Appendix E

References

- Glossary
- Acronyms
- Bibliography

NCSC
National Center for State Courts

Developed in conjunction with:

DISASTER RECOVERY JOURNAL

DRI INTERNATIONAL

Glossary

A

ACTIVATION: The implementation of business continuity capabilities, procedures, activities, and plans in response to an emergency or disaster declaration; the execution of the recovery plan. Similar terms: Declaration, Invocation.

ADVANCE TEAM: The Advance Team consists of representatives from each Court office that has a COOP plan mission. This is the immediate response element that has primary responsibility for the implementation of the deployment phase of the COOP plan, and establishment of communications connectivity between officials and the Alternate Facility. The Advance Team's duties may include reporting immediately to its normal place of duty or to the Alternate Facility and making it operationally ready to receive the full COOP plan Emergency Relocation Team as soon as possible.

ALTERNATE FACILITY: A facility other than the regular Courthouse, to which designated judge(s), chambers staff (secretary, law clerks), and clerk's office staff move to continue essential court missions and functions in the event the regular courthouse is threatened or incapacitated

ALERT: Notification that a potential disaster situation exists or has occurred; direction for recipient to stand by for possible activation of disaster recovery plan. A formal notification that an incident has occurred, which may develop into a disaster.

ALTERNATE SITE: An alternate operating location to be used by business functions when the primary facilities are inaccessible. 1) Another location, computer center or work area designated for recovery. 2) Location, other than the main facility, that can be used to conduct business functions. 3) A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of a disaster. Related Terms: Cold Site, Hot Site, Interim Site, Internal Hot site, Recovery Site, Warm Site.

ALTERNATE WORK AREA: Office recovery environment complete with necessary office infrastructure (desk, telephone, workstation, and associated hardware, communications, etc.); also referred to as Work Space or Alternative work site.

APPLICATION RECOVERY: The component of Disaster Recovery that deals specifically with the restoration of business system software and data after the processing platform has been restored or replaced. SIMILAR TERMS: Business System Recovery.

ASSEMBLY AREA: The designated area at which employees, visitors, and contractors assemble when evacuated from their building/site.

ASSET: An item of property and/or component of a business activity/process owned by an organization. There are three types of assets: physical assets (e.g. buildings and equipment), financial assets (e.g. currency, bank deposits and shares) and non-tangible assets (e.g. goodwill, reputation)

AUDIT: The process by which procedures and/or documentation are measured against pre-agreed standards.

ASSOCIATE BUSINESS CONTINUITY INSTITUTE (ABCI): BCI Membership for entry-level professionals who are currently in the business continuity or related profession.

ASSOCIATE BUSINESS CONTINUITY PROFESSIONAL (ABCP): DRI International, a non-profit corporation, certifies professionals and promotes credibility and professionalism in the business continuity industry. This is the entry level of certifications and achievable by a passing grade on an exam and approved application. Associated terms: Certified Business Continuity Professional (CBCP), Master Business Continuity Professional (MBCP).

ASYNCHONOUS REPLICATION: Data replication or mirror in which the application is allowed to continue while the data is mirrored to another site. In this case, the application data can represent a prior state of the application. It is critical to use ordered asynchronous mirroring for real-time applications. This means that each write is applied in the same order at the second or backup site as it was written in the primary site, even if the network has re-ordered the arrival of the data. Associated term: synchronous replication.

ANNUAL LOSS EXPOSURE/EXPECTANCY (ALE): A risk management method of calculating loss based on a value and level of frequency.

B

BACKLOG: a) The amount of work that accumulates when a system or process is unavailable for a long period of time. This work needs to be processed once the system or process is available and may take a considerable amount of time to process. b) A situation whereby a backlog of work requires more time to action than is available through normal working patterns. In extreme circumstances, the backlog may become so marked that the backlog cannot be cleared.

BACKUP (Data): A process by which data, electronic or paper based, is copied in some form so as to be available and used if the original data from which it originated is lost, destroyed or corrupted.

BACKUP GENERATOR: An independent source of power, usually fueled by diesel or natural gas.

BUSINESS CONTINUITY: The ability of an organization to provide service and support for its customers and to maintain its viability before, during, and after a business continuity event.

BUSINESS CONTINUITY COORDINATOR: Designated individual responsible for preparing and coordinating the business continuity process. SIMILAR TERMS: disaster recovery coordinator, business recovery coordinator.

BUSINESS CONTINUITY MANAGEMENT (BCM): 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. The management of recovery or continuity in the event of a disaster. Also the management of the overall program through training, rehearsals, and reviews, to ensure the plan stays current and up to date.

BUSINESS CONTINUITY PLAN ADMINISTRATOR: The designated individual responsible for plan documentation, maintenance, and distribution.

BUSINESS CONTINUITY MANAGEMENT PROCESS: The Business Continuity Institute's BCM process (also known as the BC Life Cycle) combines 6 key elements: 1) Understanding Your Business 2) Continuity Strategies 3) Developing a BCM Response 4) Establishing a Continuity Culture 5) Exercising, Rehearsal & Testing 6) The BCM Management Process.

BUSINESS CONTINUITY MANAGEMENT PROGRAM: An ongoing management and governance process supported by senior management and resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of products/services through exercising, rehearsal, testing, training, maintenance and assurance.

BUSINESS CONTINUITY MANAGEMENT TEAM: A group of individuals functionally responsible for directing the development and execution of the business continuity plan, as well as responsible for declaring a disaster and providing direction during the recovery process, both pre-disaster and post-disaster. SIMILAR TERMS: disaster recovery management team, business recovery management team. Associated terms: crisis management team.

BUSINESS CONTINUITY PLAN (BCP): Process of developing and documenting arrangements and procedures that enable an organization to respond to an event that lasts for an unacceptable period of time and return to performing its critical functions after an interruption. SIMILAR TERMS: business resumption plan, continuity plan, contingency plan, disaster recovery plan, recovery plan.

BUSINESS CONTINUITY STEERING COMMITTEE: A committee of decision makers, process owners, technology experts and continuity professionals, tasked with making strategic recovery and continuity planning decisions for the organization.

BUSINESS CONTINUITY STRATEGY: An approach by an organization that will ensure its recovery and continuity in the face of a disaster or other major outage. Plans and methodologies are determined by the organizations strategy. There may be more than one solution to fulfill an organization's strategy. Examples: Internal or external hot-site, or cold-site, Alternate Work Area reciprocal agreement, Mobile Recovery, Quick Ship / Drop Ship, Consortium-based solutions, etc.

BUSINESS CONTINUITY TEAM: Designated individuals responsible for developing, execution, rehearsals, and maintenance of the business continuity plan, including the processes and procedures. SIMILAR TERMS: disaster recovery team, business recovery team, and recovery team. Associated term: crisis response team.

BUSINESS IMPACT ANALYSIS (BIA): A process designed to prioritize business functions by assessing the potential quantitative (financial) and qualitative (non-financial) impact that might result if an organization was to experience a business continuity event.

BUSINESS INTERRUPTION: Any event, whether anticipated (i.e., public service strike) or unanticipated (i.e., blackout) which disrupts the normal course of business operations at an organization's location. SIMILAR TERMS: outage, service interruption. Associated terms: business interruption costs, business interruption insurance.

BUSINESS INTERRUPTION COSTS: The impact to the business caused by different types of outages, normally measured by revenue lost. Associated terms: business interruption, business interruption insurance.

BUSINESS INTERRUPTION INSURANCE: Insurance coverage for disaster related expenses that may be incurred until operations are fully recovered after a disaster. Business interruption insurance generally provides reimbursement for necessary ongoing expenses during this shutdown, plus loss of net profits that would have been earned during the period of interruption, within the limits of the policy. Associated terms: business interruption, business interruption costs.

BUSINESS RECOVERY COORDINATOR: An individual or group designated to coordinate or control designated recovery processes or testing. SIMILAR TERMS: Disaster Recovery Coordinator.

BUSINESS RECOVERY TIMELINE: The chronological sequence of recovery activities, or critical path that must be followed to resume an acceptable level of operations following a business interruption. This timeline may range from minutes to weeks, depending upon the recovery requirements and methodology.

BUSINESS RESUMPTION PLANNING (BRP): TERM Currently Being Reworked - SIMILAR TERMS: Business Continuity Planning, Disaster Recovery Planning.

BUSINESS RECOVERY TEAM: A group of individuals responsible for maintaining the business recovery procedures and coordinating the recovery of business functions and processes. SIMILAR TERMS: Disaster Recovery Team.

BUSINESS UNIT RECOVERY: The component of Disaster Recovery which deals specifically with the relocation of a key function or department in the event of a disaster, including personnel, essential records, equipment supplies, work space, communication facilities, work station computer processing capability, fax, copy machines, mail services, etc. SIMILAR TERMS: Work Group Recovery.

C

CALL TREE: A document that graphically depicts the calling responsibilities and the calling order used to contact management, employees, customers, vendors, and other key contacts in the event of an emergency, disaster, or severe outage situation.

CERTIFIED BUSINESS CONTINUITY PROFESSIONAL (CBCP): The Disaster Recovery Institute International (DRI International), a not-for-profit corporation, certifies CBCP's and promotes credibility and professionalism in the business continuity industry. Also offers MBCP (Master Business Continuity Professional) and ABCP (Associate Business Continuity Professional).

CHECKLIST: a) Tool to remind and /or validate that tasks have been completed and resources are available, to report on the status of recovery. b) A list of items (names or tasks etc.) to be checked or consulted.

CHECKLIST EXERCISE: A method used to exercise a completed disaster recovery plan. This type of exercise is used to determine if the information such as phone numbers, manuals, equipment, etc. in the plan is accurate and current.

COLD SITE: An alternate facility that already has in place the environmental infrastructure required to recover critical business functions or information systems, but does not have any pre-installed computer hardware, telecommunications equipment, communication lines, etc. These must be provisioned at time of disaster. Related Terms: Alternate Site, Hot Site, Interim Site, Internal Hot Site, Recovery Site, and Warm Site.

COMMAND CENTER: A physical or virtual facility located outside of the affected area used to gather, assess, and disseminate information and to make decisions to affect recovery.

COMMUNICATIONS RECOVERY: The component of Disaster Recovery which deals with the restoration or rerouting of an organization's telecommunication network, or its components, in the event of loss. SIMILAR TERMS: Telecommunications Recovery, Data Communications Recovery.

COMPUTER RECOVERY TEAM: A group of individuals responsible for assessing damage to the original system, processing data in the interim, and setting up the new system.

CONSORTIUM AGREEMENT: An agreement made by a group of organizations to share processing facilities and/or office facilities, if one member of the group suffers a disaster. SIMILAR TERMS: Reciprocal Agreement.

CONTINUITY OF OPERATIONS (COOP) PLAN: An action plan that provides for the uninterrupted execution of essential missions and functions of an organization in the event an emergency prevents occupancy of its primary headquarters building.

CONTACT LIST: A list of team members and/or key players to be contacted including their backups. The list will include the necessary contact information (i.e. home phone, pager, cell, etc.) and in most cases be considered confidential.

CONTINGENCY PLAN: A plan used by an organization or business unit to respond to a specific systems failure or disruption of operations. A contingency plan may use any number of resources including workaround procedures, an alternate work area, a reciprocal agreement, or replacement resources.

CONTINGENCY PLANNING: Process of developing advance arrangements and procedures that enable an organization to respond to an event that could occur by chance or unforeseen circumstances.

CONTINUITY OF OPERATIONS PLAN (COOP): A COOP provides guidance on the system restoration for emergencies, disasters, mobilization, and for maintaining a state of readiness to provide the necessary level of information processing support commensurate with the mission requirements/priorities identified by the respective functional proponent. The Federal Government and its supporting agencies traditionally use this term to describe activities otherwise known as Disaster Recovery, Business Continuity, Business Resumption, or Contingency Planning.

CRATE & SHIP: A strategy for providing alternate processing capability in a disaster, via contractual arrangements with an equipment supplier, to ship replacement hardware within a specified time period. SIMILAR TERMS: Guaranteed Replacement, Drop Ship, Quick Ship.

CRISIS: A critical event, which, if not handled in an appropriate manner, may dramatically impact an organization's profitability, reputation, or ability to operate. Or, an occurrence and/or perception that threatens the operations, staff, shareholder value, stakeholders, brand, reputation, trust and/or strategic/business goals of an organization. See: Event and Incident.

CRISIS MANAGEMENT: The overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, or ability to operate.

CRISIS MANAGEMENT TEAM: A crisis management team will consist of key executives as well as key role players (i.e. media representative, legal counsel, facilities manager, disaster recovery coordinator, etc.) and the appropriate business owners of critical organization functions who are responsible for recovery operations during a crisis.

CRISIS SIMULATION: The process of testing an organization's ability to respond to a crisis in a coordinated, timely, and effective manner by simulating the occurrence of a specific crisis.

CRITICAL FUNCTIONS: See: Mission Critical Activities.

CRITICAL INFRASTRUCTURE: Systems whose incapacity or destruction would have a debilitating impact on the economic security of an organization, community, nation, etc.

CRITICAL RECORDS: Records or documents that, if damaged or destroyed, would cause considerable inconvenience and/or require replacement or recreation at considerable expense.

D

DAMAGE ASSESSMENT: The process of assessing damage, following a disaster, to computer hardware, vital records, office facilities, etc. and determining what can be salvaged or restored and what must be replaced.

DATA BACKUPS: The back up of system, application, program and/or production files to media that can be stored both on and/or offsite. Data backups can be used to restore corrupted or lost data or to recover entire systems and databases in the event of a disaster. Data backups should be considered confidential and should be kept secure from physical damage and theft.

DATA BACKUP STRATEGIES: Those actions and backup processes determined by an organization to be necessary to meet its data recovery and restoration objectives. Data backup strategies will determine the timeframes, technologies, media and offsite storage of the backups, and will ensure that recovery point and time objectives can be met.

DATA CENTER RECOVERY: The component of Disaster Recovery which deals with the restoration, at an alternate location, of data center services and computer processing capabilities. SIMILAR TERMS: Mainframe Recovery, Technology Recovery.

DATA RECOVERY: The restoration of computer files from backup media to restore programs and production data to the state that existed at the time of the last safe backup.

DATABASE REPLICATION: The partial or full duplication of data from a source database to one or more destination databases. Replication may use any of a number of methodologies including mirroring or shadowing, and may be performed synchronous, asynchronous, or point-in-time depending on the technologies used, recovery point requirements, distance and connectivity to the source database, etc. Replication can if performed remotely, function as a backup for disasters and other major outages. (SIMILAR TERMS: File Shadowing, Disk Mirroring).

DECLARATION: A formal announcement by pre-authorized personnel that a disaster or severe outage is predicted or has occurred and that triggers pre-arranged mitigating actions (e.g., a move to an alternate site.) SIMILAR TERMS: Invocation.

DECLARATION FEE: A one-time fee, charged by an Alternate Facility provider, to a customer who declares a disaster. NOTE: Some recovery vendors apply the declaration fee against the first few days of recovery. 1) An initial fee or charge for implementing the terms of a recovery agreement or contract. SIMILAR TERMS: Notification Fee.

DEPENDENCY: The reliance, directly or indirectly, of one activity or process upon another. See: Mission Critical Activity.

DESK CHECK: One method of validating a specific component of a plan. Typically, the owner of the component reviews it for accuracy and completeness and signs off.

DESKTOP EXERCISE: See: Table Top Exercise.

DISASTER: A sudden, unplanned calamitous event causing great damage or loss as defined or determined by a risk assessment and BIA; 1) Any event that creates an inability on an organization's part to provide critical business functions for some predetermined period of time. 2) In the business environment, any event that creates an inability on an organization's part to provide the critical business functions for some predetermined period of time. 3) The period when company management decides to divert from normal production responses and exercises its disaster recovery plan. Typically signifies the beginning of a move from a primary to an alternate location. SIMILAR TERMS: Business Interruption; Outage; Catastrophe.

DISASTER RECOVERY: Activities and programs designed to return the entity to an acceptable condition. The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's critical business functions.

DISASTER RECOVERY OR BUSINESS CONTINUITY COORDINATOR: A role of the BCM program that coordinates planning and implementation for overall recovery of an organization or unit(s). SIMILAR ROLES: Business Recovery Coordinator, Business Recovery Planner, Disaster Recovery Planner, and Disaster Recovery Administrator.

DISASTER RECOVERY INSTITUTE INTERNATIONAL (DRI INTERNATIONAL): A not-for-profit organization that offers certification and educational offerings for business continuity professionals.

DISASTER RECOVERY PLAN: The management-approved document that defines the resources, actions, tasks and data required to manage the recovery effort. Usually refers to the technology recovery effort.

DISASTER RECOVERY PLANNING: The technological aspect of business continuity planning. The advance planning and preparation that is necessary to minimize loss and ensure continuity of the critical business functions of an organization in the event of disaster. SIMILAR TERMS: Contingency Planning; Business Resumption Planning; Corporate Contingency Planning; Business Interruption Planning; Disaster Preparedness.

DISASTER RECOVERY SOFTWARE: An application program developed to assist an organization in writing a comprehensive disaster recovery plan.

DISASTER RECOVERY TEAMS (Business Recovery Teams): A structured group of teams ready to take control of the recovery operations if a disaster should occur.

DISK MIRRORING: Disk mirroring is the duplication of data on separate disks in real time to ensure its continuous availability, currency and accuracy. Disk mirroring can function as a disaster recovery solution by performing the mirroring remotely. True mirroring will enable a zero recovery point objective. Depending on the technologies used, mirroring can be performed synchronously, asynchronously, semi-synchronously, or point-in-time. SIMILAR TERMS: data mirroring, data replication, file shadowing, and journaling.

DROP SHIP: A strategy for **a)** Delivering equipment, supplies, and materials at the time of a business continuity event or exercise. **b)** Providing replacement hardware within a specified time period via prearranged contractual arrangements with an equipment supplier at the time of a business continuity event. SIMILAR TERM: quick ship.

E

ELECTRONIC VAULTING: Electronically forwarding backup data to an offsite server or storage facility. Vaulting eliminates the need for tape shipment and therefore significantly shortens the time required to move the data offsite. SIMILAR TERMS: vaulting, electronic backup. Associated terms: electronic journaling.

EMERGENCY: An unexpected or impending situation that may cause injury, loss of life, destruction of property, or cause the interference, loss, or disruption of an organization's normal business operations to such an extent that it poses a threat.

EMERGENCY COORDINATOR: The person assigned the role of coordinating the activities of the evacuation of a site and/or building with the statutory and/or emergency services.

EMERGENCY OPERATIONS CENTER (EOC): A site from which response teams/officials (municipal, county, state and federal) exercise direction and control in an emergency or disaster. Associated term: command center.

EMERGENCY PREPAREDNESS: The discipline that ensures an organization or community's readiness to respond to an emergency in a coordinated, timely, and effective manner to prevent the loss of life and minimize injury and property damage.

EMERGENCY PROCEDURES: A plan of action to commence immediately to prevent the loss of life and minimize injury and property damage.

EMERGENCY RELOCATION SITE: The Emergency Relocation Site (referred to in this plan as Alternate Facility) contains the Court's COOP plan operating facility that is located outside a prime target area to which all or part of the court's essential functions may be moved in a specified disaster situation. An Alternate Facility has the minimum essential communications and information systems to enable the headquarters to continue performing essential missions and functions.

EMERGENCY RELOCATION TEAM: The Emergency Relocation Team consists of representatives from each court office that has a COOP plan. The primary Emergency Relocation Team responsibility is to help the court sustain essential functions while at the Alternate Facility. The Emergency Relocation Team also coordinates with the Alternate Facility, other COOP support teams and key agency officials during an emergency.

EMERGENCY RESPONSE PROCEDURES: The initial response to any event and is focused upon protecting human life and the organization's assets.

EMERGENCY RESPONSE TEAM (ERT): Teams of individuals who have been trained to provide rapid response to all type of emergencies and to provide assistance and act as a contact to responding outside agencies. Associated term: medical emergency response team (MERT).

ENVIRONMENT RESTORATION: Recreation of the critical business operations in an alternate location, including people, equipment and communications capability.

ENTERPRISE WIDE PLANNING: Enterprise Wide Planning is the development and implementation of a plan document to facilitate the resumption of critical business functions, (including, but not limited to, Human Resources, Facilities, Information Technology, Finance, Security, Engineering, and Sales and Marketing), to the extent that the incident causing plan activation is transparent to the organization's customers. This Enterprise Wide Planning process involves the coordination, prioritization, resource allocation, and implementation of critical business function strategies to resume normal operating capabilities.

ESCALATION: The process by which event related information is communicated upwards through an organization's Business Continuity and/or risk management reporting process.

ESSENTIAL FUNCTIONS: Essential functions are those functions, stated or implied, which are required to be performed by statute or other order, or other functions deemed essential by the chief judges and clerk of court that should not be interrupted or deferred by an emergency situation.

ESSENTIAL SERVICE: A service without which a building would be 'disabled'. Often applied to the utilities (water, gas, electricity, etc.) it may also include standby power systems, environmental control systems or communication networks.

EVACUATION: The movement of employees, visitors and contractors from a site and/or building to a safe place (assembly area) in a controlled and monitored manner at time of an event.

EVENT: Any occurrence that may lead to a business continuity incident. See: Crisis and Incident.

EXECUTIVE / MANAGEMENT SUCCESSION: A predetermined plan for ensuring the continuity of authority, decision-making, and communication in the event that key members of senior management suddenly become incapacitated, or in the event that a crisis occurs while key members of senior management are unavailable.

EXERCISE: A people focused activity designed to execute business continuity plans and evaluate the individual and/or organization performance against approved standards or objectives. Exercises can be announced or unannounced, and are performed for the purpose of training and conditioning team members, and validating the business continuity plan.

Exercise results identify plan gaps and limitations and are used to improve and revise the Business Continuity Plans.Types of exercises include: Table Top Exercise, Simulation Exercise, Operational Exercise, Mock Disaster, Desktop Exercise, and Full Rehearsal.

EXERCISE AUDITOR: An appointed role that is assigned to assess whether the exercise aims / objectives are being met and to measure whether activities are occurring at the right time and involve the correct people to facilitate their achievement. The exercise auditor is not responsible for the mechanics of the exercise. This independent role is crucial in the subsequent debriefing.

EXERCISE CONTROLLER: See Exercise Owner.

EXERCISE COORDINATOR: They are responsible for the mechanics of running the exercise. The Coordinator must lead the exercise and keep it focused within the predefined scope and objectives of the exercise as well as on the disaster scenario. The Coordinator must be objective and not influence the outcome. They perform the coordination to make sure appropriate exercise participants have been identified and that exercise scripts have been prepared before, utilized during, and updated after the exercise. SIMILAR TERMS: Exercise Facilitator, Exercise Director.

EXERCISE OBSERVER: An exercise observer has no active role within the exercise but is present for awareness and training purposes. An exercise observer might make recommendations for procedural improvements.

EXERCISE OWNER: An appointed role that has total management oversight and control of the exercise and has the authority to alter the exercise plan. This includes early termination of the exercise for reasons of safety or the aims / objectives of the exercise cannot be met due to an unforeseen or other internal or external influence.

EXERCISE PLAN: A plan designed to periodically evaluate tasks, teams, and procedures that are documented in business continuity plans to ensure the plan's viability. This can include all or part of the BC plan, but should include mission critical components.

EXPOSURE: The potential susceptibility to loss; the vulnerability to a particular risk.

EXTRA EXPENSE: The extra cost necessary to implement a recovery strategy and/or mitigate a loss. An example is the cost to transfer inventory to an alternate location to protect it from further damage, cost of reconfiguring lines, overtime costs, etc. Typically reviewed during BIA and is a consideration during insurance evaluation.

F

FELLOW BUSINESS CONTINUITY INSTITUTE (FBCI): Membership accreditation from the Business Continuity Institute for a senior, professional working practitioner with five years of full-time employment who currently works in the business continuity related profession and a member of the BCI for two years.

FILE SHADOWING: The asynchronous duplication of the production database on separate media to ensure data availability, currency and accuracy. File shadowing can be used as a disaster recovery solution if performed remotely, to improve both the recovery time and recovery point objectives. SIMILAR TERMS: Data Replication, Journaling, Disk Mirroring.

FLOOR WARDEN: Person responsible for ensuring that all employees, visitors and contractors evacuate a floor within a specific site.

FORWARD RECOVERY: The process of recovering a database to the point of failure by applying active journal or log data to the current backup files of the database.

FULL REHEARSAL: An exercise that simulates a Business Continuity event where the organization or some of its component parts are suspended until the exercise is completed. See: Exercise

G

GAP ANALYSIS: A detailed examination to identify risks associated with the differences between Business/Operations requirements and the current available recovery capabilities.

H

HAZARD OR THREAT IDENTIFICATION: The process of identifying situations or conditions that has the potential to cause injury to people, damage to property, or damage to the environment.

HEALTH AND SAFETY: The process by which the well being of all employees, contractors, visitors and the public is safeguarded. All business continuity plans and planning must be cognizant of H&S statutory and regulatory requirements and legislation. Health and Safety considerations should be reviewed during the Risk Assessment.

HIGH AVAILABILITY: Systems or applications requiring a very high level of reliability and availability. High availability systems typically operate 24x7 and usually require built-in redundancy to minimize the risk of downtime due to hardware and/or telecommunication failures.

HIGH-RISK AREAS: Areas identified during the risk assessment that are highly susceptible to a disaster situation or might be the cause of a significant disaster.

HOTSITE: An alternate facility that already has in place the computer, telecommunications, and environmental infrastructure required to recover critical business functions or information systems. Related Terms: Alternate Site, Cold Site, and Warm Site.

HUMAN THREATS: Possible disruptions in operations resulting from human actions. (e.g., disgruntled employee, terrorism, blackmail, job actions, riots, etc.).

I

IMPACT: The effect, acceptable or unacceptable, of an event on an organization. The types of business impact are usually described as financial and non-financial and are further divided into specific types of impact. See: Business Impact Analysis.

INCIDENT: An event which is not part of a standard operating business, which may impact or interrupt services, and in some cases, may lead to disaster. See: Crisis and Event.

INCIDENT COMMAND SYSTEM (ICS): Combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure with responsibility for management of assigned resources to effectively direct and control the response to an incident. Intended to expand, as situation requires larger resources, without requiring new, reorganized command structure. (FEMA Term).

INCIDENT MANAGEMENT: The process by which an organization responds to and controls an incident using Emergency Response Procedures. See: Emergency Response Procedures.

INCIDENT MANAGER: Commands the local EOC reporting up to senior management on the recovery progress. Has the authority to invoke the local recovery plan.

INCIDENT RESPONSE: The response of an organization to a disaster or other significant event that may significantly impact the organization, its people, or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan, performing damage assessment, and any other measures necessary to bring an organization to a more stable status.

INFORMATION SECURITY: The securing or safeguarding of all sensitive information, electronic or otherwise, which is owned by an organization. See: BS 7799 and ISO 17799.

INFRASTRUCTURE: The underlying foundation, basic framework, or interconnecting structural elements that support an organization.

INTEGRATED EXERCISE: An exercise conducted on multiple interrelated components of a Business Continuity Plan, typically under simulated operating conditions. Examples of interrelated components may include interdependent departments or interfaced systems.

INTEGRATED TEST: See integrated exercise.

INTERIM SITE: A temporary location used to continue performing business functions after vacating a recovery site and before the original or new home site can be occupied. Move to an interim site may be necessary if ongoing stay at the recovery site is not feasible for the period of time needed or if the recovery site is located far from the normal business site that was impacted by the disaster. An interim site move is planned and scheduled in advance to minimize disruption of business processes; equal care must be given to transferring critical functions from the interim site back to the normal business site. See Alternate Site, Cold Site, Hot site, Internal Hot Site, Recovery Site, Warm site.

INTERNAL HOTSITE: A fully equipped alternate processing site owned and operated by the organization.

INVOCATION: The act by which a Business Continuity Management or Crisis Management process is formally started. The term is often used to refer to the act of using a service such as work area recovery as offered by a commercial or third party provider. See: Activation and Declaration.

J

JOURNALING: The process of logging changes or updates to a database since the last full backup. Journals can be used to recover previous versions of a file before updates were made, or to facilitate disaster recovery, if performed remotely, by applying changes to the last safe backup. SIMILAR TERMS: File Shadowing, Data Replication, Disk Mirroring.

K

KEY STAFF: Key staff members are those personnel from particular offices designated by their organizational element as critical to the conduct of COOP plan operations. The loss of these key staff personnel during a crisis would result in actions to replace them.

KEY TASKS: Priority procedures and actions in a Business Continuity Plan that must be executed within the first few minutes/hours of the plan invocation.

L

LEAD TIME: The time it takes for a supplier to make equipment, services, or supplies available after receiving an order. Business continuity plans should try to minimize lead time by creating service level agreements (SLA) with suppliers or alternate suppliers in advance of a Business Continuity event rather than relying on the suppliers' best efforts. See: Service Level Agreement.

LOGISTICS/TRANSPORTATION TEAM: A team comprised of various members representing departments associated with supply acquisition and material transportation, responsible for ensuring the most effective acquisition and mobilization of hardware, supplies, and support materials. This team is also responsible for transporting and supporting staff.

LOSS: Unrecoverable resources that are redirected or removed as a result of a Business Continuity event. Such losses may be loss of life, revenue, market share, competitive stature, public image, facilities, or operational capability.

LOSS ADJUSTER: Designated position activated at the time of a Business Continuity event to assist in managing the financial implications of the event and should be involved as part of the management team where possible.

LOSS REDUCTION: The technique of instituting mechanisms to lessen the exposure to a particular risk. Loss reduction involves planning for, and reacting to, an event to limit its impact. Examples of loss reduction include sprinkler systems, insurance policies, and evacuation procedures.

LOST TRANSACTION RECOVERY: Recovery of data (paper within the work area and/or system entries) destroyed or lost at the time of the disaster or interruption. Paper documents may need to be requested or re-acquired from original sources. Data for system entries may need to be recreated or reentered.

M

MANUAL PROCEDURES: An alternative method of working following a loss of IT systems. As working practices rely more and more on computerized activities, the ability of an organization to fallback to manual alternatives lessens. However, temporary measures and methods of working can help mitigate the impact of a business continuity event and give staff a feeling of doing something.

MISSION-CRITICAL ACTIVITIES: The critical operational and/or business support activities (either provided internally or outsourced) required by the organization to achieve its objective(s) i.e. services and/or products. See Critical Service.

MISSION-CRITICAL APPLICATION: An application that is essential to the organization's ability to perform necessary business functions. Loss of the mission-critical application would have a negative impact on the business, as well as legal or regulatory impacts.

MOBILE RECOVERY: A mobilized resource purchased or contracted for the purpose of business recovery. The mobile recovery center might include: computers, workstations, telephone, electrical power, etc.

MOCK DISASTER: One method of exercising teams in which participants are challenged to determine the actions they would take in the event of a specific disaster scenario. Mock disasters usually involve all, or most, of the applicable teams. Under the guidance of exercise coordinators, the teams walk through the actions they would take per their plans, or simulate performance of these actions. Teams may be at a single exercise location, or at multiple locations, with communication between teams simulating actual 'disaster mode' communications. A mock disaster will typically operate on a compressed timeframe representing many hours, or even days.

N

N + 1: A fault tolerant strategy that includes multiple systems or components protected by one backup system or component. (Many-to-one relationship).

NETWORK OUTAGE: An interruption of voice, data, or IP network communications.

O

OFF-SITE STORAGE: Any place physically located a significant distance away from the primary site, where duplicated and vital records (hard copy or electronic and/or equipment) may be stored for use during recovery.

OPERATIONAL EXERCISE: See: Exercise.

OPERATIONAL RISK: The risk of loss resulting from inadequate or failed procedures and controls. This includes loss from events related to technology and infrastructure, failure, business interruptions, staff related problems, and from external events such as regulatory changes.

OUTAGE: The interruption of automated processing systems, infrastructure, support services, or essential business operations, which may result, in the organizations inability to provide services for some period of time.

P

PEER REVIEW: One method of testing a specific component of a plan. Typically, personnel (other than the owner or author) with appropriate technical or business knowledge review the component for accuracy and completeness.

PLAN ADMINISTRATOR: The individual responsible for documenting recovery activities and tracking recovery progress.

PLAN MAINTENANCE: The management process of keeping an organization’s Business continuity management plans up to date and effective. Maintenance procedures are a part of this process for the review and update of the BC plans on a defined schedule. Maintenance procedures are a part of this process.

PRE-POSITIONED ITEMS: Pre-positioned items include critical resources and unique items of equipment (e.g., computer and paper files or databases, special supplies, etc.) that can be duplicated and stored at the Alternate Facility.

PREVENTATIVE MEASURES: Controls aimed at deterring or mitigating undesirable events form taking place.

PRIORITIZATION: The ordering of critical activities and their dependencies are established during the BIA and Strategic-planning phase. The business continuity plans will be implemented in the order necessary at the time of the event.

Q

QUALITATIVE ASSESSMENT: The process for evaluating a business function based on observations and does not involve measures or numbers. Instead, it uses descriptive categories such as customer service, regulatory requirements, etc to allow for refinement of the quantitative assessment. This is normally done during the BIA phase of planning.

QUANTITATIVE ASSESSMENT: The process for placing value on a business function for risk purposes. It is a systematic method that evaluates possible financial impact for losing the ability to perform a business function. It uses numeric values to allow for prioritizations. This is normally done during the BIA phase of planning.

QUICK SHIP: See Drop Ship.

R

RECIPROCAL AGREEMENT: Agreement between two organizations (or two internal business groups) with similar equipment/environment that allows each one to recover at the other's location.

RECONSTITUTION: Also known as recovery, the transition process involving the conclusion of continuity of operations efforts and the resumption of normal operations.

RECOVERABLE LOSS: Financial losses due to an event that may be reclaimed in the future, e.g. through insurance or litigation. This is normally identified in the Risk Assessment or BIA.

RECOVERY: Implementing the prioritized actions required to return the processes and support functions to operational stability following an interruption or disaster.

RECOVERY MANAGEMENT TEAM: See: Business Continuity Management (BCM) Team.

RECOVERY PERIOD: The time period between a disaster and a return to normal functions, during which the disaster recovery plan is employed.

RECOVERY POINT OBJECTIVE (RPO): From a business perspective RPO is the maximum amount of data loss the business can incur in an event. The targeted point in time to which systems and data must be recovered after an outage as determined by the business unit.

RECOVERY SERVICES AGREEMENT / CONTRACT: A contract with an external organization guaranteeing the provision of specified equipment, facilities, or services, usually within a specified time period, in the event of a business interruption. A typical contract will specify a monthly subscription fee, a declaration fee, usage costs, method of performance, amount of test time, termination options, penalties and liabilities, etc.

RECOVERY SITE: A designated site for the recovery of business unit, technology, or other operations, which are critical to the enterprise. Related Terms: Alternate Site, Cold Site, Hot Site, Interim Site, Internal Hot Site, and Warm Site.

RECOVERY STRATEGY: See business continuity strategy.

RECOVERY TEAM: See: Business Continuity Team.

RECOVERY TIME OBJECTIVE (RTO): The period of time within which systems, applications, or functions must be recovered after an outage (e.g. one business day). RTO's are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation. SIMILAR TERMS: Maximum Allowable Downtime.

RECOVERY TIMELINE: The sequence of recovery activities, or critical path, which must be followed to resume an acceptable level of operation following a business interruption. The timeline may range from minutes to weeks, depending upon the recovery requirements and methodology.

RELOCATION: Relocation is the movement of a deployed team from a specified location to an Alternate Facility.

RESILIENCE: The ability of an organization to absorb the impact of a business interruption, and continue to provide a minimum acceptable level of service.

RESPONSE: The reaction to an incident or emergency to assess the damage or impact and to ascertain the level of containment and control activity required. In addition to addressing matters of life safety and evacuation, Response also addresses the policies, procedures and actions to be followed in the event of an emergency. SIMILAR TERMS: Emergency Response, Disaster Response, Immediate Response, and Damage Assessment.

RESTORATION: Process of planning for and/or implementing procedures for the repair of hardware, relocation of the primary site and its contents, and returning to normal operations at the permanent operational location.

RESUMPTION: The process of planning for and/or implementing the restarting of defined business processes and operations following a disaster. This process commonly addresses the most critical business functions within BIA specified timeframes.

RISK: Potential for exposure to loss. Risks, either man-made or natural, are constant. The potential is usually measured by its probability in years.

RISK ASSESSMENT / ANALYSIS: The process of identifying the risks to an organization, assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.

RISK CATEGORIES: Risks of similar types are grouped together under key headings, otherwise known as 'risk categories'. These categories include reputation, strategy, financial, investments, operational infrastructure, business, regulatory compliance, outsourcing, people, technology and knowledge.

RISK MITIGATION: The implementation of measures to deter specific threats to the continuity of business operations, and/or respond to any occurrence of such threats in a timely and appropriate manner.

S

SALVAGE & RESTORATION: The act of performing a coordinated assessment to determine the appropriate actions to be performed on impacted assets. The assessment can be coordinated with insurance adjusters, facilities personnel, or other involved parties. Appropriate actions may include: disposal, replacement, reclamation, refurbishment, recovery or receiving compensation for unrecoverable organizational assets.

SCENARIO: A pre-defined set of Business Continuity events and conditions that describe, for planning purposes, an interruption, disruption, or loss related to some aspect(s) of an organization's business operations to support conducting a BIA, developing a continuity strategy, and developing continuity and exercise plans. **Note:** Scenarios are neither predictions nor forecasts.

SECURITY REVIEW: A periodic review of policies, procedures, and operational practices maintained by an organization to ensure that they are followed and effective.

SELF INSURANCE: The pre-planned assumption of risk in which a decision is made to bear loses that could result from a Business Continuity event rather than purchasing insurance to cover those potential losses.

SERVICE LEVEL AGREEMENT (SLA): A formal agreement between a service provider (whether internal or external) and their client (whether internal or external), which covers the nature, quality, availability, scope and response of the service provider. The SLA should cover day-to-day situations and disaster situations, as the need for the service may vary in a disaster.

SERVICE LEVEL MANAGEMENT (SLM): The process of defining, agreeing, documenting and managing the levels of any type of services provided by service providers whether internal or external that are required and cost justified.

SIMULATION EXERCISE: One method of exercising teams in which participants perform some or all of the actions they would take in the event of plan activation. Simulation exercises, which may involve one or more teams, are performed under conditions that at least partially simulate 'disaster mode'. They may or may not be performed at the designated alternate location, and typically use only a partial recovery configuration.

SINGLE POINT OF FAILURE: (SPOF) A unique pathway or source of a service, activity, and/or process. Typically, there is no alternative and a loss of that element could lead to a failure of a critical function.

STAND DOWN: Formal notification that the response to a Business Continuity event is no longer required or has been concluded.

STANDALONE TEST: A test conducted on a specific component of a plan in isolation from other components to validate component functionality, typically under simulated operating conditions.

STRUCTURED WALKTHROUGH: Types of exercise in which team members physically implement the business continuity plans and verbally review each step to assess its effectiveness, identify enhancements, constraints and deficiencies. See: Exercise.

SUBSCRIPTION: See: Recovery Services Agreement \ Contract.

SUPPLY CHAIN: All suppliers, manufacturing facilities, distribution centers, warehouses, customers, raw materials, work-in-process inventory, finished goods, and all related information and resources involved in meeting customer and organizational requirements.

SYSTEM: Set of related technology components that work together to support a business process or provide a service.

SYSTEM RECOVERY: The procedures for rebuilding a computer system and network to the condition where it is ready to accept data and applications, and facilitate network communications.

SYSTEM RESTORE: The procedures necessary to return a system to an operable state using all available data including data captured by alternate means during the outage. System restore depends upon having a live, recovered system available.

T

TABLE TOP EXERCISE: One method of exercising plans in which participants review and discuss the actions they would take without actually performing the actions. Representatives of a single team, or multiple teams, may participate in the exercise typically under the guidance of exercise facilitators.

TASK LIST: Defined mandatory and discretionary tasks allocated to teams and/or individual roles within a Business Continuity Plan.

TEST: A pass/fail evaluation of infrastructure (example-computers, cabling, devices, hardware) and/or physical plant infrastructure (example-building systems, generators, utilities) to demonstrate the anticipated operation of the components and system. Tests are often performed as part of normal operations and maintenance. Tests are often included within exercises.

THREAT: A combination of the risk, the consequence of that risk, and the likelihood that the negative event will take place. Associated term: risk. Example Threats: Natural, Man-made, Technological, and Political disasters).

TRAUMA COUNSELING: The provisioning of counseling assistance by trained individuals to employees, customers and others who have suffered mental or physical injury as the result of an event.

TRAUMA MANAGEMENT: The process of helping employees deal with trauma in a systematic way following an event by proving trained counselors, support systems, and coping strategies with the objective of restoring employees psychological well being.

U

UNEXPECTED LOSS: The worst-case financial loss or impact that a business could incur due to a particular loss event or risk. The unexpected loss is calculated as the expected loss plus the potential adverse volatility in this value. It can be thought of as the worst financial loss that could occur in a year over the next 20 years.

UNINTERRUPTIBLE POWER SUPPLY (UPS): A backup supply that provides continuous power to critical equipment in the event that commercial power is lost.

V

VALIDATION SCRIPT: A set of procedures within the Business Continuity Plan to validate the proper function of a system or process before returning it to production operation.

VITAL RECORD: A record that must be preserved and available for retrieval if needed.

W

WARM SITE: An alternate processing site which is equipped with some hardware, and communications interfaces, electrical and environmental conditioning which is only capable of providing backup after additional provisioning, software or customization is performed.

WORKAROUND PROCEDURES: Interim procedures that may be used by a business unit to enable it to continue to perform its critical functions during temporary unavailability of specific application systems, electronic or hard copy data, voice or data communication systems, specialized equipment, office facilities, personnel, or external services. SIMILAR TERMS: Interim Contingencies.

ABC Acronyms

The following acronyms are used in this document and are commonly encountered in COOP planning and execution.

BIA	Business Impact Analysis
COOP	Continuity of Operations
CFR	Code of Federal Regulations
DOC	Department of Corrections
DRP	Disaster Recovery Plan (IT)
EO	Executive Order
FEMA	Federal Emergency Management Agency
FPC	Federal Preparedness Circular
HSAS	Homeland Security Advisory System
HSC	Homeland Security Council
HSPD	Homeland Security Presidential Directive
IT	Information Technology
MOU	Memorandum of Understanding
NARA	National Archives & Records Administration
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
PDD	Presidential Decision Directive
POC	Point of Contact
TT&E	Tests, Training, and Exercises

✍ Bibliography

Recommended Top Titles

2006/07 Disaster Resource Guide. <http://www.disaster-resource.com/cgi-bin/freeguide.cgi>

Bernardino, Arthur J., Jr., et al. *Business Continuity Management Mini Guide*. Williamsburg, Va.: National Association for Court Management, 2006.

Courts in the Aftermath of September 11th: Nine-Eleven Summit. New York, N.Y.: New York State Unified Court System, September 25-27, 2002. <http://www.9-11summit.org/>

Disaster Recovery Journal <http://www.drj.com/>
- DRJ's Sample DR Plans and Outlines. Disaster Recovery Journal. <http://www.drj.com/new2dr/samples.htm>

Florida Business Disaster Survival Kit: Business Continuity Planning in Today's World. Tampa, Fla.: Tampa Bay Regional Planning Council, 2004. <http://www.tampabaydisaster.org/fldisasterkit/index.html>

Gordon, James A. Comprehensive Emergency Management for Local Governments: Demystifying Emergency Planning. Brookfield, Conn.: Rothstein Associates, Inc., 2002.

Journal of Homeland Security. <http://www.homelandsecurity.org/newjournal/default.asp>

Kemp, Roger L., ed. Homeland Security: Best Practices for Local Government. Washington, D.C.: International City/County Management Association, 2003.

NCSC's Best Practice Institute. Emergency Management for Courts. Williamsburg, Va.: National Center for State Courts, 2003. <http://www.ncsconline.org/WC/Publications/Comm_CtSecEMfCtsPub.pdf>

Siegel, Lawrence, Caroline S. Cooper, and Allison L. Hastings. Planning for Emergencies: Immediate Events and Their Aftermath: A Guideline for Local Courts. Washington, D.C.: Justice Programs Office, School of Public Affairs, American University, 2005. <http://spa.american.edu/justice/resources/SJI.pdf>

Wallace, Michael, 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: American Management Association, 2004.

Waugh, William L., Jr. Living With Hazards; Dealing With Disasters: An Introduction to Emergency Management. Armonk, N.Y. M.E. Sharpe, 2000.

"When Disaster Strikes, Will Your Court Be Ready?" Judges' Journal 37 no. 4 (1998). American Bar Association.

Recommended Organizations

American Red Cross, Disaster Services <http://www.redcross.org/services/disaster/0,1082,0_319_,00.html>

Bureau of Justice Assistance <http://www.ojp.usdoj.gov/BJA>

Department of Health and Human Services, Centers for Disease Control and Prevention <http://www.cdc.gov/>

Department of Homeland Security, Emergencies and Disasters<http://www.dhs.gov/dhspublic/theme_home2.jsp>

Disaster Center <http://www.disastercenter.com/>
- Disaster Center Bookstore <http://www.disastercenter.com/Rothstein/>

Emergency Management Accreditation Program <http://www.emaponline.org/>

Federal Emergency Management Association (FEMA) <http://www.fema.gov/index.shtm>

National Emergency Management Association <http://www.nemaweb.org/>

U.S. Department of Labor. Occupational Safety and Health Administration <http://www.osha.gov/>

I. Program Management

A. Federal and State Guidance

Printed Resources

Conference of Chief Justices and Conference of State Court Administrators. *Standard Operating Procedures*. Chapter 1, “10 Essential Elements for Courtroom Safety and Security Planning.” 2006.

Hastings, Allison L. Impact of 9/11 and Other Emergency Situations on Court Administration: Report of Survey of Local Trial Courts. Washington, D.C.: Justice Programs Office, School of Public Affairs, American University, 2003.

Mecham, Leonidas Ralph, Director, AOUSC. Emergency Preparedness in the Judiciary (Urgent Information). Memorandum to All Chief Judges. United States Courts. October 17, 2001.

NEMA Biennial Report: Organizations, Operations & Funding for State Emergency Management & Homeland Security. Lexington, Ky.: National Emergency Management Association, 2004.

Online Resources

Bea, Keith. Congressional Research Service. Order No. RL 33064. Organization and Mission of the Emergency Preparedness and Response Directorate: Issues and Option for the 109th Congress. September 7, 2005. <http://fpc.state.gov/documents/organization/53095.pdf>

Casey, Pamela. A National Strategic Plan for Judicial Branch Security. Washington, D.C.: Bureau of Justice Assistance, 2006. <http://solutions.ncsconline.org/Recommended_strategies_Appendices_Final_Report_2-7-061.pdf>

GAO Reports and Testimonies Related to Disaster Preparedness, Response and Reconstruction. <http://www.gao.gov/docsearch/featured/dprr.html>

Homeland Defense Equipment Reuse (HDER) Program. U.S. Department of Homeland Security, Preparedness Directorate, Offices of Grants and Training, 2006. <http://www.ojp.usdoj.gov/odp/equipment_hder.htm>

Memorandum to All Chief Judges, United States Courts, Subject: Anthrax Testing. Administrative Office of the United States Courts, November 9, 2001. <http://www.9-11summit.org/materials9-11/911/acrobat/26/C6NewThreats/ChiefJudgeMemoAnthraxTesting.pdf>

Morial, Marc H. et al. *A National Action Plan for Safety and Security in America’s Cities.* United States Conference of Mayors, December 2001. <http://www.usmayors.org/uscm/news/press_releases/documents/ActionPlan_121101.pdf>

National Fire Protection Association. *NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs.* 2004 Edition. Quincy, Mass.: NFPA, 2004. <http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf>

National Response Plan. Department of Homeland Security. December 2004. <http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0566.xml>

Public Assistance: Applicant Handbook. Washington, D.C.: Federal Emergency Management Agency, 1999. <http://www.fema.gov/pdf/government/grant/pa/apphndbk.pdf>

Public Assistance: Public Assistance Guide. Washington, D.C.: Federal Emergency Management Agency, 1999. <http://www.fema.gov/pdf/government/grant/pa/pagprnt_071905.pdf>

Review of the United States Marshals Service Judicial Security Process. United States Department of Justice, Office of the Inspector General, March 2004. <http://www.usdoj.gov/oig/reports/USMS/e0404/final.pdf>

State Homeland Security Contacts. Department of Homeland Security. <http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0291.xml>

State Offices and Agencies of Emergency Management. FEMA. <http://www.fema.gov/about/contact/statedr.shtm>

U.S. Government's Official Web Portal for Disasters and Emergencies. <http://www.firstgov.gov/Citizen/Topics/PublicSafety/Disasters.shtml>

U.S. Marshals Service, District Offices. <http://www.usmarshals.gov/district/index.html>

Wisconsin Courthouse Security Resource Center. The Wisconsin Sheriff's and Deputy Sheriff's Association, U.S. Marshal's Office of the Western District of Wisconsin, Director of State Courts, Office of the Chief Justice of the Wisconsin Supreme Court, Fox Valley Technical College, 2000. <http://www.9-11summit.org/materials9-11/911/acrobat/27/P3&C10EmergencyPreparednessPlans/Wisconsinexcerpt.pdf>

B. Internal Coordination

Printed Resources

Final Report for the Ohio Court Security Project: Report to the Ohio General Assembly. Williamsburg, Va.: National Center for State Courts, 2003.

Office of Court Security and Emergency Preparedness. *Preparing for the Unthinkable: A Report on the Arizona Judicial Council.* Phoenix, Ariz.: Arizona Supreme Court, 2003.

Online Resources

Cohen, Lawrence D., chair. *Court Security Manual.* State of Minnesota, Conference of Chief Judges. <http://www.9-11summit.org/materials9-11/911/acrobat/26/C6NewThreats/MinnesotaCtSecurityManual.pdf>

Emergency Order, Arizona Courts, Uncontrolled Forest Fires. June 2002. <http://www.9-11summit.org/materials9-11/911/acrobat/26/C1TheAftermath/ArizonaEmergencyOrdersJune2002.pdf>

Marks, Lawrence K. and Ronald P. Younkins, chairs. *Report to the Chief Judge and Chief Administrative Judge.* New York State Unified Court System, Task Force on Court Security, October 2005. <http://www.nycourts.gov/reports/security/SecurityTaskForce_Report.pdf>

Supreme Court of Florida. Administrative Order No. AOSC01-54. *In re: Work Group on Emergency Preparedness.* November 8, 2001. <http://www.floridasupremecourt.org/clerk/adminorders/2001/sc01-54.pdf>

C. External Coordination

FEMA's National Incident Management System. <http://www.fema.gov/emergency/nims/index.shtm>

Hazard Reduction and Recovery Center. Texas A&M University. <http://archone.tamu.edu/hrrc/>

Jones, Radford W. et al. *Critical Incident Protocol – A Public and Private Partnership*. East Lansing, Mich.: Michigan State University, School of Criminal Justice, 2000. <http://www.ojp.usdoj.gov/odp/docs/cip.pdf>

Natural Hazards Center. University of Colorado. <http://www.colorado.edu/hazards/>

Northeast Document Conservation Center (NEDCC). <http://www.nedcc.org/>

D. Multi-year Strategy

Continuity of Operations (COOP) Multi-Year Strategy and Program Management Plan Template Guide. Washington, D.C.: FEMA. <http://www.fema.gov/pdf/government/coop/MYSPMPTemplateGuide.pdf>

II. Prevention

A. Risk Management

Printed Resources

Azoulay, Ofer. "Proactive Security in the World of Terrorism." *Disaster Recovery Journal*. 19, no. 1 (Winter 2006): 18-22.

Building a Better Courthouse: Technology and Design in New Court Facilities: Participant Guide. Williamsburg, Va.: National Center for State Courts, Institute for Court Management, 2003.

Baehler, Aimee and Douglas K. Somerlot. *Developing and Evaluating Courthouse Security and Disaster Preparedness: A Collaborative Process between State and Federal Courts with Curriculum Materials*. Denver, Colo.: Justice Management Institute, 2005.

Calhoun, Frederick S., and Stephen W. Weston. *Defusing the Risk to Judicial Officials: The Contemporary Threat Management Process.* Alexandria, Va.: National Sheriff's Association, 2001.

Calhoun, Frederick S., with Stephen W. Weston. *Contemporary Threat Management: A Practical Guide for Identifying, Assessing, and Managing Individuals of Violent Intent.* San Diego: Calif.: Specialized Training Services, 2003.

Court Security and Disaster Planning. Williamsburg, Va.: National Center for State Courts, Institute for Court Management, 2003.

Drewes, Jeanne M. *Risk and Insurance Management Manual for Libraries.* Chicago: ALA, 2005.

Flango, Victor, and Don Hardenbergh, eds. *Courthouse Violence: Protecting the Judicial Workplace*. Thousand Oaks, Calif.: Sage Publications, 2001.

Gordon, James A. *Comprehensive Emergency Management for Local Governments: Demystifying Emergency Planning.* Brookfield, Conn.: Rothstein Associates, Inc., 2002.

Hardenbergh, Don, Robert Tobin, and Chang-Ming Yeh. *The Courthouse: A Planning and Design Guide for Court Facilities.* Williamsburg, Va.: National Center for State Courts, 1992.

Jones, Tony L. Court Security: *A Guide to Post 9-11 Environments*. Springfield, Ill.: Charles C. Thomas, Ltd., 2003.

Marcus W. Reinkensmeyer, et al. *Court Security Guide.* Williamsburg, Va.: National Association for Court Management, 2005.

Murer, Amanda. "Communication Is the Key in Court Security." *Report on Trends in the State Courts.* Williamsburg, Va.: National Center for State Courts, 2002.

National Summit on Court Safety and Security. Participant Notebook. 2005.

National Summit on Court Safety and Security: Follow-Up Meeting. 2005.

National Workshop on Improving Court Security. National Center for State Courts and the State Justice Institute. July 12, 2006.

Sikich, Geary W. "Sept. 11 Aftermath: Seven Things Your Organization Can Do Now." *Disaster Recovery Journal* 15, no. 1 (Winter 2002): 46.

Vossekuil, Bryan, Randy Borum, Robert Fein, and Marisa Reddy. “Preventing Targeted Violence Against Judicial Officials and Courts.” *The Annals of the American Academy of Political and Social Science* 576, no. 1 (2001).

Online Resources

Garvey, Martin J., and Marianne Kolbasuk McGee. “New Priorities: The Planning and Products Needed to Weather Disasters Are Taken More Seriously Today.” *Information Week.* 905 (September 9, 2002): 36-40. <http://www.informationweek.com/story/IWK20020906S0005>

Hardenbergh, Dan. “The Future of Court Security.” Future Trends in State Courts. Williamsburg, Va.: National Center for State Courts, 2004. <http://www.ncsconline.org/WC/Publications/Trends/CtSecuTrends2004.html>

National Oceanic and Atmospheric Administrator’s Emergency Management Weather Information Network. <http://www.nws.noaa.gov/emwin/index.htm>

Rubin, Claire. “Emergency Management in the 21st Century: Coping with Bill Gates, Osama bin-Laden, and Hurricane Mitch.” Working Paper #104. Boulder, Colo.: The Natural Hazards Center, 2000. <http://www.colorado.edu/hazards/wp/wp104/wp104.html>

Rubin, Claire. “Emergency Management in the 21st Century: Dealing with Al Qaeda, Tom Ridge, and Julie Gerberding.” Working Paper #108. Boulder, Colo.: The Natural Hazards Center, 2004. <http://www.colorado.edu/hazards/wp/wp108/wp108.pdf>

B. Vulnerability Assessment

Printed Resources

Dilley, Maxx, et al. *Natural Disaster Hotspots: A Global Risk Analysis.* Washington, D.C.: World Bank Publications, 2005.

Dilley, Maxx, et al. *Natural Disaster Hotspots Case Studies.* Washington, D.C.: World Bank Publications, 2006.

Hiles, Andrew. *Enterprise Risk Assessment and Business Impact Analysis.* Brookfield, Conn.: Rothstein Associates, Inc., 2002.

Janco Associates. *Threat and Vulnerability Assessment Tool.* Sarbanes Oxley Compliance Tool. 2006.

Jones, Edmond D. *Business Threat and Risk Assessment Checklist.* Brookfield, Conn.: Rothstein Associates, Inc., 2001.

Kirchner, Terri, and Kiran Karande. ”Measuring Perceived Business Continuity Readiness of an Organization.” *Disaster Recovery Journal* 18, no. 4 (Fall 2005): 24-30.

Landoll, Douglas J. *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*. Boca Raton, Fla.: Taylor and Francis Group, LLC, 2006.

Phelps, J.R. "Would You Be Prepared In the Event of a Disaster?" *Florida Bar Journal* 80, no. 5 (May 2006): 32.

Online Resources

Fein, Robert A. and Bryan Vossekuil. *Protective Intelligence and Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials.* Washington, D.C.: U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, 1998. <http://www.ncjrs.gov/pdffiles1/nij/179981.pdf>

C. Security Awareness Training

Printed Resources

Court Security Manual. State of Minnesota, Conference of Chief Judges, 1999.

Gray, Cynthia. *Security Ideas for Judges, Spouses, and Families: An Ethics Guide for Judges and Their Families*. Chicago: American Judicature Society, 2001.

Holiman, Marsha. *Security for Personnel in Rural Courts.* Phase III Paper, Court Executive Development Program, Institute for Court Management. Williamsburg, Va.: National Center for State Courts, 2001.

Petersen, William H., and Barbara E. Smith. *Court Security: Training Guidelines and Curricula.* Alexandria, Va.: National Sheriff's Association, 1991.

Reinhart, Christopher. *Court Security Personnel.* OLR Research Report 2000 R 0794. Hartford, Conn.: Connecticut General Assembly, Office of Legislative Research, 2000.

Vulnerability Assessment Methodology Report. Washington, D.C.: Department of Homeland Security, Office for Domestic Preparedness, July 2003.

Wehenkel, Candy. "Business Continuity and Training for All Levels of an Organization." *Disaster Recovery Journal* 19, no. 1 (Winter 2006): 76-77.

Online Resources

Fautsko, Timothy. "Court Security: Are Courts Really Secure?" Annual Report on Trends in the State Courts. Williamsburg, Va.: National Center for State Courts, 2001. <http://www.ncsconline.org/WC/Publications/KIS_CtFutu_Trends01_Pub.pdf>

III. Preparedness

A. COOP Plan (includes Pandemic Annex)

Printed Resources

Alvord, Chris. “Web-Based BCP Software-as-Service.” *Disaster Recovery Journal*. 19, no. 1 (Winter 2006): 34-38.

Anderson, Neal. “Keeping Paper Trail Intact After Disaster Strikes.” *Disaster Recovery Journal* 15, no. 1 (Winter 2002): 32.

Bell, Judy Kay. *Disaster Survival Planning: A Practical Guide for Businesses.* Rev. ed. Port Hueneme, Calif.: Disaster Survival Planning.

Bernardino, Arthur J., Jr., et al. *Business Continuity Management Mini Guide*. Williamsburg, Va.: National Association for Court Management, 2006.

Braverman, Mark. “Planning for Human Continuity.” *Disaster Recovery Journal* 19, no. 3 (Summer 2006): 36-42.

Disaster Recovery Journal, Summer 2006, Volume 19, Number 3.

DiMartini, Bill. “Establishing a Corporate Business Continuity Program and Continuity Program Office.” *Disaster Recovery Journal* 19, no. 3 (Summer 2006): 62-67.

Elliot, Dominic, Ethné Swartz, and Brahim Herbane. *Business Continuity Management: A Crisis Management Approach.* New York: Routledge, 2001.

Fulmer, Kenneth. *Business Continuity Planning: A Step-by-Step Guide With Planning Forms on CD-ROM.* Brookfield, Conn.: Rothstein Associates, Inc., 2005.

Girard, John. *Disaster Management Plan for Remote Access.* Tactical Guidelines, TG-14-5458. Research Note. Stamford, Conn.: Gartner, Inc., 2001.

Glenn, John. “What is Business Continuity Planning? How Does It Differ from Disaster Recovery Planning?” *Disaster Recovery Journal* 15, no. 1 (Winter 2002): 75-76.

Graham, Julia, and David Kane. *A Risk Management Approach to Business Continuity: Aligning Business Continuity with Corporate Governance.* Brookfield, Conn.: Rothstein Associates, Inc., 2006.

Greb, David. “Ten ‘Suggested’ Commandments of Business Continuity Planning” *Disaster Recovery Journal* 14, no. 1 (Winter 2001): 32-34.

Gustin, Joseph F. *Disaster & Recovery Planning: A Guide for Facility Managers.* 2nd ed. Lilburn, Ga.: Fairmont Press, 2002.

Huff, George B., Jr. “Emergency Preparedness, Continuity Planning, and the Federal Judiciary.” *Judges Journal* 45, no. 6 (Winter, 2006).

Kalt, Hank. “Preparing for an Influenza Pandemic.” *Disaster Recovery Journal* 19, no. 3 (Summer 2006): 18-22.

Koch, Richard. “Business Continuity Best Practices.” *Disaster Recovery Journal* 14, no. 1 (Winter 2001): 58-61.

Laye, John. *Avoiding Disaster: How to Keep Your Business Going When Disaster Strikes.* New York: John Wiley & Sons, Inc., 2002.

Luevano, Fred. *How E-Business is Changing Business Continuity Programs.* Best Practices & Case Studies, Note QA-13-8626. Stamford, Conn.: Gartner, Inc., 2001.

Marcella, Albert J. and Carol Stucki. *Business Continuity, Disaster Recovery, and Incident Management Planning: A Resource for Ensuring Ongoing Enterprise Operations.* Altamonte Springs, Fla.: Institute of Internal Auditors Research Foundation, 2004.

Mitome,Yuko, Karen D. Speer, and Billie Swift. “Embracing Disaster with Contingency Planning: Contingency Planning Allows a Business to Continue with its Most Important Operations in Spite of an Event, Such as an Earthquake, That Makes Business as Usual Impossible. 48 *Risk Management* 18 (May 2001).

Noakes-Frye, Kristen, and Trude Diamond. *Business Continuity and Disaster Recovery Planning and Management: Perspective.* Technology Overview, DPRO-100862. Stamford, Conn.: Gartner, Inc., 2001.

Planning for Disaster. Mechanicsburg, Pa.: Pennsylvania Bar Institute, 2002.

Power Outage Emergency Plan: Continue Operations to Public. Superior Court of California, County of Sacramento, Carol Miller Justice Center. Revised 07/01/02.

Redmond, Michael C. and James Hammill. “The Challenge of Getting Back to Business: Business Recovery Checklist.” *Disaster Recovery Journal* 15, no. 1 (Winter 2002): 92.

Silcox, Sarah. “HR and Business Continuity: Planning for Disaster.” *IRS Employment Review* 45, no. 1 (Winter 2006): 6.

Sullivan, Sandra. “How to Work When the Workplace is Not Available. *Disaster Recovery Journal 15, no. 4 (Fall 2002): 46.*

Trends in Business Continuity and Risk Management: Business Continuity Survey. Bedford, Mass.: Envoy Worldwide Survey, 2005.

Wallace, Michael, 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: American Management Association, 2004.

Witty, Roberta. *Integrating BCP Into the IT Project Life Cycle.* Tutorials, TU-13-8386. Research Note. Stamford, Conn.: Gartner, Inc., 2001.

Online Resources

Contingency Plan: COOP Self-Assessment Guide & Checklist. Nine-eleven Summit (courts in the aftermath of September 11th). New York: 2002. <http://www.9-11summit.org/materials911/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/SelfAssessGuideChecklist.pdf>

COOP Planning in California Courts. Judicial Branch of California. <http://www.courtinfo.ca.gov/reference/rfp/disaster.htm>

COOP Plan Template Instructions. Washington, D.C.: Federal Emergency Management Association. <http://www.fema.gov/doc/government/coop/coop_plan_template_instructions.doc>

Disaster Recovery and Business Continuity Planning Audit. San Marcos, Tex.: Southwest Texas State University, Internal Audit and Advisory Services, 2003. <http://www.txstate.edu/audit_compliance/050203-disasterrecbizcont030717.pdf>

Disaster Recovery Planning for Courts: A Guide to Business Continuity Planning. Williamsburg, Va.: National Association for Court Management, 2000. <http://contentdm.ncsconline.org/cgi-bin/showfile.exe?CISOROOT=/facilities&CISOPTR=0>

Emergency Preparedness. Florida State Courts, Court Programs and Initiatives. <http://www.flcourts.org/gen_public/emergency/index.shtml>

“Emergency Preparedness in the Judiciary.” *The Third Branch* 33, no. 11 (November 2001): 1, 3, and 12. <http://www.uscourts.gov/ttb/nov01ttb/emergency.html>

Emergency Preparedness for Business: Business Emergency Management Planning. Centers for Disease Control and Prevention, National Institute for Occupational Safety and Health. <http://www.cdc.gov/niosh/topics/prepared/>

Emergency Preparedness Process Flowchart. <http://www.9-11summit.org/materials9-11/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/EmergencyPreparednessProcessFlowchart.pdf>

Emergency Preparedness Templates. Florida State Courts. <http://www.flcourts.org/gen_public/emergency/templates.shtml>

Federal Preparedness Circular. Washington, D.C.: FEMA, Directives Management System, 2004. <http://www.fema.gov/pdf/library/fpc65_0604.pdf>

FEMA. *Continuity of Operations (COOP) Programs.* <http://www.fema.gov/government/coop/index.shtm>

Florida State Courts. *Strategy for Pandemic Influenza: Keeping the Courts Open in a Pandemic*. Unified Supreme Court, Court Emergency Management Group, March 29, 2006. <http://www.ncsconline.org/WC/Publications/KIS_CtSecuPanFlu_Strategy.pdf>

Florida Supreme Court Workgroup on Emergency Preparedness. *Keep the Courts Open: Final Report*. 2002. <http://www.9-11summit.org/materials9-11/911/acrobat/27/P3&C10EmergencyPreparednessPlans/FloridaFinalReport.pdf>

New York State Unified Court System. *Emergency Preparedness and Response Planning Manual*. March 2003. <http://www.9-11summit.org/materials9-11/911/acrobat/26/manual1.pdf>

New York State Unified Court System. *Facility Emergency Preparedness and Response Plan Template*. March 2003. <http://www.9-11summit.org/materials9-11/911/acrobat/26/template.pdf>

Open for Business: A Disaster Planning Toolkit for the Small to Mid-Sized Business Owner. Institute for Business and Home Safety, 2005. <http://www.nationwide.com/documents/OpenForBusiness.pdf?WT.svl=disaster_planning_toolkit>

Petersen, R. Eric. Congressional Research Service. Order No. RL 31978. *Emergency Preparedness and Continuity of Operations (COOP) Planning in the Federal Judiciary*. September 8, 2005. <http://www.fas.org/sgp/crs/secrecy/RL31978.pdf>

Pandemic Influenza Planning

On-line resources

Centers for Disease Control and Prevention. <www.cdc.gov/flu/avian>

Department of Health and Human Services. <www.pandemicflu.gov>

World Health Organization Epidemic and Pandemic Alert and Response (EPR). <http://www.who.int/csr/disease/avian_influenza/en/index.html>

B. Evacuation Plan (Includes Shelter-in-Place)

Printed Resources

Sammon, Mary T. *Akron Municipal Court: Security Policy and Procedure Plan*. Phase III Paper, Court Executive Development Program, Institute for Court Management. Williamsburg, Va.: National Center for State Courts, 1999.

Emergency Evacuation Video: What Every Employee Should Know.. VHS/DVD. National Fire Protection Association, 2004.

Online Resources

Bea, Keith. *Disaster Evacuation and Displacement Policy: Issues for Congress*. CRS Report for Congress, Order No. RS 22235, September 2, 2005. <http://www.fas.org/sgp/crs/misc/RS22235.pdf>

Department of Homeland Security, Ready Business. *Make an Evaluation Plan*. 2006. <http://www.ready.gov/business/plan/evacplan.html>

Department of Homeland Security, Ready Business. *Make a Shelter-In-Place Plan.* 2006. <http://www.ready.gov/business/plan/shelterplan.html>

Emergency Preparedness Plan. City of New Orleans, 2006. <http://www.cityofno.com/Portals/Portal46/portal.aspx?portal=46&tabid=38>

Evacuation Plans and Procedures eTool: Shelter-in-place. U.S. Department of Labor: Occupational Safety and Health Administration. http://www.osha.gov/SLTC/etools/evacuation/shelterinplace.html

Occupant Emergency Plan: Federal Building and U.S. Courthouse: Tyler, Texas. October 2001. <http://www.9-11summit.org/materials9-11/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/OccupantEmergencyPlanTexas.pdf>

Occupant Emergency Program Guide. U.S. General Services Administration Public Buildings Service, Federal Protective Service, March 2002. <http://www.9-11summit.org/materials9-11/911/acrobat/27/P3%26C10EmergencyPreparednessPlans/GSAOccupantEmergencyProgram.pdf>

Shelter-in-Place in an Emergency. American Red Cross. February 2003. <http://www.redcross.org/services/disaster/beprepared/shelterinplace.html>

Your Evacuation Plan. American Red Cross.
<http://www.redcross.org/services/disaster/beprepared/evacuation.html>

C. Disaster Recovery (IT) Plan

Printed Resources

Baehler, Aimee and Douglas K. Somerlot. *Developing and Evaluating Courthouse Security and Disaster Preparedness: A Collaborative Process between State and Federal Courts with Curriculum Materials*. Denver, Colo.: Justice Management Institute, 2005.

D'Arcy, Paul. "Building an Effective Communications Infrastructure." *Disaster Recovery Journal* 29, no. 2 (Spring 2006): 46-48.

Diamond, Cindy. "Disaster Planning for Data Security." *Practice Innovations* 3, no. 1 (March 2002): 6-7.

Disaster Prevention and Recovery Plan for Indiana Trial Courts and Clerks. Indianapolis, Ind.: Indiana Supreme Court, Division of State Court Administration, Information Management Section, 1993.

Guendert, Steve and Rick Boyd. ”FICON and Mainframe Disaster Recovery Insourcing” *Disaster Recovery Journal* 19, no. 1 (Winter 2006): 81-82.

Hiatt, Charlotte J. *A Primer for Disaster Recovery Planning for an IT Environment*. Hersey, Pa.: Idea Group Publishers, 2000.

Kellogg, Sarah. “Disaster Recovery: Hoping for the Best, Planning for the Worst.” *Washington Lawyer: The Official Journal of the District of Columbia Bar* 20, no. 11 (July/August 2006) 22-28.

Lowell, Howard P. “Protecting Court Records: Disaster Preparedness for Court Managers.” *Court Manager* 8, no. 1 (1993): 5

Mingay, Simon. *Sourcing Recovery and Continuity Services.* Decision Framework, DF-13-5293. Research Note. Stamford, Conn.: Gartner, Inc., 2001.

Perrotta, Tom. “Courts Go Wireless to Restore Networks.” *New York Law Journal.*

Witty, Roberta, and Donna Scott. *Disaster Recovery Plans and Systems are Essential.* Gartner FirstTake, FT-14-5021. Stamford, Conn.: Gartner, Inc., 2001.

Online Resources

Conservation Online: Resources for Conservation Professionals. Stanford University Libraries, 1994. <http://palimpsest.stanford.edu/>

Farrell, Kathleen. *Safeguarding Court Records: Paper, Microfiche, and Automated Data*. United States Bankruptcy Court, Southern District of New York. <http://www.9-11summit.org/materials9-1/911/acrobat/26/C4SafeguardingCourtRecords/VitalRecords.pdf>

IBM Business Continuity and Recovery Consulting. *Disaster Recovery Plan for Central Technical Center*. May 23, 2003. <http://www.ncsconline.org/WC/Publications/KIS_BusDisCTCDisasterRecoveryPub.pdf>

IT Disaster Recovery Plan NIST 800-34. <http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>

Library Disaster Preparedness and Recovery Plan. University of Virginia Library, 2005. <http://www.lib.virginia.edu/preservation/docs/disaster/index.html>

National Center for State Courts, News Alert. *Do You Have a Disaster Recovery Plan?* 2005. <http://www.ncsconline.org/What'sNew/NewsAlerts/NewsAlertHaveRecoveryPlan.html>

Swanson, Marianne, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, and Ray Thomas. *Contingency Planning Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology*. U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2002. <http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>

D. Other Plans

Printed Resources

Blythe, Bruce T. *Blindsided: A Manager's Guide to Catastrophic Incidents in the Workplace.* New York: Portfolio Hardcover, 2002.

Chase, Dawn. "Preparing Your Office for a Scare Over Anthrax." *Virginia Lawyers Weekly* 36 (October 22, 2001): 1, 17.

De Winne, Joan. "Preparing for Major Incidents." *Forensic Science International* 159, no. 1 (May 15, 2006): S9.

Disaster Prevention and Recovery Plan for Indiana Trial Courts and Clerks. Indianapolis: Indiana Supreme Court, 1993.

Freedman, Ellen. "Preparing for and Recovering from…Disaster." *The Pennsylvania Lawyer* 28, no. 1 (January/February 2006): 44-48.

Gostin, Lawrence O., et al. "The Model State Emergency Health Powers Act: Planning for and Response to Bioterrorism and Naturally Occurring Infectious Diseases." *Journal of the American Medical Association* 288, no. 5 (August 7, 2002): 622-628.

Halsted, Deborah D, Richard P. Jasper, and Felicia M. Little. *Disaster Planning: A How-to-Do-It Manual for Librarians and Archivists.* New York: Neal-Schuman Publishers, Inc., 2005.

Hunter, Ian, and Jeremy Nixon. "Bird Flu – Why Employers Should Get Their Ducks In a Row." *New Law Journal* 155, no. 7203 (December 2, 2005):1833.

Kahn, Miriam. *Disaster Response and Planning for Libraries*, 2nd ed. Chicago: ALA, 2003.

Moed, Edward. "A Crisis Plan is a 'Must Have' for Every Company." *Disaster Recovery Journal* 15, no. 4 (Fall 2002): 25.

Morello, Dian Tunick. *Anticipate Diverse Emotional Reactions in Wake of Attacks.* Strategy & Tactics/Trends & Directions, Note COM-14-5350. Stamford, Conn.: Gartner, Inc., 2001.

National Organization on Disability. *Emergency Preparedness Initiative: Guide on the Special Needs of People with Disabilities for Emergency Managers, Planners, and Responders.* Washington, D.C.: National Organization on Disability, 2002.

National Strategy for Pandemic Influenza: Implementation Plan. Homeland Security Council, May 2006.

Wellheiser, Johanna G. and Jude Scott. *An Ounce of Prevention: A Handbook on Disaster Contingency Planning for Archives, Libraries, and Record Centres*, 2nd ed. Lanham, Md.: The Scarecrow Press, Inc., 2002.

Online Resources

Chemical Hazard Information: Federal Reading Room Appointment Line. Department of Justice, Criminal Division, February 20, 2001. <http://www.usdoj.gov/criminal/tvcs/chemical_hazard.htm>

Emergency Preparedness and Response Planning Manual. New York Unified Court System, 2003. <http://www.9-11summit.org/materials9-11/911/acrobat/26/manual1.pdf>

Gibb, John R. *Empire County Comprehensive Emergency Management Plan*. State Emergency Management Office. 2004. <http://www.semo.state.ny.us/uploads/Empire%20County%20CEMP%202004%20gibb.pdf>

Guidance for Protecting Building Environments from Airborne Chemical, Biological, or Radiological Attacks. Department of Health and Human Services, Center for Disease Control and Prevention, May 2002. <http://www.cdc.gov/niosh/bldvent/pdfs/2002-139.pdf>

Michigan Supreme Court, State Court Administrative Office. *Michigan Court Security Manual*. Lansing, Mich.: 2002. <http://www.courts.michigan.gov/SCAO/resources/publications/manuals/security/MICourtSecurityManual.pdf>

Schofield, Amy R. and Linda L. Chezem. *Public Health Law Bench Book for Indiana Courts.* Louisville, Ky.: University of Louisville, Center for Public Health Law Partnerships, 2005. <http://www.publichealthlaw.info/INBenchBook.pdf>

Siegel, Lawrence, Caroline S. Cooper, and Allison L. Hastings. *Planning for Emergencies: Immediate Events and Their Aftermath: A Guideline for Local Courts.* Washington, D.C.: Justice Programs Office, School of Public Affairs, American University, 2005. <http://spa.american.edu/justice/resources/SJI.pdf>

IV. Response

Activation of Preparedness Plan

Printed Resources

Buntin, John. "Disaster Master." *Governing* 15, no. 3 (December 2001): 34-37.

Genovese, Robert. *Disaster Preparedness Manual.* 2006 Revision. Buffalo, N.Y.: William S. Hein & Co., Inc., 2006.

Graham, David B., and Thomas D. Johns. “Emergency Response Planning: A Critical Investment.” *Natural Resources & Environment* 20, no. 4 (Spring 2006): 49.

Lippman, Jonathan. “September 11th: The New York Experience.” Conference of State Court Administrators, midyear meeting, November 30, 2001.

Maggio, Mark. “September 11th and the Crisis Response for the Federal Courts.” *Federal Probation* 66, no. 1 (June 2002): 11-15.

Shahidi, Celeste *Disaster Planning Response and Recovery for Federal Courts.* Phase III Paper, Court Executive Development Program, Institute for Court Management. Williamsburg, Va.: National Center for State Courts, 1996.

World Health Organization. *SARS: How a Global Epidemic Was Stopped.* WHO Regional Office for the Western Pacific, May 2006.

Online Resources

American Bar Association Task Force on Emergency Management and Homeland Security. Ernest B. Abbott, Chair. *Draft Checklist for State and Local Government Attorneys to Prepare for Possible Disasters*. ABA, 2003. <http://www.abanet.org/statelocal/disaster.pdf>

American Red Cross Emergency Preparedness Kits. American Red Cross, 2006. <http://www.redcross.org/services/disaster/0,1082,0_217_,00.html>

Bomb Threat Checklist. State of Tennessee: Office of Homeland Security. http://www.state.tn.us/homelandsecurity/bomb_checklist.pdf

Bomb Threat Checklist. Washington, D.C.: General Services Administration. <http://www.gsa.gov/Portal/gsa/ep/formslibrary.do?viewType=DETAIL&formId=2847FBCF6DBB682285256A730010BD43>

Disaster Supplies Kit. American Red Cross. <http://www.redcross.org/services/disaster/0,1082,0_3_,00.html>

Chemical/Biological Threat Checklist. Washington, D.C.: General Services Administration. >http://www.9-11summit.org/materials9-11/911/acrobat/27/P3&C10EmergencyPreparednessPlans/GSAChembioCheckList.pdf>

Davis, Tom, chair. *Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina.* Washington, D.C.: U.S. Government Printing Office, 2006. <http://www.gpoaccess.gov/katrinareport/mainreport.pdf>

Emergency/Disaster Training Manual for Volunteer Lawyers Following Hurricane Katrina. New Orleans: Louisiana State Bar Association, 2005. <http://www.lsba.org/home1/trainingmanual.asp#Relief>

Fact Sheet: Community Emergency Response Team (CERT) Program. Department of Homeland Security. May 29, 2003. < http://www.dhs.gov/dhspublic/display?theme=15&content=835>

Federal Response to Hurricane Katrina: Lessons Learned. February 2006. <http://www.whitehouse.gov/reports/katrina-lessons-learned.pdf>

Root, Oren. *The Administration of Justice under Emergency Conditions: Lessons Following the Attack on the World Trade Center*. New York: Vera Institute of Justice, 2002. <http://www.vera.org/publication_pdf/148_188.pdf>

U.S. Senate Committee on Homeland Security and Governmental Affairs. *Hearing on Hurricane Katrina: What Can Government Learn from the Private Sector's Response?* 109th Cong., November 16, 2005. <http://hsgac.senate.gov/index.cfm?Fuseaction=Hearings.Detail&HearingID=296>

V. Recovery

Activities to return conditions to pre-event level

Printed Resources

Alire, Camila, ed. *Library Disaster Planning and Recovery Handbook*. New York: Neal-Schuman Publishers, Inc., 2000.

Anderson, Neal. “Keeping the Paper Trail Intact after Disaster Strikes.” *Disaster Recovery Journal* 15, no. 1 (Winter 2002): 32.

Brashier, Greg. ”When Disaster Strikes: Recovering your phone system keeps your business and your customers connected when the inevitable occurs.” *Disaster Recovery Journal* 19, no. 1 (Winter 2006): 48-54.

Cedar County Clerk of Court Disaster and Response Recovery Plan. Cedar County, Iowa: Cedar County Clerk of Court, 2002.

D’Arcy, Paul. “Building an Effective Communications Infrastructure.” *Disaster Recovery Journal* 29, no. 2 (Spring 2006): 46-48.

Diamond, Cindy. “Disaster Planning for Data Security.” *Practice Innovations* 3, no. 1 (March 2002): 6-7.

Disaster Prevention and Recovery Plan for Indiana Trial Courts and Clerks. Indianapolis, Ind.: Indiana Supreme Court, Division of State Court Administration, Information Management Section, 1993.

Disaster Recovery Yellow Pages. Newton, Mass.: Systems Audit Group, Inc., 2003. (Order on-line at: <http://www.disaster-help.com/index.htm>)

Genovese, Robert. *Disaster Preparedness Manual.* 2006 Revision. Buffalo, N.Y.: William S. Hein & Co., Inc., 2006.

Green, Nancy. "Life After Death: Individual and Organizational Recovery from Crisis. *Disaster Recovery Journal* 15, no. 4 (Fall 2002): 18.Guendert, Steve and Rick Boyd. "FICON and Mainframe Disaster Recovery Insourcing" *Disaster Recovery Journal* 19, no. 1 (Winter 2006): 81-82.

Hiatt, Charlotte J. *A Primer for Disaster Recovery Planning for an IT Environment*. Hershey, Pa.: Idea Group Publishers, 2000.

Lowell, Howard P. "Protecting Court Records: Disaster Preparedness for Court Managers." *Court Manager* 8, no. 1 (1993): 5.

Moskal, Edward. "Business Continuity Management: Post 9/11 Disaster Recovery Methodology." *Disaster Recovery Journal* 19, no. 2 (Spring 2006): 56-62.

Myers, David. "Communications For When Your Business Needs It Most." *Disaster Recovery Journal* 19, no. 1 (Winter 2006): 60-62.

Shahidi, Celeste *Disaster Planning Response and Recovery for Federal Courts.* Phase III Paper, Court Executive Development Program, Institute for Court Management. Williamsburg, Va.: National Center for State Courts, 1996.

Ulicki, Mike. "Beyond Data Backup: Contingency Workspace." *Disaster Recovery Journal* 19, no. 1 (Winter 2006): 56-58.

Wise, Daniel. "Courts Struggle to Deal with Disaster's Impact" *New York Law Journal*. September 13, 2001.

Witty, Roberta, and Donna Scott. *Disaster Recovery Plans and Systems are Essential.* Gartner FirstTake, FT-14-5021. Stamford, Conn.: Gartner, Inc., 2001.

Online Resources

Conservation Online: Resources for Conservation Professionals. Stanford University Libraries, 1994. <http://palimpsest.stanford.edu/>

Farrell, Kathleen. Safeguarding Court Records: Paper, Microfiche, and Automated Data. United States Bankruptcy Court, Southern District of New York. <http://www.9-11summit.org/materials9-1/911/acrobat/26/C4SafeguardingCourtRecords/VitalRecords.pdf>

IBM Business Continuity and Recovery Consulting. *Disaster Recovery Plan for Central Technical Center*. May 23, 2003. <http://www.ncsconline.org/WC/Publications/KIS_BusDisCTCDisasterRecoveryPub.pdf>

Kaye, Judith S. "Coping with Disaster. *Judges' Journal* 40, no. 4 (Fall 2001): 43-44. <http://www.abanet.org/justicecenter/katrina/pdf/coping.pdf>

National Center for State Courts, News Alert. *Do You Have a Disaster Recovery Plan?* 2005. <http://www.ncsconline.org/What'sNew/NewsAlerts/NewsAlertHaveRecoveryPlan.html>

Swanson, Marianne, Amy Wohl, Lucinda Pope, Tim Grance, Joan Hash, and Ray Thomas. *Contingency Planning Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology*. U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2002. <http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf>

VI. Training

Printed Resources

Rothstein, Philip Jan, ed. *Disaster Recovery Testing: Exercising Your Contingency Plan*. Rothstein Associates, Inc., 1994.

Swift, Kate Marquess. “Crisis Stage: Mock Disasters Teach Lessons Needed When Real Tragedy Strikes.” *ABA Journal* 90 (January 2004): 75.

Online Resources

Counter-Terrorism: Training and Resources for Law Enforcement. <http://www.counterterrorismtraining.gov/mission/index.html>

Department of Homeland Security. Office of Grants and Training. <http://www.ojp.usdoj.gov/odp/>

Emergency Management Institute, FEMA. <http://training.fema.gov/emiweb/edu/>

FEMA’s Emergency Management Institute. *Training and Education.* <http://training.fema.gov/>

FEMA. *Emergency Management Training for Government and Emergency Personnel*. <http://www.fema.gov/about/training/emergency.shtm>

Homeland Security Exercise and Evaluation Program. <http://www.ojp.usdoj.gov/odp/docs/hseep.htm>

Natural Hazards Center. *Upcoming Conferences and Meetings Dealing with Hazards and Disasters.* <http://www.colorado.edu/hazards/conf.html>