NASCIO
Representing Chief Information Officers of the States

IT Disaster Recovery and Business Continuity Tool-kit: Planning for the Next Disaster

NASCIO Staff Contact:
Drew Leatherby,
Issues Coordinator
dleatherby@AMRms.com

Without the flow of electronic information, government comes to a standstill. When a state's data systems and communication networks are damaged and its processes disrupted, the problem can be serious and the impact far-reaching. The consequences can be much more than an inconvenience. Serious disruptions to a state's IT systems may lead to public distrust, chaos and fear. It can mean a loss of vital digital records and legal documents. A loss of productivity and accountability. And a loss too of revenue and commerce.

Disasters that shut down a state's mission critical applications for any length of time could have devastating direct and indirect costs to the state and its economy that make considering a disaster recovery and business continuity plan essential. State Chief Information Officers (CIOs) have an obligation to ensure that state IT services continue in the state of an emergency. The good news is that there are simple steps that CIOs can follow to prepare for **B**efore, **D**uring and **A**fter an IT crisis strikes. Is your state ready?

Disaster Recovery Planning 101

Disaster recovery and business continuity planning provides a framework of **interim measures** to recover IT services following an emergency or system disruption. **Interim measures** may include the relocation of IT systems and operations to an alternate site, the recovery of IT functions using alternate equipment, or execution of agreements with an outsourced entity.

IT systems are vulnerable to a variety of disruptions, ranging from minor short-term power outages to more-severe disruptions involving equipment destruction from a variety of sources such as natural disasters or terrorist actions. While many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of the state's overall risk management effort, it is virtually impossible to completely eliminate all risks.

In many cases, critical resources may reside outside the organization's control (such as electric power or telecommunications), and the organization may be unable to ensure their availability. Thus effective disaster recovery **planning**, **execution**, and **testing** are essential to mitigate the risk of system and service unavailability. Accordingly, in order for disaster recovery planning to be successful, the state CIO's office must ensure the following:

1. Critical staff must understand the IT disaster recovery and business continuity planning process and its place within the overall Continuity of Operations Plan and Business Continuity Plan process.
2. Develop or re-examine disaster recovery policy and planning processes including preliminary planning, business impact analysis, alternate site selection, and recovery strategies.
3. Develop or re-examine IT disaster recovery planning policies and plans with emphasis on maintenance, training, and exercising the contingency plan.

NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States. For more information visit www.nascio.org.

201 East Main Street, Suite 1405
Lexington, KY 40507
Phone: (859) 514-9153
Fax: (859) 514-9166
Email: NASCIO@AMRms.com

How to Use the Tool-kit

This **tool-kit** represents an updated and expanded version of business continuity and disaster preparedness checklists utilized for a brainstorming exercise at the "*CIO-CLC Business Continuity/ Disaster Recovery Forum*" at NASCIO's 2006 Midyear Conference. This expanded tool-kit evolved from the work of NASCIO's Disaster Recovery Working Group, www.NASCIO.org/Committees/DisasterRecovery. Along with NASCIO's DVD on disaster recovery, "Government at Risk: Protecting Your IT Infrastructure." (View video or place order at: www.NASCIO.org/Committees/DisasterRecovery/DRVideo.cfm), these checklists and accompanying group brainstorming worksheets will serve as a resource for state CIOs and other state leaders to not only better position themselves to cope with an IT crisis, but also to help make the business case for disaster recovery and business continuity activities in their states.

The tool-kit is comprised of six checklists in three categories that address specific contingency planning recommendations to follow **B**efore, **D**uring and **A**fter a disruption or crisis situation occurs. **The Planning Phase, Before the disaster,** describes the process of preparing plans and procedures and testing those plans to prepare for a possible network failure. **The Execution Phase, During the disaster,** describes a coordinated strategy involving system reconstitution and outlines actions that can be taken to return the IT environment to normal operating conditions. **The Final Phase, After the disaster,** describes the transitions and gap analysis that takes place after the disaster has been mitigated. The tool-kit also provides an accompanying group activity worksheet, "***Thinking Sideways***," to assist in disaster recovery planning sessions with critical staff.

IT Disaster Recovery and Business Continuity Checklists

Before the Crisis

(1) Strategic and Business Planning Responsibilities (Building relationships; What is the CIO's role on an ongoing basis? Role of enterprise policies?)

(2) Top Steps States Need to Take to Solidify Public/ Private Partnerships Ahead of Crises (Pre-disaster agreements with the private sector and other organizations.)

(3) How do you Make the Business Case on the Need for Redundancy? (Especially to the state legislature, the state executive branch and budget officials.)

(4) General IT Infrastructure and Services (Types of redundancy; protecting systems.)

During the Crisis

(5) Tactical Role of CIOs for Recovery During a Disaster (Working with state and local agencies and first responders; critical staff assignments; tactical use of technology, e.g. GIS.)

After the Crisis

(6) Tactical Role of CIOs for Recovery After a Disaster Occurs (Working with state and local agencies, and critical staff to resume day-to-day operations, and perform gap analysis of the plan's effectiveness.)

Before the Crisis

(1) Strategic and Business Planning Responsibilities (Building relationships; What is the CIO's role on an ongoing basis? Role of enterprise policies?)

- ❑ **CIOs need a Disaster Recovery and Business Continuity (DRBC) plan including: (1)** Focus on capabilities that are needed in any crisis situation; **(2)** Identifying functional requirements; **(3)** Planning based on the degrees of a crisis from minor disruption of services to extreme catastrophic incidents; **(4)** Establish service level requirements for business continuity; **(5)** Revise and update the plan; have critical partners review the plan; and **(6)** Have hard and digital copies of the plan stored in several locations for security.

  Notes: _____

- ❑ **CIOs should ask and answer the following questions: (1)** What are the top business functions and essential services the state enterprise can not function without? **Tier business functions and essential services into recovery categories based on level of importance and allowable downtime. (2)** How can the operation's facilities, vital records, equipment, and other critical assets be protected? **(3)** How can disruption to an agency's or department's operations be reduced?

  Notes: _____

- ❑ **CIOs should create a business resumption strategy:** Such strategies lay out the interim procedures to follow in a disaster until normal business operations can be resumed. Plans should be organized by procedures to follow during the first 12, 24, and 48 hours of a disruption. (Utilize technologies such as GIS for plotting available assets, outages, etc.)

  Notes: _____

- ❑ **CIOs should conduct strategic assessments** and inventory of **physical assets**, e.g. computing and telecom resources, identify alternate sites and computing facilities. Also conduct strategic assessments of **essential employees** to determine the staff that would be called upon in the event of a disaster and be sure to include pertinent contact information.

  Notes: _____

- ❑ **CIOs should conduct contingency planning in case of lost personnel:** This could involve cross-training of essential personnel that can be lent out to other agencies in case of loss of service or disaster; also, **mutual aid agreements** with other public/private entities such as state universities for "skilled volunteers." (Make sure contractors and volunteers have approved access to facilities during a crisis).

  Notes: _____

- ❑ **Build cross-boundary relationships with emergency agencies:** CIOs should introduce themselves and build relationships with state-wide, agency and local emergency management personnel – you don't want the day of the disaster to be the first time you meet your emergency management counterparts. Communicate before the crisis. Also consider forging multi-state relationships with your CIO counterparts to prepare for multi-state incidents. Consider developing a cross-boundary DR/BC plan or strategy, as many agencies and jurisdictions have their own plans.

  Notes: _____

- ❑ **Intergovernmental communications and coordination plan:** Develop a plan to communicate and coordinate efforts with state, local and federal government officials. Systems critical for other state, local and federal programs and services may need to be temporarily shut down during an event to safeguard the state's IT enterprise. Local jurisdictions are the point-of-service for many state transactions, including benefits distribution and child support payments, and alternate channels of service delivery may need to be identified and temporarily established. Make sure **jurisdictional authority** is clearly established and articulated to avoid internal conflicts during a crisis.

  Notes: _____

- ❑ **Establish a crisis communications protocol:** A crisis communications protocol should be part of a state's IT DR/BC plan; Designate a **primary media spokesperson** with additional single point-of-contact communications officers as back-ups. Articulate who can speak to whom under different conditions, as well as who should not speak with the press. In a time of crisis, go public immediately, but only with what you know; provide updates frequently and regularly.

  Notes: _____

- ❑ **Communicate to rank and file employees** that there is a plan, the why and how of the plan, and their roles during a potential disruption of service or disaster. Identify members of a possible crisis management team. Have in place their roles, actions to be taken, and possible scenarios. Have a list of their office, home, and cell or mobile phone numbers.

  Notes: _____

- ❑ **Testing:** CIOs should conduct periodic training exercises and drills to test DR/BC plans. These drills should be pre-scheduled and conducted on a regular basis and should include both desk-top and field exercises. Conduct a **gap analysis** following each exercise.

  Notes: _____

- ❑ **A CIO's approach to a DR/BC plan** will be unique to his or her financial and organizational situation and the availability of trained personnel. This still leaves the question as to who writes the plans. If a CIO chooses from one of the many consultants that provide Continuity of Operations planning, he or she should make sure that staff maintains a close degree of involvement and, when completed, that the consultant(s) provide general awareness **training** of the plan. If CIOs choose to conduct planning in-house, have an experienced and certified business continuity planner review it for any potential gaps or inconsistencies.

  Notes: _____

(2) Top Steps States Need to Take to Solidify Public/ Private Partnerships Ahead of Crises (Pre-disaster agreements with the private sector and other organizations.)

- ❑ **Utilize preexisting business partnerships:** Keep the dialogue open with state business partners; periodically call them all in for briefings on the state's disaster recovery and business continuity (DR/BC) plans.

  Notes: _____

- ❑ **Set up "Emergency Standby Services and Hardware Contracts:"** Have contracts in place for products and services that may be needed in the event of a declared emergency. Develop a contract template so a contract can be developed with one to two hours work time.

  Notes: _____

- ❑ **Outsourced back-up sites may be time limited;** therefore back-up, back-up outsourcing may be necessary for continuity leap-frog.

  Notes: _____

- ❑ **Place advertisements** in the state's "Contract Reporter" every quarter; continuous recruitment is a good business practice.

  Notes: _____

- ❑ **Be sure essential IT procurement staff are part of the DR/BC plan** and are aware of their roles in executing pre-positioned contracts in the event of a disaster; also be sure to include pertinent contact information.

  Notes: _____

- ❑ **CIOs should develop** "**Emergency Purchasing Guidelines**" for agencies and have emergency response legislation in place.

  Notes: _____

- ❑ **Think outside the box:** CIOs can partner with anyone, e.g. universities, local government, lottery corporations, local companies and leased facilities with redundant capabilities.

  Notes: _____

(3) How do you Make the Business Case on the Need for Redundancy? (Especially to the state legislature, the state executive branch and budget officials.)

Risk assessment of types of disasters that could lead to the need for business continuity planning:

- **Geological hazards** – Earthquakes, Tsunamis, Volcanic eruptions, Landslides/ mudslides/ subsidence;
- **Meteorological hazards –** Floods/ flash floods, tidal surges, Drought, Fires (forest, range, urban), Snow, ice, hail, sleet, avalanche, Windstorm, tropical cyclone, hurricane, tornado, dust/sand storms, Extreme temperatures (heat, cold), Lightning strikes;
- **Biological hazards** – Diseases that impact humans and animals (plague, smallpox, Anthrax, West Nile Virus, Bird flu);
- **Human-caused events –** Accidental: Hazardous material (chemical, radiological, biological) spill or release; Explosion/ fire; Transportation accident; Building/structure collapse; Energy/power/utility failure; Fuel/resource shortage; Air/water pollution, contamination; Water control structure/dam/levee failure; Financial issues: economic depression, inflation, financial system collapse; Communications systems interruptions;
- **Intentional** – Terrorism (conventional, chemical, radiological, biological, cyber); Sabotage; Civil disturbance, public unrest, mass hysteria, riot; Enemy attack, war; Insurrection; Strike; Misinformation; Crime; Arson; Electromagnetic pulse.

❑ **Education and awareness:** Craft an education and awareness program for IT staff, lawmakers and budget officials to ensure all parties are on the same page with regards to your DR/BC plan and the need for such a plan. Prepare key talking points that outline the rationale for DR/BC planning. Utilize outside resources such as this tool-kit and NASCIO's DVD on disaster recovery, ***"Government at Risk: Protecting Your IT Infrastructure,"*** to help make the business case for disaster recovery and business continuity activities in your state.

Notes: _____

_____

_____

❑ **For federally declared states of emergency** the financial aspect has been somewhat lessened by the potential of acquiring funding grants from state or federal organizations such as FEMA. Additional funding for state cybersecurity preparedness efforts is available to states through the U.S. Department of Homeland Security's State Homeland Security Grants Program.

Notes: _____

_____

_____

❑ **Establish metrics for costs of not having redundancy:** How much will it cost the state if certain critical business functions go down – e.g. ERP issues on the payment side; citizen service issues (what it would do to the DMV for license renewals); impacts on eligibility verifications for social services, etc. How long can you afford to be down? How much is this costing you? How long can you be without a core business function?

Notes: _____

_____

_____

❑ **Up-front savings:** States obtain greater leverage for fair pricing and priority service in the event of an emergency before the emergency occurs, rather than after the emergency has occurred.

Notes: _____

_____

_____

❑ **Consider channels of delivery:** Child support payments channeled through a broker agency.

Notes: _____

_____

_____

- ❑ **Consider cycles of delivery:** The most important periods of delivery, e.g. the last week or couple of days of the month may be the most critical back-up period.

  Notes: _____

  _____

  _____

- ❑ **Realize that as the adoption rate for electronic business processes** and **online services** grows, employees with knowledge of business rules and paper processes will retire and will no longer be around for manual backup.

  Notes: _____

  _____

  _____

(4) General IT Infrastructure and Services (Types of redundancy; protecting systems.)

- ❑ **CIOs need to ensure that information is regularly backed up**. Agencies need to store their back-up data securely off site in a location that is accessible but not too near the facility in question. Such locations should be equipped with hardware, software and agency data, ready for use in an emergency. (Restore functions should be tested on a regular basis.) These "hot sites" can be owned and operated by an agency or outsourced.

  Notes: _____

- ❑ **Protect current systems:** Controlled access; uninterruptible power supply (UPS); back-up generators with standby contracts for diesel fuel (use priority and back-up fuel suppliers that also have back-up generators to operate their pumps in the event of a widely spread power outage).

  Notes: _____

- ❑ **Strategic location:** Locate critical facilities away from sites that are **vulnerable** to natural and man-made disasters.

  Notes: _____

- ❑ **Interactive voice response (IVR) systems** that are accessing back-end databases: (There may be no operators for backup that can connect patrons to services.) Seek diversity of inbound communications.

  Notes: _____

- ❑ **Self-healing communications systems** that automatically re-route communications or use alternate media.

  Notes: _____

- ❑ **Mobile communication centers** can be utilized in the event that traditional telecommunications systems are down.

  Notes: _____

- ❑ **Self-healing primary point of presence facilities** that automatically restore service.

  Notes: _____

- ❑ **Approach enterprise backup as a shared service:** Other agencies may have the capability for excess redundancy.

  Notes: _____

- ❑ **Provide secure remote access** to state IT systems for essential employees (access may be tiered based on critical need.)

  Notes: _____

- ❑ **Hot Sites:** A disaster recovery facility that mirrors an agency's applications databases in real-time. Operational recovery is provided within minutes of a disaster. These can be provided at remote locations or outsourced to one or multiple contractors.

  Notes: _____

During the Crisis

(5) Tactical Role of CIOs for Recovery During a Disaster (Working with state and local agencies and first responders; critical staff assignments; tactical use of technology, e.g. GIS.)

- ❑ **Decision making:** Prepare yourself for making decisions in an environment of uncertainty. During a crisis you may not have all the information necessary, however, you will be required to make immediate decisions.

  Notes: _____

- ❑ **Execute DR/BC Plan:** Retrieve copies of the plan from secure locations. Begin systematic execution of plan provisions, including procedures to follow during the first 12, 24, and 48 hours of the disruption.

  Notes: _____

- ❑ **Shutdown non-essential services** to free up resources for other critical services. Identify critical business applications and essential services and tier them into recovery categories based on level of importance and allowable downtime, e.g. tier III applications are shut down first. Be sure to classify critical services for internal customers vs. external customers.

  Notes: _____

- ❑ **Communicate, communicate, communicate:** Engage your **primary media spokesperson** immediately and have additional communications officers on stand-by if needed. Immediately get the word to the press; let the media – and therefore the public – know that you are dealing with the situation.

  Notes: _____

- ❑ **Implement your emergency employee communications plan:** Inform your internal audiences – IT staff and other government offices – at the same time you inform the press. Prepare announcements to employees to transition them to alternate sites or implement telecommuting or other emergency procedures. Employees can maintain communication with the central IT office utilizing **Phone exchange cards,** provided to employees with two numbers: **(1)** First number employees use to call in and leave their contact information; **(2)** Second number is where the employees call in every morning for a standing all employee conference call for updates on the emergency situation.

  Notes: _____

- ❑ **Intergovernmental communications and coordination plan:** Communicate and coordinate efforts with state, local and federal government officials. Systems critical for other state, local and federal programs and services may need to be temporarily shut down during an event to safeguard the state's IT enterprise. Local jurisdictions are the point-of-contact for many state transactions, including vehicle and voter registration, and alternate channels of service delivery may need to be identified and temporarily established. Make sure **jurisdictional authority** is clearly established and articulated to avoid internal conflicts during a crisis.

  Notes: _____

- ❑ **Back-up communications:** In the event wireless, radio and Internet communications are inaccessible, Government Emergency Telecommunications Service (GETS) cards can be utilized for emergency wireline communications. GETS is a Federal program that prioritizes calls over wireline networks and utilizes both the universal GETS access number and a Personal Identification Number (PIN) for priority access.

  Notes: _____

- ❑ **CIO's must be effectively engaged with the On Scene Coordinator (OSC)**, and the **Incident Command System (ICS)** – the federal framework for managing disaster response that outlines common processes, roles, functions, terms, responsibilities, etc. ICS supports the **FEMA National Incident Management System (NIMS**) approach; states must understand both NIMS and the ICS.

  Notes: _____

- ❑ **Leverage technology/ Think outside the box:** In a disaster situation the state's GIS systems can be utilized to monitor power outages and system availability. For emergency communications, the **"State Portal"** can be converted to an emergency management portal. Also, **Web 2.0 technologies** such as Weblogs, Wikis and RSS feeds can be utilized for emergency communications.

  Notes: _____

- ❑ **Execute "Emergency Standby Services and Hardware Contracts:**" If necessary, execute pre-placed contracts for products and services needed during the crisis. The Governor may also have to temporarily suspend some of the state's procurement laws and execute "**Emergency Purchasing Guidelines**" for agencies.

  Notes: _____

After the Crisis

(6) Tactical Role of CIOs for Recovery After a Disaster Occurs (Working with state and local agencies, and critical staff to resume day-to-day operations, and perform gap analysis of the plan's effectiveness.)

- ❑ **Preliminary damage and loss assessment:** Conduct a post-event inventory and assess the loss of physical and non-physical assets. Include both tangible losses (e.g. a building or infrastructure) and intangible losses (e.g. financial and economic losses due to service disruption). Be sure to include a damage and loss assessment of hard copy and digital records. Prepare a tiered strategy for recovery of lost assets.

  Notes: _____

- ❑ **Employee transition:** Once agencies have recovered their data, CIOs need to find interim space for displaced employees, either at the hot site or another location. Coordinate announcements to employees to transition them to an alternate site or implement telecommuting procedures until normal operation are reestablished.

  Notes: _____

- ❑ **Budgetary concerns:** Following a disaster and resumption of IT services, there may be a need for emergency capital expenditures to aid in the recovery process. Be prepared to work with the state budget officer and/ or the state's legislative budget committees.

  Notes: _____

- ❑ **Contractual performance:** Review the performance of strategic contracts and modify contract agreements as necessary.

  Notes: _____

- ❑ **Lessons learned:** Evaluate the effectiveness of the DR/BC plan and how people responded. Examine all aspects of the recovery effort and conduct a gap analysis to identify deficiencies in the plan execution. Update the plan based on the analysis. What went right (duplicate); what went wrong (tag and avoid in the future). Correct problems so they don't happen again.

  Notes: _____

Appendix 1. Thinking Sideways

Instructions: Use this worksheet in conjunction with each checklist as a group brainstorming tool.

A. Conduct a gap analysis on **Checklist** ___. Focus on what's missing and include key policy issues unique to state governments, best practices and innovative ideas that can be shared across jurisdictions:

B. Describe how states and the private sector can work together to tackle these issues, through the transference of knowledge and experience?

C. How can CIOs use this information to secure funding and other resources for business continuity?

Appendix 2. Additional Resources

Federal Government Resources

The Federal Emergency Management Agency's (FEMA's) National Incident Management System (NIMS) – NIMS was developed so responders from different jurisdictions and disciplines can work together better to respond to natural disasters and emergencies, including acts of terrorism. NIMS' benefits include a unified approach to incident management; standard command and management structures; and emphasis on preparedness, mutual aid and resource management: <http://www.fema.gov/emergency/nims/index.shtm>

FEMA's Emergency Management Institute – A federal resource for emergency management education and training. <http://training.fema.gov/>

GAO Report, ***Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure Information***. GAO-06-383, April 17, 2006: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-383>

GAO Report, ***Continuity of Operations: Agency Plans Have Improved, but Better Oversight Could Assist Agencies in Preparing for Emergencies***. GAO-05-577, April 28, 2005: <http://www.gao.gov/docdblite/summary.php?rptno=GAO-05-577&accno=A22839>

U.S. Department of Homeland Security (DHS), Safe America Foundation – <http://www.safeamerica.org/sp_cybersafety.htm>

National Institute of Standards and Technology (NIST) – Special Publication 800-34, *Contingency Planning Guide for Information Technology: Recommendations of the National Institute of Standards and Technology*: <http://csrc.nist.gov/publications/nistpubs/>

State Government Resources

Pennsylvania's Pandemic Preparation Website: <http://www.pandemicflu.state.pa.us/pandemicflu/site/default.asp>
Also see *Government Technology's* article regarding Pennsylvania's new Website: <http://www.govtech.net/news/news.php?id=99469>

New York State's, Office of General Services (OGS) **emergency contracts** prepared through the new National Association of State Procurement Officials (NASPO) Cooperative Purchasing Hazardous Incident Response Equipment (HIRE) program, are available at: <http://www.ogs.state.ny.us/purchase/spg/awards/3823219745CAN.HTM> New York is the lead state for this multi-state cooperative.

Washington State, Department of Information Technology, Tech News, ***Enterprise Business Continuity: Making Sure Agencies are Prepared***, December 2005: <http://www.dis.wa.gov/technews/2005_12/20051203.aspx>

National Organization, Academia and Consortium Resources

Business Continuity Institute (BCI) – BCI was established in 1994 to enable members to obtain guidance and support from fellow business continuity practitioners. The BCI has over 2600 members in 50+ countries. The wider role of the BCI is to promote the highest standards of professional competence and commercial ethics in the provision and maintenance of business continuity planning and services: <http://www.thebci.org/>

Disaster Recovery Institute (DRI) – DRI International (DRII) was first formed in 1988 as the Disaster Recovery Institute in St. Louis, MO. A group of professionals from the industry and from Washington University in St. Louis forecast the need for comprehensive education in business

continuity. DRII established its goals to: Promote a base of common knowledge for the business continuity planning/ disaster recovery industry through education, assistance, and publication of the standard resource base; Certify qualified individuals in the discipline; and Promote the credibility and professionalism of certified individuals: <http://www.drii.org/>

The National Association of State Procurement Officials (NASPO) has completed work on disaster recovery as it relates to procurement: <http://www.naspo.org/>

U.S. Computer Emergency Readiness Team (U.S. CERT)/ Coordination Center – Survivable Systems Analysis Method: <http://www.cert.org/archive/html/analysis-method.html>

The Council of State Archivists (CoSA) – CoSA is a national organization comprising the individuals who serve as directors of the principal archival agencies in each state and territorial government. CoSA's *Framework for Emergency Preparedness in State Archives and Records Management Programs* is available at:

<http://www.statearchivists.org/prepare/framework/assessment.htm>

AFTER THE DISASTER Hurricane Katrina not only impacted more than 90,000 square miles and almost 10 million residents of the Gulf Coast but also affected how governments will manage such disasters in the future. A collection of articles opens the dialogue about disaster response in a new book, "***On Risk and Disaster: Lessons from Hurricane Katrina***." The book, edited by Ronald J. Daniels, Donald F. Kettl (a *Governing* contributor) and Howard Kunreuther, warns of the inevitability of another disaster and the need to be prepared to act. It addresses the public and private roles in assessing, managing and dealing with disasters and suggests strategies for moving ahead in rebuilding the Gulf Coast. To see a table of contents and sample text, visit <http://www.upenn.edu/pennpress/book/14002.html> Published by the University of Pennsylvania Press, the book sells for $27.50.

Articles and Reports

"***Cleaning Up After Katrina***," CIO Magazine, March 15, 2006: <http://www.cio.com/archive/031506/view_oreck.html?CID=19049>

Continuity of Operations Planning: Survival for Government, Continuity Central: <http://www.continuitycentral.com/feature0200.htm>

Disaster and Recovery, GovExec.com: <http://www.govexec.com/features/1201/1201managetech.htm>

"***Disaster Recovery, How to protect your technology in the event of a disaster***," Bob Xavier, November 27, 2001: <http://www.techsoup.org/howto/articles/techplan/page2686.cfm>