EMERGENCY MANAGEMENT

for Records and Information Programs

2nd Edition (An Excerpt)

Virginia A. Jones, CRM, FAI

Darlene Barber, CRM

Emergency Management Concepts

"Anything that can cause a disruption in the normal operation of your business can be a disaster."[1]

The first step in the study of emergency management and the development of a comprehensive emergency management plan for records and information is to understand the concepts of emergencies and disasters. Records and information are best protected by strong, cost-efficient emergency management and business continuity plans.

An **emergency** is a sudden, urgent, usually unexpected occurrence or occasion requiring immediate action. Examples of an emergency include: a broken water pipe, a bomb threat, a severe storm, a data security breach, or other events that require actions but do not necessarily require significant efforts to control. This event does not usually result in major loss for an organization.

A **disaster,** on the other hand, is an emergency event that progresses from the realm of standard operating procedures to conditions requiring resources often beyond the organization's means. Disasters result in significant financial and operational damage and loss. Examples of disasters include: a fire that destroys a facility, a flood that causes major facility and product loss, and a tornado that causes major damage to one or more facilities and/or product loss. A disaster can be a small but localized event, such as a major fire to a business, or a widespread event, such as a natural disaster, that causes significant damage to a community.

Jeffrey Bumgarner, in *Emergency Management,* discusses three categories of disasters (or hazards): natural, technological, and social.[2] He describes **natural disasters,** or acts of nature, as geological (earthquakes), meteorological (hurricanes, tornadoes), hydrological (floods) and biological (disease pandemics).[3] Each geographic region is subject to particular natural disasters. Although such disasters cannot be averted, more accurate forecasting and sophisticated warning systems have reduced the unexpectedness of some natural disasters. The primary loss prevention measures for natural disasters are good planning and preparation.

Technological disasters are events usually caused by human error or as secondary occurrences to natural disasters. Technical disasters can include the release of hazardous materials, airplane crashes, structural failures, a security breach of data, a viral attack on the computer network, and dam failures. Collapsed buildings from an earthquake or major fire can cause the release of hazardous materials or radiation emissions. Building and equipment failure or malfunction may cause fire and flooding. Electrical malfunctions, such as defective wiring, overheated motors, and faulty switch boxes, and controllers, are the primary cause of business fires.[4]

Unlike natural disasters, technical disasters can be avoided. The mitigation part of a business continuity or emergency management plan should address potential problem areas and describe

technological security, inspection, and maintenance practices that significantly reduce the danger of technological hazards.

Human error or carelessness is often the cause of fire, theft, misinformation, and information loss. It can be prevented through employee training, adequate supervision, implementing security measures, and a constant sensitivity to potential hazards. Theft is a common problem that plagues every aspect of organizational life including information. Industrial espionage can cause significant financial loss from stolen designs and lost patent opportunities.

Social disasters are deliberate destructive activities causing illness, injury, and death. The scope of a social disaster can vary from a localized event to one with widespread destruction. Social disasters are unpredictable and can occur anywhere at any time. Acts of deliberate destructiveness include theft, espionage, vandalism, riots, terrorism, and war. Terrorism and vandalism are occurring more frequently throughout the world. Protection of records and information from acts of deliberate destructiveness is addressed primarily through application of appropriate safety and security measures. Losses from these types of disasters can be greatly reduced through adequate planning measures and implementing a loss prevention plan.

The scope of emergencies or disasters can be **community-wide events** with immediate disruption of communications and emergency services, power outages, and widespread destruction. In a community-wide disaster, employees' homes and families are often endangered and take priority over organization responsibilities. Community-wide disasters create conditions that hinder the access to and restoration of back-up information. They also pose difficulties in getting to facilities and work sites to begin records and information recovery processes.

Localized events may also include loss of life, power outages, and massive destruction; but communications and emergency services may not be affected. Localized events allow quick application of back-up procedures, although they may still hinder the start of records salvage operations. A localized event may be a tornado, a localized flood, or a bombing incident.

Organizational events strike only a single building, floor, office, or organization, and because of the narrow scope of these events, greater use of community and organization resources is possible. Applying response and recovery procedures and accessing damaged areas to begin recovery can usually be accomplished quickly. Examples of organizational events are fires, burst water pipes, breach of computer network security, or power failures.

Emergency Management

Emergency management is a planned approach for the prevention of disasters, preparedness and response to emergencies, and recovery following an emergency or disaster. Most important to any effort to safeguard records and information is to include records and information in asset protection plans. A plan for records and information should be considered a part of the organization's emergency management and business continuity plans. Organization personnel must assess risk, secure facilities, deploy resources, and conduct other activities to be successful at mitigating loss.

Emergency management professionals define four distinct programs or phases of a comprehensive emergency management plan. These four phases are mitigation (prevention), preparedness, response, and recovery.[5] While some people believe that prevention and recovery alone make up a sound plan, others believe that preparedness and recovery are the only necessary elements of a sound plan. The most effective plans include the four-phase approach.

Mitigation

The first phase of a comprehensive emergency management plan is to take steps to prevent records and information disasters from occurring. *Risk management, risk aversion,* and *loss prevention* are other terms used for the mitigation phase of emergency management. **Mitigation** is the activities or measures taken to eliminate or reduce the probability of loss should a disruptive event occur. If events do occur, having mitigated known risks will reduce the chance of emergencies turning into records and information disasters.

Mitigation activities include identifying organizational elements that are at risk, the type and levels of risk, and the probability of risk (determining the likelihood that the risk will result in a disruptive event).[6] Risk management is discussed in greater length in Section II. Prevention initiatives can also include mitigating risk by performing activities such as installing a fire suppression system in a records storage center, finding and encapsulating water pipes placed above a technical library, and implementing data security procedures.

Preparedness

Being prepared is a prerequisite for response. Being prepared means having the organization's resources positioned before a disruptive event occurs. **Preparedness** includes the activities established to assist in responding to an event. A few examples of preparedness activities include developing and updating the emergency response plan, testing emergency systems, training personnel, stocking emergency supplies, lining up approved recovery vendors, and establishing hot or cold sites.[7]

Preparedness also means that personnel can recognize a disruptive event immediately and activate the emergency response plan. All the planning in the world cannot help an organization if its personnel cannot recognize a small problem before it develops into a disruptive event. Training, plan testing, and emergency simulation are vital to the success of the emergency response program. Section III presents more detail on exercising the plan and simulating emergencies.

Response

After someone recognizes an emergency or potential disruptive event, the emergency response plan is activated. **Response** includes the activities established to react immediately to an emergency event. Responding to an event means initiating resources necessary to protect or secure the organization from loss. Activities immediately before, during, or directly after events are *response activities.*[8]

Response activities include contacting the emergency response team, notifying appropriate authorities, securing facilities, issuing press releases, activating emergency response systems, and notifying records and information recovery resources. At this point, the emergency management plan leads into the recovery phase. Section IV covers the response phase in more detail.

Recovery

Recovery includes activities associated with restoring resources or operations following a disruptive event. It involves all activities necessary to restore the organization's systems and processes to normal operating status. Recovery phase activities can include dehumidifying records, restoring information onto computers, and returning vital records from offsite emergency storage. The organization can divide the recovery process into two phases, depending on the extent of the loss.[9]

Usually, the short-term recovery phase involves the restoration of vital systems and processes that can get the organization's mission, product, or service back into production. The organization's customers need to be maintained in order to maintain a revenue stream. Once the vital systems are restored, personnel can begin the second phase of recovery—the restoration of secondary systems and processes. Recovery and the resumption of operations are discussed in Section V.

In today's competitive environment, any business, industry, or government

DISASTER SNAPSHOT

The city archive in Cologne, Germany, collapsed on March 3, 2009, killing two men in a neighboring building and destroying about 15 percent of the historic documents housed in the archive. An investigation into the collapse revealed that a foreman of a crew working on the metro line going under the archive intentionally used fewer steel reinforcements at the site of the accident, selling the unused metal to scrap dealers, and falsifying the protocols for the work site.

The surviving documents, which date back as far as 1,000 years, were in varying states when rescue workers pulled them from the archive rubble, but less than one-quarter had been torn apart. Experts have since been working to piece them back together using software that was developed to restore shredded documents from the East German secret police, the Stasi.

Source: The Local, "Construction worker confesses in Cologne archive collapse case," *The Local: Germany's News in English,* 3 March 2009. 13 March 2011 <http://www.thelocal.de/article.php?ID=25131>.

organization must position itself to accept challenges that lie ahead. If a situation occurs that affects profitability or retained earnings, continued operation may be jeopardized. Planning is vital and necessary to mitigate losses. No organization can afford to lose customers because of failure to plan for and to manage disruptive events.

Business Continuity

Business continuity management (BCM) is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value creating activities.[10] To be successful, business continuity management must be fully integrated across the entire organization as a required management process. Business continuity management includes business continuity planning, which focuses mainly on incident response and, depending on the organization, can include records and information security and risk management processes.

A **business continuity plan (BCP)** is the documentation of a predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption.[11]

Like emergency management, business continuity management relies on both critical business process identification and risk management results to determine the various priorities, tasks and procedures to include in the plans. While emergency management attempts to identify and mitigate all possible risks, business continuity management focuses on mitigating those risks that the organization cannot absorb—the risk tolerance of an organization. Risk tolerance is discussed more thoroughly in Chapter 3.

Benefits of Emergency Management and Business Continuity Planning

Comprehensive emergency management and business continuity planning yields many benefits for an organization's records, information, and assets if an emergency event occurs.

Stakeholders in the organization can gain comfort by knowing that measures have been taken to protect the organization from loss. Emergency management and business continuity planning includes the following benefits.

1. *Quick resumption of operations.* When an organization's personnel establish a plan, train personnel, complete preparedness activities, and test the plan, they are ready to handle a disruptive event. Even more important, if an event occurs, it has a good chance of being controlled so that it does not turn into a records and information disaster. These efforts result in the ability to maintain or resume normal operations quickly.

   Quick resumption of operations leads to continued profitability or revenue flow. An effective plan gives an organization the ability to successfully respond quickly to any major disruption that threatens its survival. Quick resumption of operations adds value to an organization and the products and services it delivers.

2. *Improved safety.* The courts could hold an organization negligent for not having a plan when an event caused an injury or took an employee's life. Material and supplies can be replaced; personnel are not recoverable. The U.S. Occupational Safety and Health Administration (OSHA) requires all employers to develop and implement an emergency action plan that includes protection procedures for personnel during and after an emergency.[12]

   The emergency management or business continuity plan should address key activities, such as training and risk mitigation, that will help keep people safe. Training provides the necessary knowledge to allow people to act safely and effectively. It also takes the surprise out of response activities. When an organization carries out training programs, personnel are more likely to behave appropriately in an emergency situation.

3. *Vital asset protection.* Emergency and business continuity management includes plans for protecting the organization's vital assets. The plan protects shareholders' investments, secures employees' jobs and retirement benefits, safeguards research, protects personal information, and maintains customer confidence and trust. Immediate resumption of operations and protection of personnel provide understandable benefits in addition to protecting material assets. For example, personnel can safeguard facilities, products, fleets, equipment, and furnishings during a disruptive event. However, without proper planning, the loss of any one of these assets will cause severe problems for the organization.

4. *Reduced insurance costs.* An emergency management or business continuity plan is a close partner of business insurance and security. Inadequate insurance and security can be ineffective and costly. The plan contains specific information about assets and risks, low cost preventive measures, and the cost of each protection program (such as a computer hot site, offsite records storage, or back-up hardware). Additionally, the plan contains schedules for periodic facility inspections and personnel training.

   Well-designed and maintained emergency management and business continuity plans can translate into premium reductions for specific types of business insurance. Organizations can reduce other types of insurance in addition to premium reductions through improved security, maintenance, and training programs. If an emergency management or business continuity plan is in place, an organization may reduce business resumption insurance and records restoration insurance costs that are portions of a total insurance package.

5. *Improved security.* The process of preparing an emergency management or business continuity plan includes a review of present security procedures to protect organizational facilities, personnel, records, and information from theft or acts of vandalism or terrorism. For example, the plan should include detailed procedures to monitor and control access to the facilities and equipment that contain vital records and information. Security is an important part of the mitigation phase of emergency or business continuity management.

6. *Legal compliance.* Organizations have defined legal responsibilities toward their shareholders, employees, government agencies, citizens, and customers. These responsibilities include taking reasonable measures to protect the organizations' assets, including records and information, and to remain in compliance with laws and regulations. Laws and regulations require emergency management or business continuity capabilities in several ways.

   - A specific *law* or *regulation* requires an organization to have an emergency management or business continuity plan.
   - A *contract* or *agreement* may require an organization to have a plan.
   - Legal precedent, as set by court cases, determine that organizations must have an established emergency management or business continuity plan.
   - A law or regulation may require compliance in such a way that protection from loss of records and information is implied.

7. *Reduction of errors from shock factor.* Without a plan, people will react haphazardly to a disruptive event. Some people may make mistakes due to insufficient or incorrect information, and some may freeze with fear and not react at all. Emergency management and business continuity plans are valuable tools in reducing the initial shock of a negative event.

   Emergency response planning exercises or mock drills place people in "what if" situations that increase awareness of how to behave in real events. People can reduce their fear and stress if they know what is expected of them. If an organization trains its employees and provides a plan for them to read and understand, they will behave more effectively.

The organization's emergency management and business continuity plans should address all four phases of emergency management—*mitigation, preparedness, response,* and *recovery.* The organization that has developed comprehensive emergency management and BC plans will benefit greatly.

Records and Information Management Practices

Five elements of records and information management impact an effective emergency management or business continuity plan. (These elements are generally accepted practices. Some organizations may not implement all aspects of the elements due to resource constraints.)

1. Consider information as a critical resource throughout the organization.
2. Establish and maintain a current records and information inventory, an information systems inventory, and an inventory of electronically stored information (ESI).
3. Establish and maintain a documented records classification and retrieval system throughout the organization.
4. Establish and maintain documented records retention and disposition policies and procedures for the entire organization.
5. Develop and distribute a records management manual that includes all records and information management policies and procedures.

Information Viewed as a Resource

In most organizations critical resources receive the most support for mitigation and recovery efforts. Many organizations, however, do not always consider the records and information that are a part of the business processes of a critical resource. The growth of electronic recordkeeping systems as a basic business convention justifies the identification of information holdings as essential resources. Electronic records and data are essential tools in most business processes.

Statutory and regulatory requirements place a responsibility on the organization to identify and safeguard records and information necessary to show legal compliance, fiscal compliance, and to protect personal privacy. Security of these data and information should be part of emergency management or business continuity plans.

Some records and information are necessary during an event, and many are necessary afterwards for recovery. The administrative elements of emergency response include requirements for the creation and maintenance of certain essential records during an event. These records document response actions taken, the timeline of response actions, accounting for fund expenditures, documentation of any injuries sustained during response, and damage assessment records as the event progresses.

Records needed for damage financial recovery should also be considered a resource by the organization. Insurance companies will want damage documented, including "before" and "after" factors such as ownership, condition, cost, and so on. According to one director with the U.S. Federal Emergency Management Agency's (FEMA) Infrastructure Branch, "The most important thing for applicants [for FEMA's disaster recovery funding] is to be able to provide FEMA with a clear and complete view of their damages, the work they performed or will perform, and the costs they incurred." "The easiest way to do this is by having accurate and complete records."[13]

Records Inventory and ESI

To implement a successful plan to identify and protect records, organizations need to review the process of creating, arranging, storing, and retrieving records and information. A **record** is "recorded information, regardless of medium or characteristics, made or received by an organization in pursuance of legal obligations or in the transaction of business."[14] Information is recorded in many formats. Paper, microfilm, photographs, a variety of magnetic media, optical disks, audio tapes, and video recordings are all used as original media for creating, using, storing, and/or retrieving information. In addition, electronic records and data can be structured data sets, like databases; semistructured

applications, like word processing files, email, and scanned images; and unstructured repositories, like file servers.

Data on the function, media or format type, and use of records and information collected on the records inventory are very useful to emergency management or business continuity planning. Data aid in determining records and information location and vulnerabilities and in identifying any existing protection. The inventory of existing records and information also aids in identifying and protecting vital records. An electronically stored information (ESI) data map for all electronic records can be used to identify electronic records and data that may have been damaged or lost. The map should include the custodian of the record, which electronic systems and formats are used to store the records or data, any limitations to accessibility of the records, and the retention policies for the records and data. Recovering records or data with expired retention is not economically feasible.

Documented Records Classification and Retrieval System

Lost or misfiled records and information can result in serious legal and monetary losses for an organization. Poorly organized files and inadequate labeling and indexing make finding records and information time-consuming and increases the likelihood of misfiling a record. These consequences are as true for electronic files as they are for paper files. Unorganized documents on diskettes, CDs, DVDs, hard drives, flash drives, external hard drives, or back-up tapes result in very time-consuming searches. Poorly labeled or named electronic files result in lost (unable to be retrieved) records.

Organized and well-indexed records are essential to timely and efficient resumption of operations following a disruptive event. Disorganized records and information significantly increase the cost of the recovery phase of emergency or business continuity management. Unorganized or poorly indexed records and information are nightmares to salvage or recreate from other sources. Documented indices and classification and retrieval systems help speed the re-creation of records from backups and other sources when necessary.

Documented Records Retention and Disposition Policy and Procedures

Records retention schedules, file plans, and records destruction policies are established to satisfy legal, audit, and business need requirements. Records management policies and procedures can be organized in a records management manual that should also include the emergency management or business continuity plan for records and information.

Without some type of established records management program, organizations leave themselves open to detrimental results. An organization can suffer fines, loss of legal rights, loss of revenue and profit, and uncollectable receipts. Sometimes, litigation can be lost because the lack of a records and information management retention and disposition program is interpreted as willful destruction of evidence. To protect the organization, policies and procedures should be in place to track all records destroyed. This tracking includes records destroyed during a disaster or during records salvage attempts following a disaster.

The records retention schedule helps identify *vital* or *mission-critical records*—records essential to critical business processes. **Critical business processes** are those parts or elements of an organization that are vital to everyday operations. If these critical processes are not performed, the organization may lose revenue and profits, experience increased operating costs following recovery, and possibly lose customers. The records retention schedule aids in indicating records of immediate value and priority during an emergency. A schedule also can function as a tool for pinpointing records and information that should exist and, therefore, must be found and recovered. Protecting records without knowing location, media, methods of protection, and the value of individual records is difficult. Without a records retention schedule and

QUICK TIPS

- Lists of file folder labels or word processing document names can function as file indexes.
- Every organization needs some form of a records retention schedule. Many professional organizations and records storage companies have sample business records retention schedules that can be adapted to any small organization's general business records.
- A one-page statement adopted by the board of directors or governing commission can be considered a records disposition policy.

organization file plan, reconstruction and salvage from a disorganized body of records and information will be very costly.

Emergency Management and Business Continuity for Records and Information

An emergency management or business continuity plan can be a significant catalyst for improving a records management program. The plan combines records management, information systems, telecommunications, and archival functions under a single, comprehensive program.

Where possible, the records and information emergency management or business continuity plan should also be a part of the overall organizational emergency management or business continuity program. In organizations where no comprehensive plan exists, the records and information plan must cover more criteria. These criteria may include requiring facility improvements or eliminating vulnerabilities. It may also include planning communications links and operations centers to restore access to records during a natural disaster.

Remember that recovery of records and information is only a small part of emergency management or business continuity plans. Safety of individuals will always take precedence over recovery of records and information, and the reestablishment of critical business processes will have priority.

An **emergency management or business continuity plan for records and information** is an approved, written, implemented, and periodically tested program to identify, protect, and reconstruct/salvage an organization's vital records and to establish procedures for the immediate resumption of business operations in case of a disaster. It is a dynamic, changing document requiring ongoing review and improvement. An emergency management or business continuity plan for records and information is used to:

- Identify mitigation measures against the loss of records and information.
- Identify alternative sources of the organization's records and information.
- Provide the basis for a systematic response to disruptive events that threaten an organization's records and information.
- Identify emergency response personnel and their roles.
- Establish procedures for recovery of damaged records and information.
- Establish recovery priorities.
- Identify sources of supplies, equipment, and services for recovery and restoration of damaged records and media.

New information technologies make records and information emergency management or business continuity planning more challenging and more complex. Records are created and stored on a variety of media and each of these different media requires some specific loss prevention and recovery techniques. Procedures for protecting and reconstructing information stored on magnetic media differ from those for protecting and salvaging information contained on paper records. A piece of paper can usually be quickly and easily dried after a flood, but a computer disk or tape needs technical expertise, and immediate, knowledgeable action to preserve the information it contains. Plans must include and provide for all media on which records are created and stored.

The type of physical damage to the records will determine the salvage methods necessary to recover the information. Fire-damaged records, particularly film and magnetic media, are often difficult to salvage. Vital records lost through theft, misfiling, or data entry error must often be reconstructed from designated back-up copies. Water-damaged records are the most frequent objects of salvage efforts and form the center of many records and information emergency management and business continuity plans.

An emergency management or business continuity plan for records and information has four objectives:

1. *Mitigation.* Identify and adequately protect the organization's vital records and information.
2. *Preparedness.* Reduce the risk of disasters caused by human error, deliberate destructiveness, building/equipment failure or malfunction, and the adverse consequences of all disasters by mandating specific security, maintenance, and training programs; establishing vital records programs; planning response strategies; and by explaining policies, procedures, and resources to be activated in emergency situations.
3. *Response.* Ensure the organization's ability to continue or resume operations effectively after a major event by activating the response plan and setting in place planned alternative operating procedures and locations.
4. *Recovery.* Ensure the organization's ability to recover lost or endangered information rapidly by reconstructing and/or salvaging damaged records after a major disaster. Establish detailed recovery procedures and a management structure to carry out these procedures.

The operational impact of a disruptive event is defined by the length of time it shuts down or interrupts an essential business process or organizational function. Where records and information can be restored or salvaged, the impact is usually confined to the period immediately following the event. Where records and information are lost or destroyed, the organization may be affected for many years.

A primary benefit of an emergency management or business continuity plan is rapid resumption of operations or services. The technological atmosphere of most organizations requires immediate access to electronic information for most business processes. Plans should provide procedures for routine data backup, protective storage of back-up data, and alternative sites to ensure this access.

QUICK TIP

Emergencies for some small businesses can happen at any time, especially if the business is located adjacent to another business. Discussing the importance of emergency management principles and concepts with business neighbors can often prevent a records and information disaster.

Planning information protection can lead to improved information security. The need for physical security of records is widely recognized. Organizations do not always consider the need to protect internal information, particularly electronic data and records. Increasing use of Internet services, email, and social media can expose an organization to many information security problems. Patent or design information can be stolen, personal information can be compromised, computers can be exposed to viruses, and unwise email conversations can become legally embarrassing.

Protection of records is essential to meet statutory and regulatory requirements. If a regulatory authority requires accounting records to be produced during an audit, those records must be protected against loss. Records required by litigation must be produced or accounted for even if the organization was put out of business by a disaster. Records and data containing personal information must be secured. In the United States, the Internal Revenue Service holds officers and directors responsible for creating and maintaining organization records. The Foreign Corrupt Practices Law holds specific officers and directors of some organizations liable for negligence when they fail to take reasonable precautions to protect an organization's records. The Office of the Comptroller of the Currency requires officers of nationally chartered banks to review their contingency plans annually. Almost every state has legislation setting the required procedures for responding to a breach of personal data.

Emergency management and business continuity planning can improve information systems operations. Planning protection and recovery procedures will show any deficiencies in hardware and software compatibility and accessibility, comprehensive information and system security programs, comprehensive and consistent data backup, data back-up storage and recovery procedures, and cross-training on using software and database programs.

Some elements of a plan may be fully in place before the planning process begins; some may only be in an elementary stage. A plan can be a powerful stimulus for enhancing security, viewing improved

management of information as essential to a company's survival, and establishing more effective methods for managing all company information. Establishing and using the plan can make the difference between inconvenience or slight delay and catastrophic loss.

A solid emergency management or business continuity plan for records and information can improve the response to requirements of the overall organization plan. Information accessed quickly and accurately during a disruptive event or immediately following an event greatly increases the speed of resumption of operations.

"In the wake of the 9/11 terrorist attack, one brokerage firm stood out in terms of IT Disaster Recovery: Cantor Fitzgerald. Its office was located in the World Trade Center towers in New York City and was seriously affected in terms of lives and data lost. Yet, within a few days of the disaster, Cantor Fitzgerald was believed to be operational in another location, having recovered much of the information lost due to a well-planned IT Disaster Recovery Plan (DRP)."[15]

Lesson Learned

"The continued operations of an organization depend on management's awareness of potential disasters, their ability to develop a plan to minimize disruptions of critical functions and the capability to recover operations expediently and successfully."[16]

CHAPTER 1 CHECKLIST

Emergency Management Concepts

- ☐ Know and understand the difference between a records and information "emergency" and a "disaster."
- ☐ Know and understand the four phases of emergency management: mitigation, preparedness, response, and recovery.
- ☐ Know and understand the benefits of emergency management planning:
  - ☐ Quick resumption of operations
  - ☐ Improved safety
  - ☐ Protection of vital assets
  - ☐ Reduced insurance costs
  - ☐ Improved security
  - ☐ Legal compliance
  - ☐ Reduction of errors from shock factor

Records and Information Management Practices

- ☐ Consider information as a critical resource throughout the organization.
- ☐ Establish and maintain a current records and information inventory and a current ESI map.
- ☐ Establish and maintain a documented records and information classification and retrieval system throughout the organization.
- ☐ Establish and maintain documented records retention and disposition policies and procedures for the entire organization.
- ☐ Develop and distribute a records management manual that includes all records and information management policies and procedures. At a minimum, this manual should include a records retention schedule, documented file systems, an emergency response plan, and records disposition policy and procedures.

Emergency Management for Records and Information

- ☐ Understand the objectives of an emergency management or business continuity plan for records and information.
- ☐ Identify all records media and understand the protection and recovery methods necessary to safeguard each type of records media.
- ☐ Determine any statutory and regulatory requirements for the protection of the organization's records.
- ☐ Determine any elements of the plan that may already exist within the organization.

NOTES

1. Michael Wallace and Lawrence Webber, *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities and Assets* (New York: AMACOM, 2004), xi.
2. Jeffrey B. Bumgarner, *Emergency Management* (California: ABC CLIO, Inc., 2008), 13.
3. Bumgarner, *Emergency Management,* 13.
4. "Some Common Fire Cause," *Fire Safety Fundamentals,* vol. 3 (n.p.: Factory Mutual Systems, n.d.), 2.
5. Bumgarner, *Emergency Management,* 17.
6. Rae Zimmerman, "The Relationship of Emergency Management to Governmental Policies on Man-Made Technological Disasters," *Public Administration Review* 45, special issue January 1985): 37.
7. David McLoughlin, "A Framework for Integrated Emergency Management," *Public Administration Review* 45, special issue (January 1985): 166.
8. McLoughlin, "A Framework for Integrated Emergency Management,"166.
9. McLoughlin, "A Framework for Integrated Emergency Management,"166.
10. Ian Charters FBCI, *A Management Guide to Implementing Global Good Practice in Business Continuity Management, Section 1: BCM Policy & Programme Management* (Business Continuity Institute, United Kingdom: 2008), 5.
11. National Institute of Standards and Technology, SP800-34, *Contingency Planning Guide for Information Technology Systems* (June 2002), D-4.
12. U.S. Code of Federal Regulations §1917.30.
13. Federal Emergency Management Agency, "Good Record Keeping Speeds Local Disaster Recovery," FEMA media release number: 1850-004, Release Date: August 4, 2009.
14. ARMA International, *Glossary of Records and Information Management Terms,* 3rd ed., (Prairie Village, KS: ARMA International, 2007), 20.
15. Krishna Chandler, "Disaster Recovery – Lessons Learned from the Hurricanes," *EMS Newsletter* (October 18, 2005).
16. Wallace and Webber, *The Disaster Recovery Handbook,* xi.