Business Continuity and Disaster Recovery Planning and Management: Technology Overview

Summary

A broad range of technologies can support a company's business continuity planning and implementation—and reduce the impact of disruptions from natural disasters, technology failures or criminal acts.

Table of Contents

List Of Tables

Technology Basics

Business disruptions—whether the result of natural disasters, technology failures or criminal acts—can threaten the very survival of a company. Such disruptions cannot always be predicted or prevented, but sound planning can dramatically reduce the damage they cause. But effective preparation for disaster recovery and business continuity is a job for the entire company.

Business Survival in an Uncertain World—The Basics Remain Constant

Major business interruptions—particularly those featuring dramatic disasters—grab attention and focus it on one vector of threat at a time. It is important, however, to keep the broad perspective, "the big picture," in mind. Although business continuity planners naturally check their own company's vulnerability to the natural or man-made disaster making news at the moment, the economic trends of the past 18 months demonstrate that the greatest threat to most businesses is simply "less business." Factors to consider for business survival are complex, extending beyond data security and physical security. Being prepared for business interruption involves analysis of every aspect of the organization's management so that the company is positioned to survive the erosive effects of the winds of change as well as the sudden blast of a hurricane.

Using the Available Tools and Tactics

Tools and tactics to manage the process of business continuity planning and disaster recovery need to be used in concert with financial planning and corporate governance information systems. Some important questions that emerge for technical officers and their continuity planning colleagues are: How can the company integrate continuity planning with overall corporate risk management? Of the products, consultants and services available, which kind of help best fits each company's needs? Should the company build and maintain the solution or contract for services? How can the company use continuity planning tools to prepare decision-makers to think creatively and flexibly when handling a crisis? Answering these questions requires understanding the services that support making business continuity decisions.

The Need for Business Continuity/Disaster Recovery Planning and Management

What Organizations Don't Expect *Will* Hurt Them

In the aftermath of recent natural disasters, terrorism, Internet-based data sabotage and executive malfeasance, organizations recognize the need to be prepared for the unexpected. A recently completed 20-year survey of Fortune 500 crisis readiness by the University of Southern California's Center for Crisis Management has demonstrated two troubling conclusions: (1) the incidence of intentional damage to corporate assets has risen markedly during the past 10 years, and (2) between 75 percent and 95 percent of Fortune 500 companies are not prepared to manage a new type of crisis.

Thus, the question is: What can business continuity planners do to become proactive in crisis-preparedness?

Continuity planning tools and disaster recovery services can provide all the "what" and many of the "how" elements of the answer. The average organization's requirement for recovery time from a major system outage currently ranges between two and 24 hours. *IT organizations* are very aware of the many vulnerabilities of the networks that support the business processes—because they have the responsibility of maintaining availability. The *business groups*, which use the systems over those networks, are aware

of the cost of that maintenance, but not necessarily the specific IT services that support the expected availability. Thus, an organization is pushed by the expectations—and requirements—from all sides:

- Customers expect supplies and services to continue—or resume rapidly—in all situations.
- Shareholders expect management control to remain unchanged throughout any crisis.
- Employees expect both their lives and livelihoods to be protected.
- Suppliers expect to be able to continue shipping, keeping the supply chain intact.
- Regulatory agencies expect their requirements to be met, regardless of circumstances.
- Insurance companies expect due care to be exercised.

High expectations for continuity and rapid recovery demonstrate the need for the integration of business continuity planning into enterprise-level initiatives. Business continuity preparation, adequately supported throughout the organization, embodies the strategic framework for a corporate culture that embraces a variety of tactics to mitigate risks that might cause:

- Business process failure.
- Asset loss.
- Regulatory liability.
- Customer service failure.
- Damage to reputation or brand.

Crisis Management: Preparing for the Unexpected

The key challenge of business continuity preparation is not technology, but the internal marketing "business" aspects that begin at the foundation level of any project and continue throughout its life cycle: justification, executive buy-in, broad organizational support, and governance and politics. Perhaps the most important point to make about business continuity support technologies is that their effectiveness depends entirely on the organization's top-down commitment to the entire business continuity/disaster recovery project, including the updating and testing necessary for maintenance.

Research implies that business infrastructure remains less protected than its stewards think it is, and such surprises usually lie in failure to consider the full scope of issues that continuity planning must encompass.

Two curable causes of disappointing continuity plan performance may be viewed as "spotty plans" (with gaps) and "plan rust" (from inadequate testing). Testing is expensive, and a company's commitment to it may depend on the *perceived* cost of disruption—which can be less than feared through the use of selected testing tactics, such as broad-brush walkthroughs for logistics and "worst case" scenario exercises limited to the most likely events and the highest-cost risks.

Successful plans must be updated and tested regularly, a process which includes re-training employees in their roles, re-training that should include practice in thinking nimbly and creatively in worst-case scenario examples. Such nimble thinking demands thorough knowledge of available resources and other elements of the continuity and recovery plan. Such plans share several characteristics:

- Executive and board-level support.

- Clear concise directions for action at every level.
- Integration with the corporate management culture, as an ongoing activity.
- Inclusion of risk management considerations.
- Prioritization of vulnerabilities.
- Coordination with suppliers and customers.
- Continual internal marketing to maintain participant awareness and motivation, with regular "what if" drills in creative solution implementation.

New Interest in Crisis Management Procedures Testing

When the TOPOFF crisis management exercise for Top Officers of the United States first occurred in May 2000, little public attention focused on these realistically challenging role-playing exercises involving the senior officials at all levels of government responsible for directing crisis management and consequence management response to a real weapons of mass destruction (WMD) attack. The second TOPOFF, in May 2003, attracted far more attention to the national-level simulations designed to produce a more effective, coordinated, global response to WMD terrorism. The five-day full-scale exercise and simulation of how the U.S. would respond in the event of a WMD attack involved cooperation among federal, state, local and Canadian partners. The exercises were videostreamed or Webcast in realtime over the Internet for the civilian and military emergency response communities.

Basics of Business Continuity Preparation

What Does the Business Need?

Solid requirements engineering for any type of business support project begins with the fundamental question: What does the business need? Business continuity planning is no exception. Elements required for continuity and recovery plans include:

- Mission Statement for the Plan—This document must be consistent with the company's mission statement and establish the objectives and scope of the plan.
- Executive Sponsor—Who owns the plan, has primary accountability for it and reports to the board on corporate risk management? Who else in senior and operational management positions serves on the "Continuity Planning Board"?
- Scope—What is included in the plan overall, and what is included in each part of an integrated plan? What is not included at all?
- Implementation Charter—Who is empowered to develop and implement the plan, with its related updates, tests and reports for continuous improvement?
- Regulatory Compliance—Which regulations or best-practice standards govern the plan?
- Stakeholders—What are the titles, and continuity-related activities, of the plan's constituents?
- Key Measures—What metrics gauge the plan's performance? These measures should be straightforward to measure an objective. Each test of the plan as well as each reality-triggered implementation of the plan should report on these metrics. Service-level agreements among the internal stakeholders and with recovery service providers should reflect related key measures.

- Policies and Procedures—What business policies apply to continuity/recovery operations? What behaviors do they prescribe? What procedures must be carried out to satisfy the policies? How are the policies enforced?
- Program Elements—What are the components of the continuity/recovery program necessary to satisfy the mission statement within the scope of the program? These include the plan itself and its maintenance as well as the elements it describes, such as contact lists, activation triggers, decision-trees, information security, physical security, awareness and training programs, and budget.

The Phases of Business Continuity Planning, Implementation and Management

The significance of each major phase of continuity planning merits attention because each phase contributes to building all four areas of business continuity: disaster recovery, business recovery, business resumption and contingency planning:

- **Phase 1—Establish the foundation**. These alignment and analysis steps are necessary to obtain executive sponsorship and the commitment of resources from all stakeholders. Without a basis of business impact analysis and risk assessment, the plan cannot succeed and may not even be developed. The audience for the business case phase of the planning document is the executive(s) who will authorize the plan's implementation.
- **Phase 2—Develop and implement the plan**. Here, attention to detail and active participation by all stakeholders ensure the development of a plan worth implementing. The plan itself must include the recovery strategy with all of its detailed components and the test plan. The audience for the implementation section of the plan document is the staff which will follow the plan's directions for continuity and recovery. Its existence and maintenance establish trust with the board of directors, shareholders and customers.
- **Phase 3—Maintain the plan**. The best plan is only as effective as it is current. Every tactic of business resumption and recovery must be kept up to date and *tested* regularly. The audience for the testing section of the plan document is the implementation staff. It is important that this staff know how demanding maintenance is, what (if any) tools are provided to assist with the process and how important plan maintenance is for building trust among the company's stakeholders.

Service Options

One significant trend among business continuity service vendors is to focus on business continuity as a whole—both continuity planning and disaster recovery (DR), and fold information security (InfoSec) into the business continuity planning (BCP) framework. Recovery itself must be speedy (under 24 hours, with two hours the ideal maximum outage) for high-availability systems—and the facilities must provide continuity not only of the data center (the "glass house"), but also of all critical aspects of its clients' businesses. This focus provides clients a more integrated service while allowing the vendor to maintain better account control:

- **Contract Priorities**. A word of caution: service contracts require careful negotiation with an eye to the company's highest priority requirements and the vendor's capabilities and priorities. Recovery contract cost-control includes tactics such as requiring the highest-ticket services (for example, remote disk mirroring) only for the most mission-critical systems, and longer recovery periods for applications with less immediate effect on the business cash. Issues of vendors' regional capabilities and commitments to higher-priority industry clients merit serious consideration. In the growing

InfoSec/BCP/DR market, vendors are expanding their capabilities as rapidly as they can, so contract managers should keep close tabs on the most efficient and cost-effective solutions available.

- **Time Frames and Performance Levels**. The contract can stipulate time frames for delivery of services as well as performance levels; for example, how long it will take for a drop-ship service to deliver the new equipment to the recovery site and whether their staff or the client's will install the equipment.
- **External Factors that can Influence Performance**. Realistic expectations of vendor performance include items to be included in the contract as well as external factors that may affect the vendor at the time of the catastrophe. External factors can include a number of unpredictable variables—such as whether the catastrophe is regional and affects the vendor's other local clients whose industries may receive priority treatment for recovery: military, government and healthcare typically must be recovered before manufacturing and retail sites. While a lower-priority client can do little about the necessary delay in recovery under those circumstances, simply knowing what to expect can help set timelines and expectations for both employees and customers.

Consulting and Planning Assistance

- **Software and Consulting**. Many service providers offer combinations of tactical consulting with business continuity planning and management software, sometimes including full continuity management services and hot-site facilities.
- **Hardware and Consulting**. Hardware vendors may combine continuity planning consultancy with rapid hardware replacement shipment, mobile-site delivery or hot-site facilities.
- **Internet E-Commerce Continuity and Consulting**. Communications and networking vendors may offer high-availability networking and rapid recovery solutions with tactical consulting.
- **Product-Independent Consulting**. Consultants who provide analyses, audits and tactical recommendations based on such studies offer objectivity in the development of the specifications a company should use to select business continuity products and services.
- **PC-Based Planning Tools**. Virtually all hot-site vendors offer some type of PC-based tool for developing the disaster recovery plan. In many cases (like consulting services), these packages are provided to a client organization as an enticement to acquire full hot-site services.

Recovery Assistance

Stand-alone considerations for off-site recovery remain a significant part of the continuity management strategy. Specific types of service may be combined to provide the exact package any company specifies:

- **OEM Insurance**. Hardware companies may offer a form of insurance guaranteeing that they will replace damaged computer equipment with a system of equal or greater processing capacity within a specified period. The insurance cost is usually six to eight percent of the monthly maintenance bill.
- **Quickship**. Most third-party leasing vendors provide guaranteed rapid shipment of replacement hardware as a recovery option. Customers pay a priority equipment search fee and the normal leasing charges plus a premium when they request shipment. Particular attention must be paid to the vendor's commitment to high-priority industry clients in the customer's region, so that realistic delivery expectations can be set in the case of region-wide disasters.

Commercial Recovery Sites

Commercial recovery sites permit an organization to continue computer and network operations in the event of a computer or equipment disaster. These sites and services are subscribed to by contract. When the subscribing organization actually uses the hot or cold site, other fees will be incurred in addition to the basic monthly charge:

- **Hot Site**. A hot site is a fully equipped, operationally ready data center offering specific hardware platforms ready for almost immediate use when the service provider is notified of a disaster. A hot site has all the equipment needed for the enterprise to continue operation, including office space and furniture, telephone jacks and computer equipment. Employees report to work at the hot site instead of the usual location. Subscriptions to commercial hot sites are based on the hardware specifications required to recover a "like" computer configuration. Subscriptions average 40 months' duration; cost from hundreds to hundreds of *thousands* of dollars (U.S.) per month, depending on the company's requirements. Contracts generally allow hot-site use for up to eight weeks in disaster mode.
- **Cold Site**. A cold site is an empty, environmentally conditioned computer room with office space, telephone jacks and so on, ready for the computer equipment to be moved in. The cold site is also available on a subscription basis, much more cheaply than a hot site—costing between $500 and $2,000 per month—but because the customer provides and installs all the equipment needed to continue operations, it takes longer to get an enterprise in full operation after the disaster. (Often such equipment is provided through a contract with an equipment leasing company.) Some hot-site providers generally include this cold-site service in the basic cost of a hot site for use after the subscriber has exceeded its occupancy time at the hot site. On the other hand, the vendor may allow only equipment included in the hot-site contract to be placed in the cold-site.
- **Mobile Site or Porta-Site**. Mobile computer/office environments available for smaller hardware configurations or emergency office environments. **Mobile sites** are stand-alone units on mobile trailers. **Porta-sites** are transported to the facility and constructed on-site. These options cost essentially the same as cold sites. The advantage of mobile sites is that they can be set up in a parking lot or other company area, bringing the work area to the end user.

Data Storage

- **Off-Site Storage**. Depending on budget and geographical risks, off-site storage for backup data on tape or disk could be the building next door, a bank safety deposit box or the branch office across town. A better choice is a secure, climate-controlled, fireproof media vault at a storage facility maintained by a commercial media storage provider. At higher cost, some vendors offer a service level of storage providing media that can quickly become live—sometimes called "electronic vaulting." Companies must ensure that contractually defined accessibility of the off-site copy meets original requirements, as for all outsourced elements of the business continuity solution.
- **Electronic Vaulting (or Advanced Recovery Services)**. Data is sent directly from the subscriber site to the hot site. This costly service requires that a direct-access storage device (DASD) be dedicated to the subscriber, preventing the service from being shared with other subscribers. PC/LAN electronic data vaulting is emerging as a popular service.
- **Remote Disk Mirroring**. Similar to electronic vaulting, but with the data updated continuously, remote mirroring eliminates the possibility of lost data. This arrangement usually costs more than vaulting because it often requires higher capacity WAN links. This approach does not reduce the amount of time that the affected data center is inoperative.

Technology Analysis

Tactics and Technologies

A wide variety of techniques, technologies and processes can support disaster recovery planning and implementation. Some of these tactics apply to everyday data management, but provide the additional benefit of enabling full and timely recovery. Tactics addressing major current continuity issues include:

- **Network Simplification**. Simpler IT infrastructure reduces costs overall, but it also facilitates continuity solution implementation because of the fewer objects on the network and the fewer differences among them, the easier it is to recover that infrastructure after a catastrophe.
- **Hosted Solutions and Application Service Providers** (**ASPs)**. Host vendors provide the necessary infrastructures and platforms for the client's applications, while ASPs outsource complete data center functions. Both can offer the advantage of reliability as long as the vendor's data center design has multiple, diverse fiber routes and provisions for disaster survival.

Supporting technologies can be used individually or in combination. Some technologies recently developed or advanced over previous versions include:

- **Expert Systems**. The expert system focuses on eliminating predictable outages (hardware or software failure and so on), identifying defects before they affect service.
- **Backup Power**. Beyond the data center, all user worksites must have power restoration capabilities to maintain operations.
- **Content Distribution Networks**. Distributing data reduces WAN cost and speeds data delivery to users by storing the data close to them. Distributing the data overcomes the single-point vulnerability of the traditional single data-center model.
- **Multiprotocol Label Switching (MPLS)-Enabled Frame Relay WAN Services**. Any-to-any connectivity enables a site to reach other company sites, as well as stand-by sites. With Internet Protocol (IP) routing performed in the MPLS core, all sites on the virtual private network (VPN) can now communicate "directly" to each other.
- **Load Balancing for Servers and Contact Centers**. Besides its operational efficiencies, load balancing reduces a company's vulnerability to a single outage—of one server or of an entire contact center.
- **Dual Data Writing for Mirrored Storage**. In support of remote disk mirroring, data is written simultaneously to two storage devices.
- **Phone Call Redirection**. Whatever the recovery location, continuity demands that phone calls destined for the original office be redirected easily to the stand-by site—through a company's private network or a third-party call-forwarding service.
- **Wireless Solutions**. Wireless LANs, cellular phones and 3G mobile offer the potential to provide backup when a wireline solution fails—if the local cellular service provider has the capacity to support the necessary volume of calling.
- **Voice Over IP (VoIP)**. VoIP offers cost savings, more efficient deployment of new integrated applications and sophisticated voice functionality. In addition, it increases security by replacing multiple networks with a single IP network to simplify planning and operational issues.

Business Use

Government entities, retailers with e-commerce channels, as well as finance (banking, securities and insurance), health and regulated utilities industries currently use business continuity products and services most heavily. Increasing reliance on e-business has added retailers with e-commerce channels, along with Internet service providers (ISPs) and ASPs, to this user group. Continuity planning and management has penetrated large to midsize companies across all industries, particularly those attempting compliance with industry regulations or the International Organization for Standardization (ISO900X/IEC) standards. Ironically, the 2002 British Government Department of Trade and Industry survey found that only 15 percent of people responsible for IT security were aware of the standards set forth in ISO 17799:

- **Government**—Federal regulatory legislation drives much industrial use of business continuity services. Governmental self-regulation to ensure continuity of all operations and services underwent heavy scrutiny during Y2K systems preparedness efforts. What probably contributed to the uneventful continuity of federal services through the Y2K episode was the array of Continuity of Operations Planning (COOP) Office of Management and Budget (OMB) circulars and presidential directives driving risk management for all federal agencies. Every U.S. federal department and agency has taken business continuity measures in accord with the COOP directives. All U.S. state governments and national governments worldwide have in place ongoing efforts to establish and expand continuity planning and management resources, including the TOPOFF exercises of the past three years and many local plan-testing activities that are part of continuous improvement efforts. Vendors doing business with government agencies must often demonstrate compliance with governmental regulations and industry best practices.
- **E-Commerce**—E-tailers, ISPs and ASPs have learned about the vulnerability of the Internet and e-commerce to business disruptions from the recent attacks suffered by prominent e-commerce companies, such as Yahoo, eBay, CCN News and America Online. These attacks come as e-business grows increasingly dependent on the reliability and availability demands by customers for online 24×365 service operations. Every major provider of business continuity resources now offers high-availability e-commerce recovery services at commercial hot sites.
- **Finance**—The U.K. Financial Services Act and similar legislation in most nations include comparable requirements. Even without regulation, the finance industry would have strong bottom-line motivation to avoid business disruption. In the U.S., the Gramm-Leach-Bliley Act, the Expedited Funds Availability Act and SAS70 audit reports require effective business continuity plans and resources. For example, the *FDIC Comptroller*'s *Handbook* requires national banks to include restoration of the Internet banking channel among the regularly tested elements of their business continuity plans. In September 2002, a *Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* proposes policies to enhance established continuity and recovery requirements to guard against systemic risks to critical markets. Although the white paper binds only core clearing and settlement organizations for federal funds, foreign exchange, commercial paper, USG and agency securities and corporate debt and equity securities, its proposed tactics guide industry trends. Recommended practices include:
  - Recovery objective of four hours or less after the event—moving toward an emerging industry objective of two hours.
  - Use of out-of-region recovery/resumption resources not dependent on the same labor pool or infrastructure components as the primary site.

  - Routine testing (and cross-institutional testing) of internal recovery and resumption arrangements for required connectivity, functionality and volume capacity.

- **Health**—Health-related businesses have always secured resources for ensuring the availability of service in the face of disruptive events. Since Congress adopted the Health Insurance Portability and Accountability Act (HIPAA) in 1996, the U.S. health industry (healthcare plans, providers and clearinghouses) has also had to implement standardized electronic claims and payment systems. Those systems became folded into established continuity strategies and spurred even greater development of well-managed plans and recovery resources. Since April 2003, HIPAA Privacy Rule compliance further requires protecting the privacy of patient information. In February 2003, the Department of Health and Human Services (HHS) published the final HIPAA Security Rule, which becomes effective 21 April 2005.
- **Regulated Utilities**—The continuity of power, telecommunications and water utilities is a critical assumption of the continuity plans for other public services (hospitals, police, fire/rescue, schools and other designated "shelters," and government offices) and large or regulated business and services (banks, insurance companies, brokerages, Internet communications services). As these entities' operations continuity needs have expanded into total business continuity, so have their plans and the software infrastructure supporting the plans themselves:
  - The U.S. Federal Communications Commission (FCC) oversees coordinated network service continuity planning by telecommunications carriers and other providers of telecommunications service.
  - The U.S. Environmental Protection Agency (EPA) enforces many environmental regulations, including its provisions for business continuity, to ensure the availability of safe power and water supplies and services despite disruption scenarios.
  - State Departments of Environmental Services and Public Utilities Commissions (in some states called Public Services Commissions) oversee enforcement of state Public Utilities Code legislation, ensuring reliability (continuity) of business and service. In other countries, national and regional governmental agencies enforce similar legislation requiring plans for continuity of critical infrastructure services after disruptive emergencies.

Benefits and Risks

Benefits

Business continuity support provides specific expertise and services that ensure a company's capability to cost-effectively maintain operations despite a crisis. Once the necessary types of support have been selected, the business continuity solution should present substantial benefits.

Efficient Resource Commitment and Task Allocation

The decision-making process for selecting vendors and apportioning tasks to them and to employees requires risk analysis and return-on-investment (ROI) consideration. That exercise demonstrates fiscal responsibility to all executives and to both internal and external auditors.

Reliable, Accurate Notification and Distribution in a Crisis

Software that includes distribution and notification capabilities helps to ensure that the right people—including disaster recovery service providers—receive immediate notice of recovery plan activation. Integrating the plan's "calling tree" database into the corporate employee contact information database

guarantees that the right parties receive each type of notification, with a minimum of database maintenance effort. Periodic tests ensure accuracy.

Thorough Plan Management Reporting and Updating

Version tracking is important to the risk management team, and periodic snapshots of the entire plan or elements of it are necessary for business functions, such as budgeting, staffing, regulatory reporting and competitive analysis.

Risks

Project Fails to Involve Employees From All Business Units

Overlooking employees from all business units incurs two major risks: (1) inadequate or improper planning of tactics and resources for those units and (2) lack of budgetary support from that unit for plan maintenance/testing.

Neglecting Review, Maintenance and Testing

Realistic testing of business continuity plans—so critical to recovery plan success—depends on the importance executives *beyond* the CIO/CTO place on business continuity. If other executives fail to support testing with budget and resource allocations, they fail to understand the importance of up-to-date plans for their own business units. They need to be reminded that plans are often updated based on points of failure during a test.

Committing to a Contract Without Performing Due Diligence

Without due diligence, an organization may be dazzled by impressive vendor Web sites and vendor-managed demonstrations, resulting in unrealistic expectations of a vendor's reputation, capabilities, support and policies. For example, even the best vendor may have higher priority clients (government, military, healthcare) in a particular region, putting another client's recovery at risk of delay.

Failure to Read the "Standard" Contract Clauses Carefully

"Standard" business continuity contracts may contain traps for the client (automatic renewal clauses) and back-door disclaimers for the vendor (exceptions to the recovery time commitment). For example, a *force majeure* clause is commonly present to excuse a vendor from liability in the event it fails to live up to contract obligations due to an unforeseen event outside the vendor's control—one that could not be avoided by exercise of "due care." Contract should include clear examples of such events. Otherwise, there is the risk that the vendor could fail to perform for reasons *within* its control. Be sure to review the service contract with an attorney well acquainted with such contracts.

Concentrating on the IT Department at the Expense the Business

While the IT function is well positioned to act as a facilitator, IT serves the business operations. Planning efforts must take into account *all* aspects of business continuity—data, finance, buildings, communications, equipment, personnel, customer service, knowledge assets and so on. Otherwise, if the IT department is the only part of the company prepared for disaster, the result could be a nice safe data center but no way for the business units to operate or communicate with their systems.

Standards

International, Cross-Industry Standards

- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17799:2000 *Information Technology—Code of Practice for Information Security Management*, an international version of British Standard 7799-1:1999, was published in December 2000. It contains 10 major sections, one of which is business continuity management (Section 11); however, parts of Physical and Environmental Security (7), Asset Classification and Control (5) and Security Policy (3) would also apply. Section 11 of ISO 17799 is devoted solely to business continuity and disaster recovery.
- ISO/IEC Technical Report (TR) 13335, *Guidelines for the Management of IT Security* (*GMITS*), 13335-2: *Managing and Planning IT Security*, contains requirements for procedural security, including business continuity.
- ISO 9002 quality assurance model applies to organizations that produce, install and service products. It implies industry standards for IT Security and the broader subject of general product security, including continuity planning for IT systems—both as products themselves and as environmental support—and all other aspects of business operations (physical, environmental, personnel) whose disruption would affect product security.
- NIST Special Publications (SP) 800 Series (parts 3, 4, 12, 14, 16 and 18) require contingency, disaster recovery and continuity of operations plans.

Industry-Specific Standards and Regulations

U.S. Federal Government

Government agencies with essential missions at federal, state and local levels have always had continuity plans. The COOP directives produced by the Office of Management and Budget (OMB) and the President of the United States outline the objectives of business continuity planning for all federal departments and agencies. Examples are as follows:

- **Presidential Decision Directive (PDD) 67**, issued 21 October 1998, requires federal agencies to develop Continuity of Operations Plans for Essential Operations.
- **PDD 63**, issued in May 1998, calls for a national effort to ensure the security of the United States' critical infrastructures—the physical and cyber-based systems essential to the minimum operations of the economy and government. It sets a goal of a reliable, interconnected and secure information system infrastructure by the year 2003 and requires the federal government to serve as a model to the rest of the country for how infrastructure protection is to be attained.
- **OMB Circular A-130**, Appendix III, "Security of Federal Automated Information Resources," published in 1993, ensures that appropriate business continuity plans were put in place for all federal general-purpose systems and major applications, which include the mission-critical applications identified under the Y2K program.
- **Executive Order 12656** (Section 202) of 1988 requires the head of each federal department and agency to ensure the continuity of essential functions in national security emergencies by providing for safekeeping of essential resources, facilities, and records and establishment of emergency operating capabilities.

Finance

- **The Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System**, in its new version issued 18 April 2003, holds legal weight—unlike the original version, which provided regulatory guidance. Under this version, the Office of the Comptroller of the Currency (OCC) will take action against banks that fail to comply with the document requirements for disaster recovery by the U.S. financial system. The new version gives firms more latitude to determine the distance between their live and recovery sites, an issue that drew much negative reaction during the comment period for the original plan.
- **Federal Financial Institutions Examination Council (FFIEC) Information Systems Examination Handbook** 2003 update is being updated in separate booklets that will eventually replace the original Handbook. One booklet guides examiners evaluating financial institution and service provider risk management processes for availability of critical financial services. The booklet for supervision of technology service providers guides examination of services performed for financial institutions. It emphasizes that the ultimate responsibility resides with an institution's management and board of directors to ensure outsourced activities are conducted in a safe and sound manner, in compliance with related laws and regulations.
- **Basel Committee on Banking Supervision, Bank for International Settlements (BIS), Publication 82—Risk Management for Electronic Banking, Principle 13: The Third Consultative Paper** (published 28 April 2003) contains the final modifications to its proposal for a new capital adequacy framework. The new capital adequacy framework places new demands on BC and DR for financial services. The BIS's September 2002 update of its "Sound Practices for the Management and Supervision of Operational Risk" provides a framework for effective management and supervision of operational risk by banks and supervisory authorities when evaluating operational risk management policies and practices. The original May 2001 publication states that banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services. Expected completion date is fourth quarter of 2003, with implementation effective in member countries by year-end 2006.
- **The U.S. Sarbanes-Oxley Act (SOX)**, a new rule issued by the SEC on 31 October 2002, responds to revelations of executive and auditing malfeasance scandals by expanding the requirements for corporate reporting for auditors, managers and audit committees. Auditing firms, for example, must keep for at least seven years *every* document that influences its report about a client, including such bits as a CEO's e-mail or a sticky note with some figures on it. Evolving legal interpretations of the rules imply that, pragmatically, every public (and possibly private) company must keep these records too in order to avoid liability in an unforeseeable investigation. The preservation of the systems which process and store these records takes on increased importance.
- **Gramm-Leach-Bliley Act** of 1999 (compliance deadline 1 July 2001), Section 501(b) Financial Institutions Safeguards, requires that the agencies described in Section 505(a) establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical and physical safeguards for the security and confidentiality of customer records and information.
- **SAS70 Reports** (1993) in accord with a statement on Auditing Standards Number 70 issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA)—review the processing of transactions by service organizations, such as electronic data processing (EDP) centers and banks. SAS70 reports must be performed by certified external auditors, who examine

general computer controls, qualified service providers, participant eligibility, and claim system application controls and review the findings with management.

- **The Expedited Funds Availability (EFA) Act**, enacted by the U.S. Controller of Currency on 1 January 1989, requires federally chartered financial institutions to have a demonstrable business continuity plan to ensure prompt availability of funds. Regulation CC (12 C.F.R. Part 229) from Board of Governors of the Federal Reserve System implements the EFA. The regulation also establishes rules for the prompt collection and return of unpaid checks. Regulation CC contains three subparts. Subpart A defines terms and describes administrative enforcement. Subpart B specifies availability time frames within which banks must make funds available for withdrawal. Subpart C establishes the rules to ensure the speedy return of checks, the responsibilities of paying and returning banks, authorization of direct returns, notification of nonpayment of large-dollar returns by the paying bank, check endorsement standards and other charges related to the check collection system.

Health

- **HIPAA**—In April 2003, the U.S. HIPAA Privacy Rule to protect patients' health information went into effect. The Privacy Rule affects all forms of protected information, including oral and hand-written communications, as well as the electronic forms covered in the original 1996 Act, which requires healthcare plans, providers and clearinghouses to adopt standardized electronic claims and payment systems. Noncompliance fines start at $100 for failure to meet a standard, but range up to $250,000 and 10 years' imprisonment for the wrongful use or disclosure of individual health information for commercial advantage, personal gain and the like. Also, accreditation agencies, such as the Joint Commission on Accreditation of Health Care Organizations (JCAHO), inspect for compliance during their accreditation process. In February 2003, the Department of HHS published the HIPAA Security Rule, which becomes effective 21 April 2005. The Security Rule applies only to patient-identified electronic Protected Health Information (PHI). The electronic signature standard has been removed, although HHS states that it will be published later as a separate regulation. Section 164.306(a) of the Security Rule states four general requirements for covered entities, from which many specific standards and implementation specifications derive. Some of the implementation specifications associated with the standards in the Security Rule are required, and the others are addressable.
- **Food and Drug Administration's (FDA's) Code of Federal Regulations (CFR), Title XXI, 1999**—The rule establishes the requirements for electronic records and electronic signatures to be considered trustworthy, reliable and essentially equivalent to paper records and handwritten signatures executed on paper. It applies to any electronic-format records covered by FDA regulations, including records that are required to be maintained whether or not they are submitted to the FDA.

Utilities

The Telecommunications Act of 1996, Section 256, "**Coordination for Interconnection,**" requires the FCC to establish procedures to oversee coordinated network planning by telecommunications carriers and other providers of telecommunications service. It also permits the FCC to participate in the development of public network interconnectivity standards by appropriate industry standards-setting bodies. The act recognizes the need for disaster recovery plans, but also acknowledges the existence of inadequate testing because of the rapid deployment of new technologies.

Information Technology (Outsourced Services and Corporate Departments)

The National Institute of Standards and Technology (NIST) Special Publication 800-34, ***Contingency Planning Guide for Information Technology Systems*** **(2002),** defines detailed recommendations from the NIST, a division of the Technology Administration of the U.S. Department of Commerce. It joins the NIST Special Publications (SP) 800 series (parts 3, 4, 12, 14, 16, 18 and now 34) requiring contingency, disaster recovery and continuity of operations plans. While the document serves as official guidance only to U.S. government agencies, IT professionals in all industries pay due attention to such publications. SP 800-34 asserts that successful contingency planning management must ensure (1) understanding of the IT Contingency Planning Process and its place within the overall Business Continuity Plan process; (2) development or re-examination of contingency policy and planning process and application of the elements of the planning cycle, including preliminary planning, business impact analysis, alternate site selection and recovery strategies; and (3) development or re-examination of IT contingency planning policies and plans with emphasis on maintenance, training and exercising the contingency plan.

Price vs. Performance

Who Pays for Business Continuity and Recovery—And How Much?

For a company to stay in business during a disruptive event and to continue in business in the months and years that follow requires more than allocating a small percentage (averaging 4 percent) of the data center budget. All essential departments and functions must continue to operate at something approaching normal productivity.

The data center is only one part of the organization that must consider the need for business continuity.

Therefore, since business continuity and recovery strategies and tools benefit the entire organization, the costs of the business continuity program are best borne by all operational and support units. For Business Continuity Planning software, costs range from about $10,000 for one or two locations with one to three planners, up to a high of $175,00 for a Web-server license with many users, and an average of 15 percent annual maintenance contract. Disaster Recovery vendor prices vary so widely depending on the size of the company and scope of its requirements that no standard price range is meaningful; planners should request pricing for a consistent set of criteria from several Disaster Recovery vendors.

Selection Guidelines

Each company's selection of a business continuity solution must rely on its unique impact and risk analyses as guidelines. The "best" solution for business continuity planning and management will consist of the right mix of internal controls and tools with outsourced services that will meet the company's requirements for managing physical, technological, legal, regulatory and human resource aspects of business continuity. These elements may include:

- Business Continuity Planning software
- Business Continuity Planning consulting service
- Data backup and storage services and facilities (owned or leased)
- Business (physical and data) restoration facilities and services (owned or leased)
- Insurance for losses
- Documentation of regulatory compliance

Ongoing review and testing of the continuity plan and recovery resources is essential, as the initial solution will change over time, depending on the company's reliance on rapidly changing technologies, the existence of manual workarounds for technological failure and each operation site's exposure to environmental risk factors, such as power outages and natural disasters. With many vendors encompassing several aspects of business continuity, the purchaser of continuity and recovery services needs to perform rigorous due diligence in evaluating vendors and services.

Create a Balance Between Internal and Outsourced Elements

Once identified, the components of the continuity solution range across the spectrum from fully internal to fully outsourced elements. Again, each company must determine its own best balance between full internal resources and their management, or management of some internal resources and some outsourced services, or fully outsourced continuity management and resources. Each option has its apparent costs, as well as hidden costs—particularly the hidden costs of internal resource maintenance and management.

A decision process may include a variety of risk/value/cost considerations:

- Survey key players in every business unit to ensure that no data resources are omitted in determining: What is the cost of system downtime? What is the cost of private data becoming public?
- Which business information, processes and their supporting systems require 24×365 availability?
- What are the most likely disruptive occurrences at each corporate site?
- Which solutions are most readily available for each type of crisis?
- Which solutions for prevention and recovery meet the systems' availability demands cost-effectively?

Choose the Right Fit for the Shape of the Organization

Initiating a business continuity and disaster recovery plan and managing it first demand an assessment of what the company needs from the plan overall, then a determination of what internal resources exist and selecting external resources to fill in the gaps. Then the work of plan development and maintenance begins. The table *Business Continuity Planning and Management Solution Development Process* presents a potential path to follow and outlines possible options and deliverables along the way. Each organization will follow a different path, based on its initial needs assessment.

Table 1: Business Continuity Planning and Management Solution Development Process

Phase 1: Develop the Foundation	
Considerations	**Solution Options**
Is there executive support across all units of the organization?	• Advisement-only consultant • Consulting service from established hardware and software vendors • Software for business impact analysis (BIA) and risk assessment with or without the software vendor's consulting service

Table 1: Business Continuity Planning and Management Solution Development Process	
Phase 1: Develop the Foundation	
Considerations	**Solution Options**
Needs: • BIA • Risk Assessment	**Deliverables**: • BIA report with values of all assets and costs of all disruption scenarios • Risk assessment report with risk/benefit analysis and continuity priorities
Develop the Foundation: Points to Consider for Consultant or Software Selection:	
• Whether the organization needs the objectivity of an external analyst • Account management motives of product and service vendors who offer initial analysis free/inexpensively	
Phase 2: Develop the Plan	
Considerations	**Solution Options**
Does the organization have in-house expertise in continuity planning and management?	• Advisement-only consultant • Consulting service from established hardware vendor • Software for business continuity planning with or without the software vendor's consulting service
Needs: • Business units' established continuity plans (if any) • BCPM team member identification • Prioritization of continuity-targeted operations and systems • Comparison pricing among alternative solutions • Comparison pricing among competing vendors of each solution • Selection of resources for crisis prevention and rapid recovery • Allocation of funding for plan implementation and maintenance	**Deliverables**: • Matrix of established plans and recommended adoption of best practices • Business continuity roles/responsibilities and call list • Operations and systems priority list • Business continuity requirements (specifications for request for proposal [RFP]) • Solution cost comparison and recommendations • Vendor cost comparison and recommendations • RFP developed and sent to potential vendors • Vendor proposals evaluated and ranked for recommendation • Funding allocated for plan implementation and maintenance
Develop the Plan: Points to Consider for Consultant, DR Resource and Software Vendor Selection:	
• Objectivity of internal assessment vs. external analyst • Account management motives of hardware and software vendors • Years of experience in clients similar to your company • Current client evaluations of the vendor • The vendor's short- and long-term growth plans • Scalability of the vendor's platform to support your company's new capabilities • The vendor's strategic partners	

Table 1: Business Continuity Planning and Management Solution Development Process	
Phase 1: Develop the Foundation	
Considerations	**Solution Options**
Phase 3: Maintain the Plan	
Considerations	**Solution Options**
Does the organization have sufficient internal resources to carry out this effort?	• Advisement-only consultant • Consulting service from established hardware vendor • Software for business continuity with or without the software vendor's consulting service
Needs: • Employee training on continuity procedures • Automated (or manual) update of plan resource lists to reflect current corporate data • Automated (or manual) notification of plan updates • Test trigger events and scheduled tests • Performance of triggered and scheduled tests • Evaluation of test results • Implementation of post-test plan updates	**Deliverables**: • Continuity procedures employee training package • Methodology description for update of plan resource lists to reflect current corporate data • Methodology description for notification of plan updates • List of test trigger events and scheduled tests • Methodology description for performance of triggered and scheduled tests • Methodology description for test results evaluation • Methodology description for post-test plan update implementation
To Maintain the Plan: Points to Consider for Vendor Review and Assessment (in previous contract period):	
• Track record of success for crisis avoidance • Track record of success for rapid recovery (mean time to repair [MTTR] statistics) • Priority of the business's industry among the vendor's clients in the same region	

Technology Leaders

The hot-site industry—offering full data centers for client companies that need to relocate in an emergency—has successfully recovered hundreds of companies since its inception in the early 1980s. A large number of those recoveries resulted from regional events affecting multiple subscribers simultaneously, with no client ever having been denied access to a recovery facility because of excessive demand.

Major Vendors in the Business Continuity Market

Today, vendors offer a broad spectrum of services for business continuity—continuity plan development and maintenance, and plan activity implementation and management, including disaster recovery. Some vendors, like **IBM Business Continuity and Recovery Services** and **SunGard Availability Services**, offer a wide range of services. Services can include risk analysis and management, disaster avoidance, consultation, recovery centers, and a range of business continuity and planning services, including hot sites. Other companies, such as **Business Protection Systems**, **LBL Technology Partners, Rentsys Recovery Systems** and **RSM McGladrey**, specialize in one niche, such as business continuity planning software, or in one geographic area:

- **Agility Recovery Solutions** (formerly GE Disaster Recovery Services) was re-named effective 9 September 2002, following its purchase by a private investment firm. GE Capital IT Solutions remains a primary supplier of inventory. Agility offers mobile recovery, guaranteed technology replacement (quickship) and consulting.
- **Business Protection Systems International (BPSI)** offers the **Business Protector** suite of tools for creating and maintaining business continuity plans. The scalable Business Protector Web- and PC-based tools can meet the needs of various company sizes, budgets and continuity planning knowledge.
- **Comdisco**—see *SunGard Availability Services*.
- **Computer Alternate Processing Sites (CAPS)** offers consulting, including business continuity planning, BIA, hot sites and online business continuity planning through the RecoveryPlanner product.
- **Computer Security Consultants, Inc. (CSCI),** offers the **RecoveryPAC** software product. Its recovery planner combines with its data collection utility and multiple database features to facilitate plan maintenance.
- **GE Disaster Recovery Services**—see *Agility Recovery Solutions*.
- **Hewlett-Packard Business Continuity and Recovery Services** offers planning and testing, hot sites, mobile recovery, consulting and managed services.
- **IBM Business Continuity and Recovery Services** (a business unit within IBM Global Services) offers consulting, including risk analysis and management; crisis management; recovery assessment and planning; recovery services—including fully equipped hot sites; and managed continuity services.
- **LBL Technology Partners** offers the **LBL Contingency Planner**, knowledge-based software fully integrated with the Microsoft Office Suite. The product automates plan development through hundreds of electronic tools, guides, templates and samples.
- **Recovery Point Systems** offers a comprehensive "single point" **Integrated Disaster Recovery Site (IDRS)** in Gaithersburg, Maryland. Designed for rapid recovery of high-availability business functions. Recovery Point serves a diverse array of commercial and government clients.
- **Rentsys Recovery Services** offers a backup/recovery facility near Boston (Billerica, Massachusetts) with 300 end-user recovery seats and a separate large system remote customer suite for rapid recovery of high-availability business functions, with conference rooms, a dining area and workout facility, and an on-site hotel. In addition, Rentsys offers data vaulting, quick-ship, mobile recovery facilities and continuity planning consulting.
- **RSM McGladrey** offers **Business Continuity Planning System** software, which provides automated risk assessment and business impact analysis, interface capability to third-party project management products, plan audit module, automated advice, and Internet backup and restore procedures.
- **Strohl Systems** BCP software tools provide business impact analysis and a continuity plan builder with plan templates, an Open Database Connectivity (ODBC)-compliant relational database, foreign language modules, automated importing and printing, plan notification and approval, and simplified security. Corporate network and Web versions support collaborative planning.

- **SunGard Availability Services** offers a full range of information availability services, including hot sites. A subsidiary, SunGard Planning Solutions, provides business continuity planning software and consulting services. Services and products reflect 2001 acquisition of Comdisco.

Table 2: Business Continuity Vendors at a Glance

	Full-Service Consulting	Management Services	BCP Software	Hot Sites	Cold Sites	Off-Site Data Storage	Hardware Quick Ship
Full-Service, Diverse Capability Vendors							
Agility Recovery Solutions (formerly GE Disaster Recovery Services)	•			•			•
CAPS	•		•	•		•	
GE Disaster Recovery Services —see *Agility Recovery Solutions*							
Hewlett-Packard Business Continuity and Recovery Services	•	•		•		•	•
IBM Business Continuity and Recovery Services (a business unit within IBM Global Services)	•	•		•	•	•	•

Table 2: Business Continuity Vendors at a Glance							
	Full-Service Consulting	Management Services	BCP Software	Hot Sites	Cold Sites	Off-Site Data Storage	Hardware Quick Ship
Full-Service, Diverse Capability Vendors							
SunGard Availability Services	•	•	•	•	•		
Industry Niche or Regional Vendors							
BPSI	•		•				
CSCI			•				
LBL Technology Partners	•		•				
Recovery Point Systems		•		•		•	•
Rentsys Recovery Services	•			•		•	•
RSM McGladrey	•		•				
Strohl Systems	•		•				

Insight

A companywide business impact analysis—leading to a practical business continuity strategy and a detailed contingency plan—can deliver significant benefits. An analysis of this type requires the active involvement of all levels and all departments of the company. A business continuity strategy that is complete, testable and maintainable will likely satisfy both stockholders and regulators. And clearly established tactics for responding to business disruptions—especially tactics that ensure the continuity of high-value communications with employees, external partners and other stakeholders—will significantly reduce the damage caused by unforeseen, and sometimes unforeseeable, business disruptions. The bottom line: Resilient companies are resilient because they *plan* for resilience.