



BEST PRACTICE

Business Preparedness and Continuity Guidelines (2005 and 2008)(BUDGET, DEBT and CEDCP)

Background. Governments face many types of unscheduled disruptions to business operations. Disruptions to business operations may come from a variety of causes such as natural or manmade disasters, terrorism, and technology failures. Threat situations, domestic attacks, and natural disasters all present challenges to maintaining business operations.

Governments have a responsibility to minimize disruptions in the services they provide. Many government services are essential to the public's health and safety and to the protection of property. Disruptions in those essential services may range from temporary inconvenience to significant harm to individuals and the community.

Governments also have the responsibility for mitigating the effects of disasters on the communities they serve. In 1999, the GFOA developed a Recommended Practice, *Technology Disaster Recovery Planning*. This revised recommended practice expands that guidance and addresses additional aspects of comprehensive disaster and recovery planning.

Recommendation. The Government Finance Officers Association (GFOA) recommends that governments develop, test, and maintain a plan to continue their basic business operations during and immediately after disruptive events. Governments must be able to anticipate problems, detect threats and determine effective protective actions to enable them to continue to function. A government's response to disruptive events should be consistent with the type and severity of the event. State and local governments must be prepared to react to various disasters immediately, knowing that aid from the federal government may not come in a timely fashion.

1. *Plan Development.* A government must assess its own unique disruption risks. A strategy should be developed to mitigate risk and control costs.
 - a. *External Planning Resources.* The federal government, under the auspices of the U.S. Department of Homeland Security, offers a variety of resources to assist governments in ensuring business preparedness and continuity:
 - i. *Disaster and Emergency Recovery Plan Assessment.* The Office for Domestic Preparedness (ODP) is a component of the U.S. Department of Homeland Security's Office of State and Local Government Coordination and Preparedness (SLGCP). Its goal is to help states, cities, counties, towns and villages gain an objective assessment of their capability to prevent or respond to and recover from a disaster so that modifications to a plan can be made before an actual event occurs.
 - ii. *Disaster and Emergency Recovery Plan Testing.* A government's disaster and emergency recovery plan should be tested periodically. The Homeland Security Exercise and Evaluation Program (HSEEP), which is under the ODP, provides both a rationale and policy for designing, developing, conducting and evaluating testing exercises. HSEEP is a threat- and performance-based exercise program that includes a cycle, mix and range of activities of varying degrees of complexity. HSEEP provides a series of four reference manuals to assist state and local jurisdictions in designing training exercises, conducting the exercises, evaluating the results and improving the plan to correct deficiencies.

- iii. *Federal Emergency Management Agency (FEMA) Guidelines.* FEMA is another department within Homeland Security. Governments are encouraged to review preparedness guidance available on FEMA's website that covers (1) Emergency Operations Planning Guidance, (2) Interim Guidelines, Terrorist Incidents, (3) Tool Kit, Terrorist Incidents, (4) State and Local Guide for All-Hazards Emergency Operations Plan, (5) Emergency Operations Center Assessment Checklist, and (6) Continuity of Operations Guidance for State and Local Governments. While most emergency situations are handled locally, when there is a major incident help may be needed from other jurisdictions, the state, and the federal government. National Incident Management System (NIMS) provides a consistent nationwide template for organizations to work together effectively and efficiently to prepare for, prevent, respond to and recover from domestic incidents, regardless of cause, size or complexity, including acts of catastrophic terrorism. An Introduction to NIMS is a Web-based awareness level course that explains NIMS components, concepts and principles. All personnel with a direct role in emergency preparedness, incident management, or response are advised to complete this training.
- b. *Other Planning Considerations.* Governments should consider the following items, in addition to the resources provided by the federal government, when designing business preparedness and continuity guidelines.
- i. *Emergency Response Plan Compliance.* When developing response plans, governments must make sure that they are compliant with applicable local, state, federal, Occupational Safety and Health Administration (OSHA), and Environmental Protection Agency (EPA) guidelines.
 - ii. *Risk Management.* The risk manager should assess potential areas of insurance coverage in planning for any type of disruption. The risk manager should be aware of potential pre-qualifications like flood zone compliance, adopted building codes, etc.
 - iii. *Resiliency.* The concept of resiliency should be an integral part of disaster preparedness. Resiliency emphasizes the capacity of infrastructure, operations, and even social systems to respond to and recover from extreme events. Resilient systems reduce the probabilities of failure, the consequences of failure (such as deaths and injuries, physical damage, and negative economic and social effects), and the time for recovery. To address resiliency, governments should assess the "criticality" and "vulnerability" of their systems. By distinguishing critical systems and recognizing vulnerabilities, resiliency-enhancing projects can be planned and budgeted for.
 - iv. *Administrative Support Functions.* A government should plan to have such functions as human resources, purchasing, treasury, legal, and risk management accessible during an emergency situation. A back-up system for payment to staff and to make investments or debt payments should be available. For specific items like investments and payments on debt obligations, contact information (office, mobile, and home) for the professional bond and investment team (trustees, remarketing agents, advisors, brokers, banks, etc.) should be available to all members of the finance team, and a copy should be kept off site with these individuals as well (car or home). Confidentiality of information taken offsite should be a consideration. The use of password protected flash drives is an option.
 - v. *Communication with the Public.* It is essential that a government communicate (with one voice) to citizens during a time of disruption. When a crisis occurs, immediately get the word to available media. The government should direct the public on where to go for more information. Planning in advance will help identify what the most effective way is to communicate with various groups or neighborhoods. While the mode of communication may vary (e.g., Web sites, phone recordings at the government main office, text messaging systems, crisis hot line, radio, television, REVERSE 911,

mailings or newspapers), updates should be given regularly. Gather information as quickly as possible. Monitor media reports and correct errors immediately.

- vi. *Outsourced/Recovery Services*. A government should assess the ability of providers of outsourced services themselves (e.g., garbage collection) to recover from unscheduled disruptions.

2. *Plan Implementation*. After developing a business preparedness and continuity plan, the following steps should be implemented.

- a. *Record Keeping*. Governments should develop a plan and procedures for contemporaneous record keeping in a format acceptable to FEMA. Compliance with FEMA regulations will simplify the reimbursement process.
- b. *Personnel Assignments and Communication in the Wake of a Disaster or Emergency*. Governments should formally assign personnel from each department or agency to serve on the disaster and emergency recovery team. The assignment of personnel should be planned. A strong business continuity plan maps out an organizational structure and lists roles and responsibilities, so employees are aware of their tasks. Essential and non-essential classifications may be used. Home and cell phone numbers as well as e-mail addresses for all essential employees should be updated regularly, with a duplicate list kept at a remote site. In addition, governments should establish procedures for assembling the team in the wake of a disaster or emergency. Those procedures should take into account the possibility that one or more ordinary means of communication may not be available in such circumstances (e.g., cell phones, e-mail) and specify appropriate alternative means of communication in such an eventuality. A government may also wish to develop specific policies for disaster service workers during times of emergency.
- c. *Mutual Aid Agreements*. Many state and local governments enter into mutual aid agreements to provide emergency assistance to each other in the event of disasters or emergencies. These agreements often are written, but occasionally are arranged verbally after a disaster or emergency occurs. Mutual aid agreement policies should address both written and verbal mutual aid agreements and the eligibility of costs under the Emergency Management Assistance Compact (EMAC).
- d. *Outsourced/Recovery Services*. A government should negotiate contingent contracts for recovery services in advance. If a government is not legally authorized to negotiate contingent contracts, the government should establish an emergency procurement process and identify criteria that would activate the process.
- e. *Disaster and Emergency Recovery Plan Safeguard*. A government's disaster and emergency recovery plan should be safeguarded to ensure that it is available in the event of a disaster or emergency. Specific incident/emergency management responses may require assembly areas or record keeping at a safe distance from the site of the incident.

References

- GFOA Best Practice, "Technology Disaster Recovery Planning," 1999 and 2007.
- GFOA Best Practice, "Ensuring Adequate Documentation of Costs to Support Claims For Disaster Recovery Assistance," 2008.
- United States Department of Homeland Security. Office for Domestic Preparedness (<http://www.ojp.usdoj.gov/odp/>).
- United States Department of Homeland Security. Office for Domestic Preparedness, "Homeland Security Exercise and Evaluation Program (HSEEP)" (<http://www.ojp.usdoj.gov/odp/docs/hseep.htm>).
- Federal Emergency Management Agency (<http://www.fema.gov>).

Approved by the GFOA's Executive Board, October 17, 2008.