The Ohio Auditor of State's

BEST Practices

Volume 4, Issue 1 Winter 2007

INSIDE

A Message from Auditor of State Betty Montgomery

Dear Colleague,

A disaster – natural or otherwise – is something we all hope we never have to endure. Unfortunately, as some of you know all too well, disaster can strike at any time and in any place. Ohio has seen its share of natural disasters, mostly in the forms of flooding, tornadoes, severe storms, and blizzards. Many organizations also have been victims of fire or other accidental and catastrophic damage.

When it comes to dealing with disaster situations, the best defense is a good offense. What does this mean for local governments? It means investing the time, energy, and resources into developing a strong, working disaster recovery plan that anticipates likely situations and takes proactive steps to minimize impact on essential services and maximize recovery times.

Too often, our auditors find that local governments don't have adequate disaster recovery plans in place and have often responded to disasters without a great deal of preparation. There have been instances where there was a lack of clear direction, coordination of services, and a lack of accountability for taxpayer dollars spent to address the crisis. With a disaster recovery plan, however, governments can include strong controls to enhance the level of coordination and accountability as they work to resume operations.

Look no further than The U.S. Department of Agriculture's National Finance Center (NFC) for a good example of preparedness. NFC provides payroll services for more than half a million federal employees. When faced with a worst-case-scenario situation – Hurricane Katrina – the NFC ensured that workers were paid on time both during the category 4 hurricane and in its aftermath thanks to more than 20 years of strategic disaster planning. Read more about this remarkable example by clicking on the *Government Leader* article featured on page 12.

As my administration draws to a close, it's my pleasure to present to you my final edition of our award-winning publication *Best Practices*. In this addition we've tried to provide you with the basics of getting a disaster recovery plan started. Nearly every county in Ohio has been impacted by catastrophic events at one time or another. I encourage you to share ideas and experiences with one another and not let your agency be caught unprepared the next time disaster strikes.

Sincerely,

Betty Montgomery

Betty Montgomery
Ohio Auditor of State

Introduction

"He who fails to plan, plans to fail."
-Proverb

Disaster Recovery Planning

Our nation recently marked the one year anniversary of Hurricane Katrina and the five year anniversary of 9/11. Disasters such as these have raised awareness of the need for disaster recovery plans. Despite these monumental disasters, however, most governments still do not have formal disaster recovery plans to help them survive a disaster (e.g., Pandemic Influenza) and to resume essential operations.

One of the biggest obstacles to disaster recovery planning is overcoming the belief that "it won't happen here." Unfortunately, it's undeniable that small and sometimes large disasters happen periodically, even here in Ohio. Still need convincing? Take a look at disasters declared in Ohio at the Federal Emergency Management Agency (FEMA) website. During the past five years, most Ohio counties have been impacted by disaster declarations as a result of severe winter storms, flooding, tornadoes, mudslides and high winds (http://www.fema.gov/news/disasters_state.fema?id=39#em). As the old saying goes, "it's not a matter of if, but when."

Disaster recovery planning, simply defined, is the process an organization uses to prepare for events that disrupt normal operations. A disaster recovery plan, also called a business resumption plan, incorporates the actions an organization anticipates taking when normal operations are disrupted. The main objective of such planning is to help an organization survive a disaster and to guide the organization in resuming normal business operations.

Disaster recovery plans may also help a government recover from more common events resulting from software corruption or human error. The planning process can help governments identify and address significant risks to their daily operations such as over-reliance on key employees, a lack of documentation or ineffective backup procedures.

Although simple definitions can be given for disaster recovery planning and the resulting plan itself, the development of a planning process and a completed plan are often far from simple, requiring input from numerous individuals at every level and spanning all organizational units. If properly designed and implemented, a comprehensive disaster recovery plan minimizes the risk of loss of data, and the risk that operations important for the functioning of the organization cannot or will not be restored in a timely, cost-effective manner after a disastrous event.

According to disaster recovery literature, the planning process should stress the following points:

- Gaining a thorough understanding of the planning process to encourage participation and to generate support throughout the organization;

- Recognition that there are four distinct phases following a disaster that an organization must undergo – *Mitigation*, *Preparedness*, *Response* and *Recovery*;

- Concentration on prevention strategies as well as recovery process;

- Examination and prioritization of key functions so recovery efforts may be focused on mission-critical operations;

- Selection of a well-balanced disaster recovery team that reflects various management levels and organizational components; and

- Development of a viable plan that is easy to read, understand, update, and test with regularity.

The Auditor of State's Office (AOS) is providing this information so governments will have a framework to develop a disaster recovery planning process and a corresponding disaster recovery plan. Because each organization is unique, governments can use the objectives outlined below to develop their own detailed and customized steps. Please note that each government's organizational structure, operational unit locations, technology integration and other factors will determine the level of detail necessary for their individual recovery steps.

Remember, it's better to prepare for your organization's survival by putting a plan in place before disaster strikes, rather than thinking of strategic recovery efforts for the first time when your building is aflame.

Disaster Recovery Planning Objectives

Objective 1: Generate Awareness and Involve Elected Officials / Upper Management in the Planning Process

Including leadership at the highest level is critical to ensure needed resources are available for the planning process and to develop a functioning plan. One common obstacle to effective planning is the belief that the IT department is responsible for and will take care of disaster recovery planning. Although an IT department may have the authority and responsibility to ensure regular backups are performed and stored away from the data center, IT departments alone do not have the authority to coordinate effective planning across multiple departments and among numerous elected officials, as is the case for county government. Because the IT department has historically been responsible for disaster recovery planning, there has been a proliferation of recovery plans focused on restoring computer resources rather than the business operations those resources support.

To inform management of the business risks associated with disaster recovery and to garner management support for the planning process, the following steps need to be performed:

Conduct a Disaster Impact Study / Business Impact Analysis - Identify a number of disasters to which the government is most susceptible and determine their likely impact on the organization, including their impact on critical services and functions. A disaster could be as simple as water damage from a small fire that sets off the sprinkler system to a major incident resulting in the destruction of the government building and loss of life. Although it may seem as though there are an endless number of disaster scenarios, keep in mind that their impact can largely be grouped into one or more of the following three categories: loss of information/data, loss of access, and loss of personnel.

Some key questions to ask in assessing the impact of the disaster include:

- How many and what kind of resources would be lost?
- What are the total costs to the organization?
- How will the public be affected by the disaster and the loss of services?

Garner Management Support - It is necessary for upper management to gain an understanding of the estimated physical, business, and financial losses to the organization. This heightened awareness among management will help in fostering support for the disaster recovery process throughout the organization. Further, management involvement is vital to ensure the project is controlled and can accomplish the task on time and within budget. Upper management should also decide on an acceptable length of time that certain critical functions can remain inoperable. This will help in determining where recovery efforts should first be focused.

Gather Resources - Upper management must indicate how much money the government is willing to invest in standby equipment, user forms and supplies, testing, etc. Management "buy-in" is needed to release the resources both in direct monetary terms and staff time for the disaster recovery process. Disaster recovery is not a project with a pre-defined start and end date. Finalized disaster recovery plans should be living documents that are regularly tested and exercised.

Objective 2: Build a Diverse Planning Team and a Mission-Driven Planning Process

Once upper management has provided its support and resources are secured, a team must be selected and a project plan developed. The following points should be considered in building a disaster recovery team and developing a workable plan:

Appoint Authority and Ensure Team Diversity - Since assembling key personnel during the wake of a disaster is difficult, management should appoint someone to be in charge of the process (i.e., Program Manager) as well as an alternate. Additionally, the make up of the team should be diverse, reflecting key departments and various management levels within the organization. It is also important to involve not only management but also front-line employees in designing, planning, testing, refining, and executing the plan. Each member's input will be vital to ensure that all critical functions are considered in the resulting disaster recovery plan.

The names and contact information for members of the disaster recovery team should be maintained in multiple locations and kept up-to-date. Governments should also designate a process to assemble the team when a disaster strikes.

Define the Scope of the Planning Process (Mission Statement) - Project scope must be defined to ensure the project is organized and manageable given the resources provided. This is often accomplished by developing a mission statement with predefined expectations and desired results to guide the planning process.

Develop Goals and Assign Specific Tasks - Goals with associated timetables should also be developed to meet the parameters of the planning process. For example, a government may want to perform a damage assessment of its technical infrastructure within a set amount of time following a disaster. Finally, pre-assign as many specific tasks as possible so team members know what to do before the disaster even occurs, as members of the planning team generally fulfill key roles in the government's actual disaster recovery process.

Objective 3: Analyze and Assess the Organization

One of the primary objectives of the disaster recovery team is to conduct a comprehensive analysis of the organization to determine the functions or services that are critical to its operations and survival. In performing this analysis, the team should do the following:

Determine Key Business Functions - What are the core functions that the organization performs? For example, core functions of the Auditor of State's Office include auditing the financial statements of all public entities in the State, paying the State's obligations via warrants and Electronic Fund Transfers, and providing technical expertise through consulting and training services.

Determine Key Component Units or Divisions - Where are your key business functions performed? Are they centrally located or do they span several locations (keeping in mind that a disaster may impact operations at one location but not another)?

Determine Degree of Automation Used to Accomplish Key Functions - How are your core functions accomplished in the organization? Are computers used? How do manual and automated systems come together to accomplish the day-to-day tasks? Identify key partners necessary for providing core services (e.g., banks, utilities, other governments, service organizations, vendors).

Identify Significant Risks - It is often effective to have a brainstorming session to identify significant risks and failure points which could impact the recovery process. As part of this analysis, the team should consider all potential types of disasters and their impact on operations including the worst-case scenario – loss of life and facility/resource destruction.

Objective 4: Rank Major Business Areas

In most instances all systems cannot be (or don't need to be) "up-and-running" immediately after a disaster has occurred. Since resources are finite, they must be spent in a manner to support essential operations first. As such, the next task for the disaster recovery planning team is to determine a priority list for the organization.

Prioritize Core Critical Functions - The most critical or "mission-critical" activities must be ranked. The information gathered in the organizational analysis (Objective 3) is key to prioritizing the government's critical functions. With these rankings in mind, the government can more easily decide how long to suspend each operation and designate alternative (i.e., manual) backup strategies to carry out its more critical functions.

Prioritize Hardware and Software - Similarly, after mission-critical systems have been identified, a listing of the equipment used to perform these functions should be compiled and prioritized. For example, a working payroll system is likely more important than a dog license database.

Objective 5: Identify Resources

Resources are necessary to address disaster recovery costs and needs. These resources should be identified and compiled for quick access in a disastrous event. More specifically, the government should do the following:

List Personnel - Compile a list of both the recovery team and other key personnel in the organization. The list should include all contact numbers for these individuals so they can be reached at any time of day. Consider using a "call tree" in which key employees are responsible for contacting a group of individuals who in turn are responsible for contacting the next group, and so on. Also, provide multiple means for employees to contact the organization. If the disaster is widespread, employees may not be at their homes, or the communication channels may not be operational.

List Vendor Representatives and Safety Services - Contact numbers should be compiled for outside organizations including key vendors and safety services. Emergency numbers for police, fire and other agencies may be needed depending on the type of disaster that occurs. Also, contact numbers should be gathered for any critical operation that requires vendor interaction and/or assistance.

Compile Support Agreements - All support agreements should be gathered for the organization's mission-critical computer hardware and software systems.

Compile Insurance Policies - Any applicable property or computer equipment policies should be listed. Information should include contact numbers, contract terms and policy numbers.

Gather Supplies - Form and check stocks should be identified and the locations listed. Sundry supplies like paper, and general office supplies should also be listed and locations identified.

List Other Equipment and Software Inventories - A list should be made of the organization's non-mission critical equipment and software as it may be a resource to restore the mission-critical operations or may be used to develop a "workaround" so key operations can remain functional.

<u>Objective 6:</u> Implement Response and Recovery Steps

A vital section of the plan features the actual steps needed to assess and respond to a disaster. As such, the disaster recovery team must determine a systematic way to accomplish the following tasks:

Assess Level of Damage - The team should develop forms to be used in determining the types and degrees of damage to equipment, buildings, etc. for each department/business unit. Governments should contact their respective county emergency management agency which has trained personnel who are able to assess most types of physical damage.

Involve Key Vendors - Vendor assistance may be a key part to restoring operations. Their involvement should be determined and factored into the action steps. For example, if an electrical storm short circuits a mission-critical database, the government should create an action step to contact the database vendor to assist in restoring its operability.

Appropriate Resources - The appropriation of resources (monetary, equipment, personnel, etc.) is key to recovery timetables and action plans. They must be coordinated so they can be put into use quickly. Action steps must include guidance on accessing resources expeditiously in the wake of a disaster.

Implement Corrective Action - No matter the basis, corrective action plans should be as detailed as possible to provide users of the plan guidance on restoring damaged equipment.

Objective 7: Develop Alternatives to Processing

In some situations mission-critical systems cannot be restored in a timely basis. In these contingencies, processing may need to be performed by other means. The recovery team should include the following alternatives to processing key data within the disaster recovery plan:

Develop Partial Processing Methods - Could other equipment be used to perform partial processing of key data? For example, develop an action step whereby personal computers or other equipment is used to track certain transactions if the disaster left a critical database inoperable.

Create Manual Processing Methods - Can a paper or manual system be used on a temporary basis to process key data? For example, in the wake of a disaster that disables credit card machines, a government could process credit/debit card payments using carbon paper receipts in place of processing them electronically.

Objective 8: Employ Risk Reduction Strategies

Several strategies should be employed to help reduce the risks associated with disasters. In the long-run, reducing the risk of a disaster is more cost-efficient than concentrating all your efforts on minimizing the effect of a disaster once it has occurred. The disaster recovery team should consider the following risk reduction strategies in the formal recovery plan:

Evaluate Equipment and Systems for Redundant Capabilities - Computer equipment can be purchased that has redundant components, or entire redundant systems can be installed. In case one system is disabled as a result of a disaster, another system could be used to resume operations. As is often the case, governments own computers that have the capability of assuming the computing tasks of other computers.

Create a "Hot Site" - Governments can work with a vendor to install a hot site, which is a duplicate copy of an organization's data center that is created and stored at an off-site location. A hot site enables a government to continue computer and network operations in the event of a disaster. For example, if a government's data processing center is destroyed by a flood, the government can transfer all data processing operations to a hot site, which would have all the necessary equipment to resume operations.

Conduct Regular Media Backups - Backup involves copying files or databases so they are preserved in case of equipment failure or a disaster. Governments should also develop an accompanying backup policy to ensure employees understand the backup process. The backup policy should document data retention requirements and include provisions for periodic testing of backups. Now is the time to discover hardware malfunctions, media failure or missing files, not after the disaster strikes. This is a critical step and one often overlooked by governments.

Rotate Off-site Backup Media - All backup media should be incorporated in an off-site rotation schedule to ensure backup media would not be compromised by the same disaster as the original data source. As such, media should be stored in a secure, environmentally controlled location and at a sufficient distance from the primary data center.

Objective 9: Test and Update the Plan

Once completed, the plan must be reviewed and tested to ensure its viability. The plan will also need to be updated as the components of the plan change. For example, personnel and vendor information is likely to change with time. Such changes should be reflected in the plan. The recovery team should address the following:

Test the Plan - The completed plan should be tested on a regular basis. Don't get discouraged, testing WILL find flaws in the plan. The results of the test should be evaluated and the plan should be modified as appropriate. This will ensure the plan is viable and participants are familiar with the necessary response and recovery steps. Testing starts with small steps and moves towards a full scale exercise (see http://training.fema.gov/EMIWeb/IS/is120.asp). Be aware that key employees may not be available in a real disaster either because they cannot or choose not to come to work. Therefore, randomly remove a percentage of employees from the drill to better replicate situations where certain employees are unavailable. Additionally, funding must be sought to ensure resources are available to test the plan on a regular basis.

Periodically Update and Review the Plan - The plan should be reviewed by all employees on a periodic basis to ensure its reasonableness and any outdated information should be updated. The plan must be readily available, in hardcopy, to all who have roles in the execution of the plan. Additionally, key personnel should keep a copy of the plan at home in case the disaster destroys those copies maintained at the work site.

Summary

If you're beginning to think that developing a plan is an overwhelming task, keep in mind that no plan is perfect and each disaster situation will bring its own surprises. The key is to make employees aware of what could happen and to provide tools and strategies to address whatever happens. Consider the comment made by the Director of the USDA National Finance Center which successfully implemented its plan after Hurricane Katrina, "If you can get 80 percent of it down, the other 20 percent becomes manageable."

Also keep in mind that there are plenty of resources available to assist in developing the plan, from consultants and vendors, to books, websites, and plan templates. Use the available resources and tailor the plan to your government. However, if you end up with a document that you dust off once a year and give to the auditors, you probably have not succeeded in developing a successful recovery process.

In addition to a written document, your goal should be to raise the level of awareness in your organization so that when there are changes to the hardware, software, staffing, or policies, employees throughout the organization will consider how it might impact the recovery process and have a mechanism for ensuring changes are addressed in the plan. Make your plan a living document and work to keep it relevant for the government, the public and your co-workers who may have to use it in possibly the worst of circumstances.

Sample Disaster Recovery Plans

City of Hillsboro, Ohio
www.auditor.state.oh.us/publications/bestpractices/hillsboro.pdf
The City of Hillsboro has developed a comprehensive disaster recovery/business resumption plan that features a well-defined scope with goals and objectives and specific steps that must be taken following a disaster. The plan not only focuses on technical resources but also considers the resumption of the government's underlying business processes that a disaster would disrupt. Uniquely, depending on the degree of disruption to the government's operations, the plan also features three distinct escalation plans - minor (less than 24 hours), intermediate (greater than 24 hours but less than 72 hours) and major disruption (greater than 72 hours).

State Library of Ohio – Libraries
http://winslo.state.oh.us/services/LPD/disaster_frnt.html
The State Library of Ohio has developed a disaster preparedness plan specific for small public libraries in Ohio and has made it available online. The plan includes a helpful template and instructions to help smaller libraries with limited budgets develop their own workable plans. Although developed specifically for smaller libraries, the plan can easily be customized for other types of governments.

Additional Resources

Ohio Emergency Management Agency
http://www.ema.ohio.gov/ema.asp
Established under Section 5502 of the Ohio Revised Code, the Ohio Emergency Management Agency (EMA) is the central point of coordination within the state for response and recovery from disasters. Effective emergency management systems are a tiered effort, beginning with county EMAs. When an emergency exceeds the capacity of local government, they request the assistance of the state through the Ohio EMA. If an emergency response exceeds the capacity of the Ohio EMA, aid is requested from the president through the Federal Emergency Management Agency (FEMA). To access disaster recovery information from FEMA, visit http://www.fema.gov/index.shtm. For Ohio's Continuity of Operations Plan template, best practices, and other helpful information visit http://www.ema.ohio.gov/plans/Coop.zip.

Cisco − Disaster Recovery: Best Practices White Paper
www.cisco.com/warp/public/63/disrec.html

Government Leader
Magazine article, "When Crisis Comes: How NFC overcame calamity and kept its operations going"
http://www.governmentleader.com/issues/1_6/features/134-1.html

Disaster Recovery Journal
Sample Disaster Recovery Plans and Outlines
http://www.drj.com/new2dr/samples.htm

Disaster Recovery: Best Practices White Paper
http://www.cisco.com/warp/public/63/disrec.html

Disaster Recovery World
Directory of business continuity planning and disaster recovery planning software and services. Also, contains sample business continuity & disaster recovery plans.
http://www.disasterrecoveryworld.com/index.htm

Government Finance Officers Association (GFOA)
Computer Disaster Recovery Planning
http://www.gfoa.org/services/nl/computer-disaster-recovery.shtml

Contingency Planners of Ohio
http://www.cpohio.org/Default.aspx

Council of State Archivists, Archives Resource Center
Information Resources on Archives and Records Administration for State and Local Governments
http://www.statearchivists.org/arc/states/res_disa.htm#salvage

Disaster Recovery Community Web Portal
http://www.disasterrecoveryforum.com/

The Disaster Recovery Guide
http://www.disaster-recovery-guide.com/

State of Ohio IT Policy
Business Resumption Planning
http://www.disaster-recovery-guide.com/

Classic Mistakes
Computer World has a number of articles relating to the topic of disaster recovery planning.
http://www.computerworld.com/newsletter/0,4902,92268,00.html

American Bar Association
Article, "Disaster Recovery and Business Continuity" focuses on the legal community; however, also includes references and links to many general resources.
http://www.abanet.org/lpm/lpt/articles/slc10051.html

The Tips Page

Preparing Federal Schedules for Counties

The AOS recommends that counties follow the steps below when preparing their federal schedules for purposes of their Single Audit:

1. Assign grant coordinating responsibilities to one employee who would track the county's various grants and prepare the federal schedule. This position would likely reside in the Office of the County Auditor.

2. Communicate frequently with the Board of County Commissioners and County Department Heads as to the importance of notifying the County Auditor of Federal Programs applied for so the funds can be set up and budgeted.

3. Require all County departments to forward a copy of all grant agreements and award letters to the County Auditor.

4. Compare the prior year's federal schedule with the current year's schedule for reasonableness and discuss any anomalies with the department or agency that received the grant in question.

5. Verify reported Catalog of Federal Domestic Assistance (CFDA) numbers and grant program titles on the CFDA website at http://12.46.245.173/cfda/cfda.html.

6. Review the revenue/expenditure ledgers for obvious federal grant transactions and work with the Office of the County Treasurer to identify grants received via electronic fund transfers, as most are received in this manner.

7. Identify any monies passed-through to another agency and any sub-recipients among the various boards/commissions/departments within the county.

8. Review the minutes of the legislative body (e.g., Board of County Commissioners) for evidence of grants applied for and accepted/awarded.

9. Prepare a confirmation form in early January for each county department to be used to identify the granting agency, amounts received, amounts expended, the program name, CFDA number if possible, and the local funds used.

10. Remind the various county departments that federal funds often pass through a state department and may not appear to be a federal grant. As such, communicate with the granting agency to confirm the grant information.

11. Review audit bulletins that may address federal grant issues.

AUDITOR OF STATE
BETTY MONTGOMERY
88 E. BROAD ST., 5TH FLOOR
COLUMBUS, OH 43215