and reporting (horizontal scalability). Server-based block replication tools are just emerging on the market and work similarly to disk-to-disk remote copy, but operate on the host. They require more management overhead than remote copy, but cost significantly less. File-based replication products such as those from NSI and Legato are popular on NT and Windows 2000 platforms.
Action Item: For RTOs of less than 24 hours, evaluate transaction and data replication techniques.

Strategic Planning Assumptions: Through 2002, software licensing issues will slow adoption of capacity-on-demand services for disaster recovery (0.8 probability). Due to high costs, cascading remote copy techniques will have limited market potential for disaster recovery through 2003 (0.8 probability).

Emerging Technologies/Services

- Capacity on demand/emergency back-up
- Wide-area clusters
  - HP Continental Clusters
  - IBM Geographically Dispersed Parallel Sysplex
- Cascading Data Replication



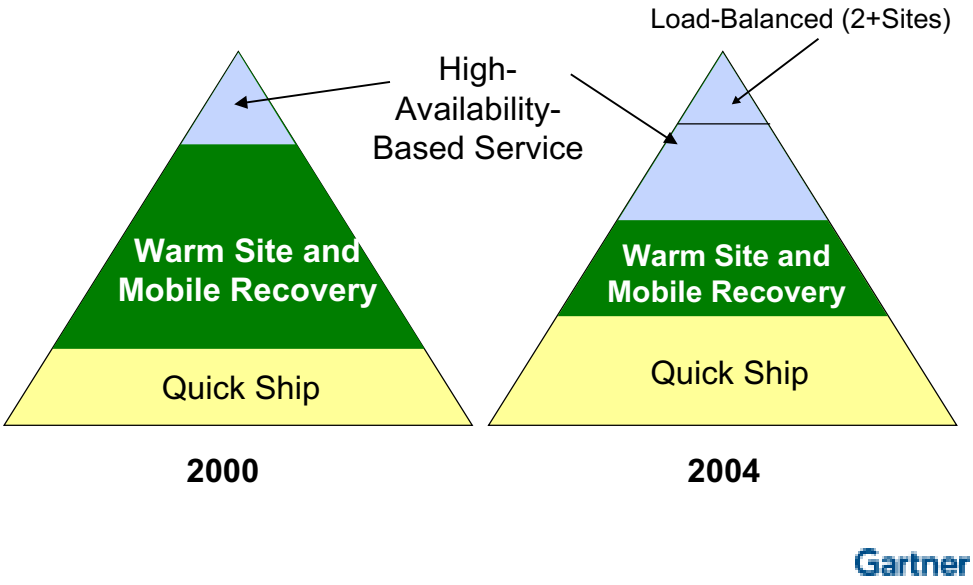
Source: Gartner Research

Conclusion: E-commerce drives increased requirements for continuous availability and shorter recovery times and points. Many emerging technologies/service offerings are designed to increase business continuity flexibility, reduce costs and reduce recovery times. IBM, HP and Sun have introduced capacity-on-demand/emergency backup programs to enable an increase in CPU capacity under emergency conditions (e.g., disaster or peak volumes). Typically, increases are permanent and paid for as used; however, there is a desire to enable throttling of capacity to meet e-business workload variability. This will require significant changes in software licensing practices. Wide-area clusters are being deployed by Type A enterprises with very short RTO/RPO. These include IBM's Geographic Parallel Sysplex service offering (40 km distance limitations) and HP's Continental Clusters (unlimited distances). In addition, the combination of available fiber-optic networks and remote-copy mirroring technologies has fueled new cascading service offerings. Cascading service offerings enable synchronous mirroring over a shorter distance, with asynchronous mirroring to the recovery site. Their main benefit is to reduce impact to production application performance (caused by network latency); however, their high cost will limit their market potential through 2003 (0.8 probability). In addition, service providers will perform a greater amount of operational tasks such as tape backup/archival at regional facilities. These services will have lower margins than traditional DR hot-site subscriptions but will be required to enable "one-stop shopping" and high-availability services. *Action Item: Select a service provider with local presence and resources.*

Conclusion: E-commerce is transforming the market for business continuity services.

Strategic Planning Assumption: By 2003, there will be a polarization in recovery windows, with critical business processes and application systems requiring recovery in less than 24 hours and non-critical ones requiring recovery in four days or more (0.8 probability).

Disaster Recovery: Market Dynamics



Source: Gartner Research

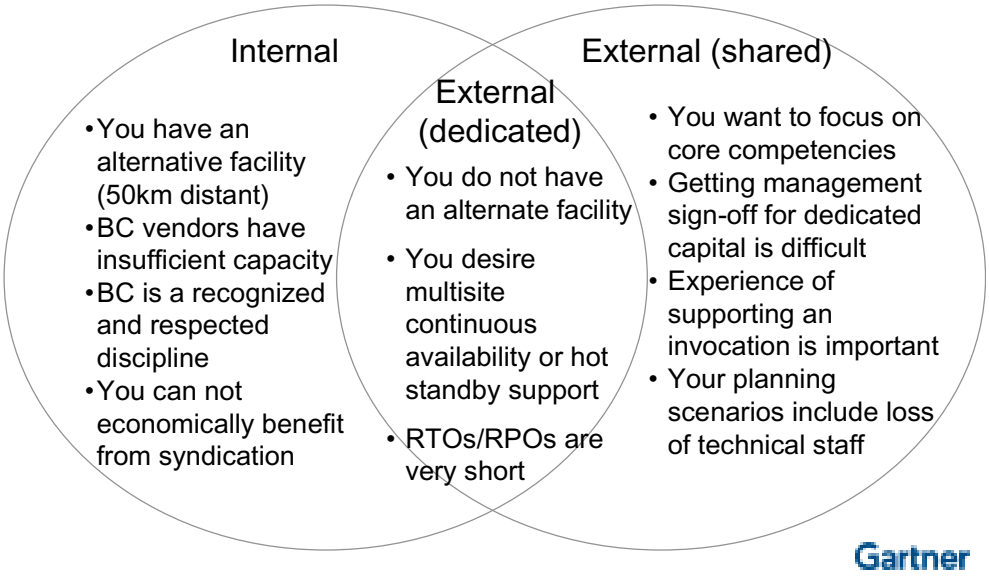
As business process dependence on technology increases, so, too, does the business cost of outages. E-business and ERP systems are examples of where significant outages directly affect an enterprise's operations and revenue, and quite possibly, its survival. As a result, requirements for recovery time and point objectives are shortening and driving changes in the BC services industry. A greater number of applications will require recovery in less than 24 hours, and many, especially e-business applications, will be designed for processing simultaneously across multiple data centers (e.g., building disaster recovery into the architecture). Consequently, the proportion of DR services using high-availability methods (mirroring, shadowing, hot standby, load-balanced physical sites) will greatly increase in overall proportion. In fact, the primary DR/BC service providers (Comdisco, IBM, SunGard) have already geared up to enable production operations within their facilities to capture e-business market share.

At the other end of the spectrum, we believe there will be a polarization in DR windows, and most noncritical applications will not require DR windows of less than four days; quick-ship programs will be the most common alternative for the DR requirements of these applications. Although some applications will continue to require a two- to three-day recovery window, these will be much reduced. As such, the profile of recovery services used will change.

Tactical Guidelines: In evaluating insourcing vs. outsourcing, enterprises must consider cost, skills, access, recovery times, capacity/resources and support.

Disaster recovery outsourcing can be full-service or selective; in either case, enterprises must ensure that their providers themselves have disaster protection.

Resource Internally or Externally



Source: Gartner Research

Conclusion: E-commerce is transforming the market for business continuity services.

While a substantial part of the business continuity process cannot be outsourced, much of the equipment and labor required to plan for and support the recovery can be. Outsourcing the resourcing of the recovery plan can be cost-effective, as the cost of the equipment is syndicated in the United States among 100 (six to 35 in Europe) other enterprises. It is sometimes impractical to outsource because there are no local resources to support the recovery or the recovery window is too small (and the risk is too high) to consider sharing equipment. In these cases, enterprises may use dedicated equipment at their own or a service provider's location, or for Web applications, operate in a load-balanced mode across multiple facilities to enable continuous availability (at their own or a service provider's location). In large installations, the BC vendor may not have the necessary capacity or the workload may not be able to be partitioned across multiple machines. Other enterprises choose to outsource because they do not want to capitalize the necessary equipment or they are not confident of their ability to maintain the critical capacity in the "recovery" location. Service providers can offer the resources necessary to support testing without disrupting an organization's normal operations. Its staff also has the experience of supporting live invocations, which are always times of stress for operational staff. It may also be that the organization's own staff is unavailable to run the recovery.

Action Item: When considering e-business service providers, evaluate their BC/DR experience.

Tactical Guidelines: Multinational enterprises should evaluate worldwide suppliers as well as regional ones to maximize negotiation leverage.

In selecting an e-business service provider, evaluate its ability and experience in providing continuous-availability services.

North American Business Continuity Market

Full-Service Providers

- Comdisco Recovery Services and Web Availability Services
- IBM Business Continuity Recovery Services and Outsourcing Services
- SunGard Recovery Services and E-Sourcing

Business Continuity and Internet Services

- Professional services
- Planning software
- Hot/warm/cold standby
- Mobile/static facilities
- Mainframe/midrange/desktop
- Quick ship
- Peripherals
- Networks
- Work area
- Specialized ancillary services such as check processing and data recovery

What's new — Full-service Web hosting with BC "designed in," multisite infrastructures for continuous availability, Web site and network "throttling" for performance

Gartner

Source: Gartner Research

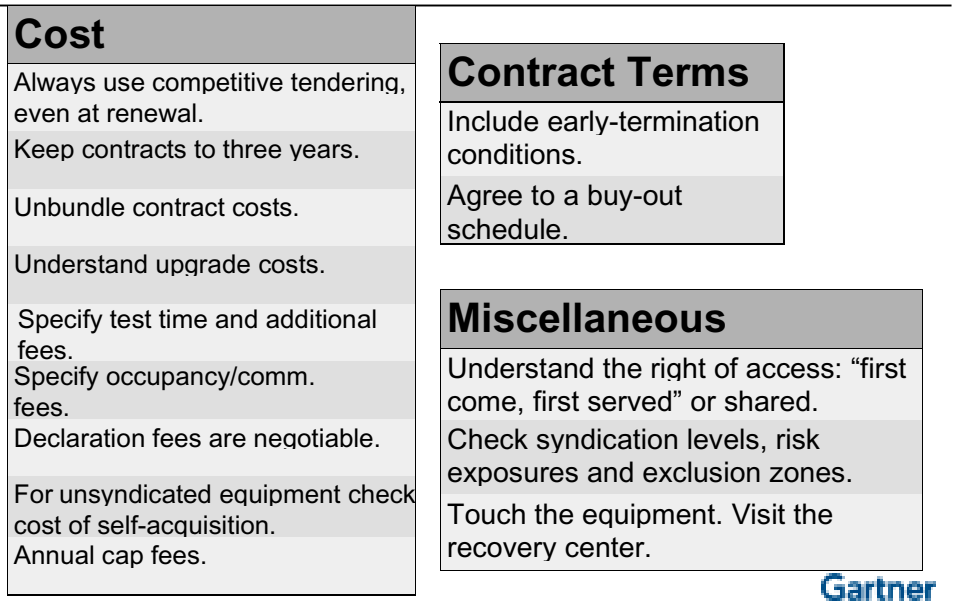
Conclusion: E-commerce is transforming the market for business continuity services.

The business continuity market is extremely fragmented, with many players in each market niche. Therefore, comparison of the different players is almost impossible; each one has a different area of emphasis and expertise. The range of products and services and the number of individual suppliers of varying degrees of specialization mean that the business continuity market in aggregate does not lend itself to Gartner's Magic Quadrant assessment. However, the players fall broadly into two categories: full-service providers and product- or service-specific suppliers. Full-service suppliers offer — either directly from their own resources or indirectly through subcontracted integration capabilities with other vendors — the spectrum of services listed in the chart above. In terms of revenue and expressed client interest, the three full-service providers (i.e., Comdisco Recovery Services, IBM Business Continuity Recovery Services and SunGard Recovery Services) are the most substantial participants in the North American market, and enterprises report that competition among them is increasingly close on grounds of cost. In addition, due to intense competition from Web-hosting service providers, Comdisco, IBM and SunGard have broadened their offerings to include full-service Web hosting, with availability and continuity services included.

Action Item: For high-end Web sites, evaluate Comdisco, IBM and SunGard for hosting and continuity services.

Tactical Guideline: Competitive tendering at renewal will reduce prices by between 20 percent and 50 percent.

Negotiating a Favorable BC Contract — Balance Risk With Economies of Scale



Source: Gartner Research

Conclusion: E-commerce is transforming the market for business continuity services.

Business continuity service providers traditionally make their money from investing in equipment and people, then syndicating them to as many clients as possible without compromising risk or service. Enterprises must understand the subscription levels, and who and where their fellow subscribers are, to ensure they are mitigating their own risks. Beware of the cheapest supplier, which may be oversyndicating or managing risk badly.

Changing service providers can be a painful process requiring modifications to the business continuity plan, more testing and familiarization with the new facilities. However, substantial savings are to be made if competitive tendering is introduced. Make sure the components of the proposal from the vendors are understood. Costs will continue to drop over the next five years, so keep the contract to three years. The contract should include termination clauses related to changes in circumstances, such as an acquisition or outsourcing of the data center, increases in costs beyond an agreed limit and test failures due to recovery facilities proving unsuitable. The incremental costs of adding additional capacity should be clearly indicated. Some vendors insist on a declaration fee, but the value can be negotiated. Always check the right of access and what happens if the vendor has multiple invocations. For dedicated equipment that the service provider will provide uniquely for the contract, check the cost of acquiring the equipment. Unbundle contract costs so that they can be compared to other service providers' proposals.

Recommendations

Applications architecture/design must include new continuous availability requirements, including planning for physical site outages, regardless of cause.

An end-to-end analysis of the information flow through internal and external processing environments is required to successfully provide for recovery options for all potential scenarios.

Integrate business continuity planning into the enterprise project life cycle to ensure that recovery needs are identified in the initial phases of new projects, including "project creep" and major upgrades.

Institute an information classification process to ensure that information critical to the enterprise is not disclosed during the problem management life cycle.

Testing e-business recovery plans requires an integrated effort of all parties involved with the business transaction. The participation of all outside service providers is critical to the success of the recovery process. When not possible to conduct a live test of a BC plan, or a component plan, conduct a tabletop testing to ensure that external dependencies are addressed. The contracts with outside service providers must address BC needs.

Enterprises should plan for multiple sites up front when designing the application architecture to increase the flexibility of options and better meet multisite needs.

Evaluate Web site and all integrated content/applications' availability and recovery strategies to ensure they meet business requirements.

For RTOs of less than 24 hours, evaluate transaction and data replication techniques.

Select a service provider with local presence and resources.

When considering e-business service providers, evaluate their BC/DR experience.

For high-end Web sites, evaluate Comdisco, IBM and SunGard for hosting and continuity services.

Source: Gartner Research

BCP requires many resources in the enterprise to unite and act as a team. Keys to success include:

- Obtaining senior management support from the beginning
- Establishing a BC organization structure, including budget management and process integration points (e.g., with information security, problem management, change management, business and technology risk management)
- Performing the BIA/risk analysis in the application and business process project life cycle:
  - Understand critical business processes and risks
  - Determine business process RTO/RPO
- Developing BC plans keeping in mind any additional risks to be included in scenario planning:
  - Business resumption
  - Business recovery
  - Disaster recovery
  - Contingency planning
  - Crisis management
- Evaluating technologies to reduce RTO/RPO, ideally during application design
- Evaluating BC service providers to help plan, implement and host
- Testing, testing, testing
- Return to the top of the list and repeat the process on an ongoing basis.

This is the final
page of the presentation

Click to continue...