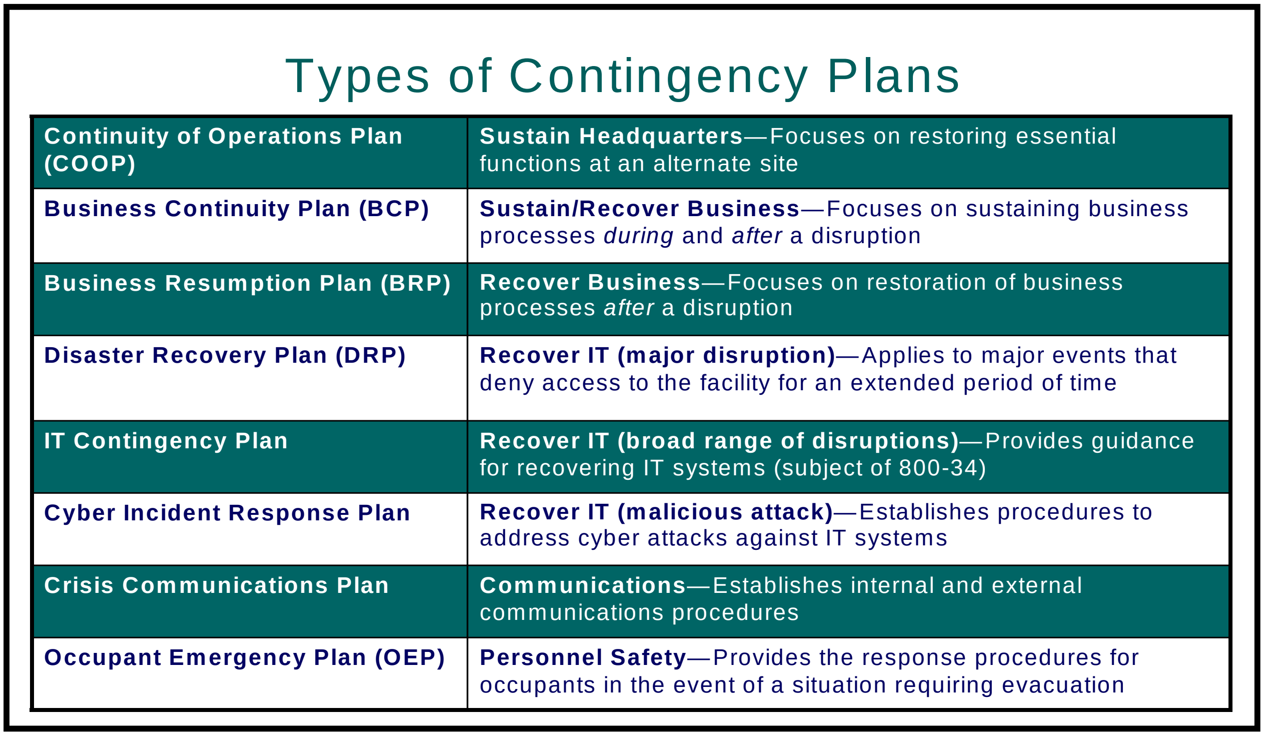
CHAPTER 14, PART 1
DISASTER RECOVERY AND BUSINESS RESUMPTION PLANS

1 BACKGROUND

The mission of the Office of the Chief Information Officer (OCIO) is to strategically acquire and use information and technology resources to improve the quality, timeliness, and cost effectiveness of USDA service delivery to its customers. The rapid pace of technological change and the way business is conducted has necessitated that USDA's major systems, which support the day-to-day core business processes, are able to function in emergencies or disasters. Most IT systems are vulnerable to many types of disruptions such as power outages, water damage, fire and viruses. These vulnerabilities are managed through risk assessments and appropriate security controls. Risk results from a variety of factors but are typically labeled as:

- Natural - hurricane, tornado, flood, fire
- Human - sabotage, virus, operator error
- Environmental - equipment failure, outage, electric power failure

Implementation of IT Contingency Plans is critical in ensuring that USDA business will continue at an acceptable level in the face of a major incident or disaster. An organization would use the suite of plans in figures 1 & 2 to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's IT systems, business processes, and the facilities. This type of planning is part of a larger process to ensure information survivability of data. Survivability implies that the data and process can be recovered regardless of the disaster or emergency.



Types of Contingency Plans

Continuity of Operations Plan (COOP)	**Sustain Headquarters**—Focuses on restoring essential functions at an alternate site
Business Continuity Plan (BCP)	**Sustain/Recover Business**—Focuses on sustaining business processes *during* and *after* a disruption
Business Resumption Plan (BRP)	**Recover Business**—Focuses on restoration of business processes *after* a disruption
Disaster Recovery Plan (DRP)	**Recover IT (major disruption)**—Applies to major events that deny access to the facility for an extended period of time
IT Contingency Plan	**Recover IT (broad range of disruptions)**—Provides guidance for recovering IT systems (subject of 800-34)
Cyber Incident Response Plan	**Recover IT (malicious attack)**—Establishes procedures to address cyber attacks against IT systems
Crisis Communications Plan	**Communications**—Establishes internal and external communications procedures
Occupant Emergency Plan (OEP)	**Personnel Safety**—Provides the response procedures for occupants in the event of a situation requiring evacuation

Figure 1, IT Contingency Plans

Plan Definitions

Continuity of Operations Plan - COOP focuses on restoring an organization's (usually a headquarters element) essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. Because a COOP addresses headquarters-level issues, it is developed and executed independently from the BCP. Presidential Decision Directive (PDD) 67 mandates implementation of a viable COOP capability. Minor disruptions that do not require relocation to an alternate site are typically not addressed; however, the COOP may include the BCP, DRP and BRP as appendices. The Continuity of Operations (COOP) Planning Staff (CPS), under the Assistant Secretary for Administration, Office of Procurement and Property Management, serves as USDA's focal point for continuity of operations (COOP) and continuity of government (COG) program.

Business Continuity Plan (BCP): The BCP focuses on sustaining an organization's business functions during and after a disruption. An example of a business function may be a payroll or consumer information process. A BCP may be written for a specific business process or may address all key business processes. Information technology (IT) systems are considered in the BCP in terms of support to the business processes. In some cases, the BCP may not address long-term recovery of processes and return to normal operations, solely covering interim business continuity requirements. A disaster recovery plan, business resumption plan, and occupant emergency plan may be appended to the BCP. Responsibilities and priorities set in the BCP should be coordinated with those in Continuity of Operations to eliminate possible conflicts.

<u>Business Resumption Plan</u> – The BRP addresses the restoration of business processes after an emergency, but unlike the BCP, lacks procedures to ensure continuity of critical processes throughout an emergency or disruption. Development of the BRP should be coordinated with DRP and BCP. This plan may be appended to the BCP.

<u>Disaster Recovery Plan (DRP)</u> - This plan applies to major, usually catastrophic, events that deny access to the normal facility for an extended period. Frequently, DRP refers to an IT-focused plan designed to restore operability of the target system, application, or computer facility an alternate site after an emergency. The DRP scope may overlap that of an IT contingency plan; however, the DRP is narrower in scope and does not address minor disruptions that do not require relocation. Dependent on the agency's needs, several DRPs may be appended to the BCP.

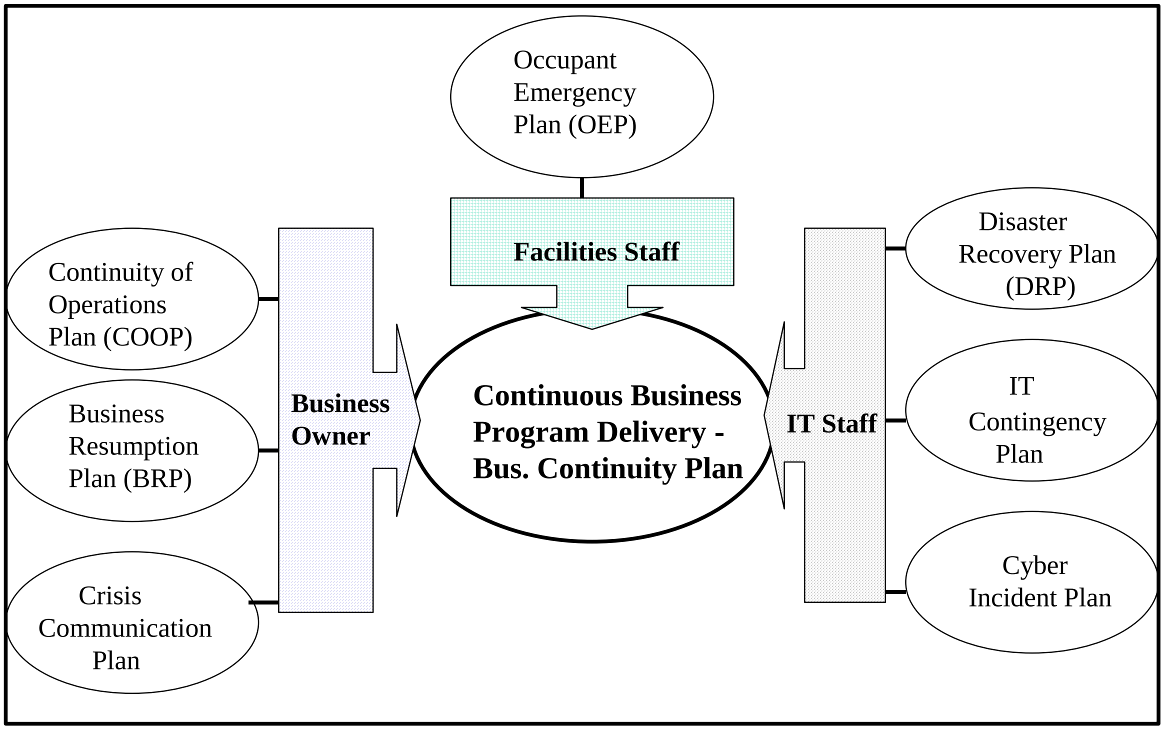
<u>IT Contingency Plan</u> (<u>Continuity of Support Plan)</u>– A set of advance arrangements and established procedures that provide guidance to enable an organization to recover mission critical IT services at a "local" or alternative site" following a "minor" or "major" disruptive event. Plan duration is for short or long term effects. OMB Circular A-130 requires the development and maintenance of continuity of support plans for general support systems and contingency plans for major applications. This planning guide considers continuity of support planning to be synonymous with IT contingency planning. Because an IT contingency plan should be developed for each major application and general support system, multiple contingency plans may be maintained with the agency or mission area BCP.

<u>Cyber Incident Response Plan</u> – This plan establishes procedures to address cyber attacks against an agency IT system(s). These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware, software, or data (e.g., a virus, worm, or Trojan horse).

Crisis Communications Plan - Organizations should prepare their internal and external communications procedures prior to a disaster. A crisis communications plan is often developed by the organization responsible for public outreach. The crisis communication plan procedures should be coordinated with all other plans to ensure that only approved statements are released to the public. Plan procedures should be included as an appendix to the BCP. The communications plan typically designates specific individuals as the *only* authority for answering questions from the public regarding disaster response. It may also include procedures for disseminating status reports to personnel and to the public. Templates for press releases are included in the plan.

Occupant Emergency Plan – This plan provides the response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property. Such events would include a fire, hurricane, criminal attack, or a medical emergency. OEPs are developed at the facility level, specific to the geographic location and structural design of the building. General Services Administration (GSA) owned facilities maintain plans based on the GSA OEP template. The facility OEP may be appended to the BCP, but is executed separately.

FIGURE 2, PLAN RELATIONSHIPS


Occupant Emergency Plan (OEP)
Facilities Staff
Continuity of Operations Plan (COOP)
Business Resumption Plan (BRP)
Crisis Communication Plan
Business Owner
Continuous Business Program Delivery - Bus. Continuity Plan
IT Staff
Disaster Recovery Plan (DRP)
IT Contingency Plan
Cyber Incident Plan

IT Contingency Planning Program Interrelationships

IT Contingency Planning involves all preventative processes necessary to continue program delivery, including those that are not necessarily IT related. The Computer Security Act of 1987, OMB Circular A-130, Appendix III, and PDD 63 require contingency planning for major systems as part of the security management process. Specifically, these mandates require that contingency planning be conducted for each major system. NIST Publication 800-34, Contingency Planning Guide for Information Technology Systems, provides additional guidance that will be used to establish USDA's IT Contingency Program. In order for plans in this program to be effective they must be executable, sustainable and tested on a regular basis. In the event of a disruption, the Business Impact Analysis (BIA) for major systems will determine how rapidly a system must be recovered. The BIA, a critical part of contingency planning, is conduct by the business owner and is used to establish contingency requirements and priorities in the event of a significant disruption in service.

Another critical component of this planning involves the development and implementation of the Disaster Recovery Plan (DRP) and Business Resumption Plan (BRP). These plans are designed to ensure that agencies and staff offices have the ability to maintain an acceptable level of business activities during and after a disaster. They also provide for a smooth and rapid restoration of major IT systems. DRP and BRP ensure that each agency establishes accountability for implementing, testing, and ongoing maintenance of these plans. In addition, they support the recovery of these systems in accordance with predetermined resumption strategies and disaster recovery measures. USDA IT and Business Program managers must collaborate and communicate on how to continue business and recover if service is disrupted.

The DRP refers to an IT-focused plan designed to restore operability of the target system, applications or computer facility at an alternate site after an emergency. It is narrower in scope than a COOP and does not address minor disruptions that do not require relocation. The BRP contains instructions or procedures describing how the business will be restored after a significant disruption has occurred and must be coordinated with other plans such as DRP, Occupant Emergency Plan (OEP), Contingency of Operations Plan (COOP), and Business Continuity Plan (BCP) which provide for the resumption of critical processes in providing acceptable level of service to customers. Therefore, integration of activities will ensure cohesiveness and that an effective IT Contingency Planning Program exists within the agency.

2 POLICY

Each agency and staff office will establish an IT Contingency Planning process. An executable DRP and BRP will be developed for each major system to ensure core business functions can be restored to full operation with minimum downtime in the event of a disruption or disaster. Contingency Planning will be incorporated and integrated in the system development life cycle process for all IT systems.

Each agency will use the departmental enterprise-wide software, Living Disaster Recovery Planning System (LDRPS), or approved comparable software to develop all USDA DRP and BRPs. Templates for these plans can be found in the LDRPS software. These plans will be implemented, tested and maintained for all major systems in support of critical business functions. All Plans must be detailed, routinely reviewed, and updated to provide for reasonable continuity of IT support in the event of a disaster. It is recommended that the agency require certification of the Contingency Planning Coordinator. Each agency and staff office shall take the following contingency planning actions:

a Conduct a Business Impact Analysis (BIA) to identify and prioritize critical IT resources. This analysis also determines the acceptable minimum level of system support necessary to restore mission critical core business functions and ranks business functions for restoration purposes.

b Identify preventive controls, which are measures to reduce the effects of an IT system disruptions. These measures can increase system availability and reduce contingency life costs;

c Develop recovery strategies to ensure that the system may be recovered quickly and effectively following an incident;

d Develop disaster recovery and business resumption plans that must include guidance and procedures for restoring the system that supports core business functions; the recovery procedures should be detailed enough that other personnel with the same job functions could perform the recovery tasks.

e Maintain and update DRP and BRPs. Agencies and Staff Offices must update plans biannually for major systems or following any significant change to their computing or telecommunications environment.

f Schedule testing for these plans. Develop a testing program and schedule for tests with review by CS, as required. Table Top testing should precede Live Testing to ensure the written plan is executable. Any deficiencies revealed by the tests must be corrected. The type of test and extent of testing will depend upon:

- criticality of agency business functions
- cost of executing the test plan
- budget availability
- complexity of information system and components

g Train employees. Assure sufficient employees are trained to provide alternates for key recovery positions.

h Participate in audit reviews. CS, GAO, OIG will conduct informal and formal review of all plans to ensure that they are executable and in compliance with standards.

Policy Exception Requirements – Agencies will submit all policy exception requests directly to the ACIO for Cyber Security. Exceptions to policy will be considered only in terms of implementation time; exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature and will require that each agency report this policy exception as a Plan of Action & Milestone (POA&M) in their FISMA reporting until full compliance is achieved. Interim exceptions cannot extend beyond the fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with a updated timeline for completion. CS will monitor all approved exceptions.

3 RESPONSIBILITIES

a The Associate CIO for Cyber Security will:

(1) Provide guidance and strategies to agencies and staff offices to assist them in establishing an Information Survivability Program; this includes contingency planning actions, developing, testing, and implementing executable DRP and BRPs;

(2) Review agency DRP and BRPs; track and monitor agency compliance with this policy. Provide an assessment report of all IT Contingency Plans to each Agency Administrator;

(3) Work closely with OIG to review all plans and provide the OIG assessment findings to each Agency Administrator or Agency Head. In addition, provide a specific timeline to complete any necessary revisions to ensure an executable plan;

(4) Identify measures that may enable enterprise-wide advantages in DRP and BRP activities across the Department;

(5) Direct, coordinate, and perform oversight reviews in compliance with this policy, as required;

(6) Observe DRP and BRP testing, as required;

(7) Evaluate and recommend a specific course of action to remedy deficiencies found during review of plans or tests; and

(8) Take necessary actions to impose penalties, if necessary, to ensure compliance with policy.

b Agency Heads/Administrators will:

(1) Designate a senior management official to establish and manage an Information Survivability Program within their agency or staff office;

(2) Provide annual budgeted funding and staffing for disaster recovery and business resumption activities such as testing, training and off-site storage; report all related security costs as required by OMB for system DRP, BRP and contingency planning for IT systems; and

(3) Ensure that all major systems are identified and prioritized in order of criticality and that all plans are reviewed, approved, and certified with a signature.

c Agency Chief Information Officer will:

(1) Establish and manage the IT Contingency Planning Program within the organization. Ensure that the positions and staff years are established to develop, implement, and maintain DRP and BRPs for each major system. Designate and train a Contingency Planning Coordinator;

(2) Advise and recommend to senior management within the organization solutions regarding DRP and BRPs based on CS reviews;

(3) Ensure that DRP and BRPs are: developed using the departmental enterprise software or an approved equivalent for major systems identified; ranked according to priority with the maximum system outage appropriate to the delivery of products and services; reviewed bi-annually, and executable in the event of a major incident or disaster. Ensure that there is an alternate backup site with operating procedures and personnel designated to run specific applications at the site;

(4) Ensure that DRP and BRP recovery solutions are closely coordinated and integrated with all emergency preparedness plans for major systems, interconnected systems and business processes as part of the system development life cycle;

(5) Test DRP and BRPs at least bi-annually or when a significant change occurs to the system unless an approved waiver has been obtained;

(6) Ensure that recovery procedures are developed and implemented;

(7) Provide specialized training and certification opportunities to the Contingency Planning Coordinator, appropriate training to all disaster recovery and business resumption team personnel and general disaster awareness training for all employees; and

(8) Ensure that all DRP and BRPs are reviewed and approved by the Agency Head; an electronic copy of all plans will be saved in the Enterprise recommended or other approved software; CS reserves the right to review all plans.

d The Contingency Planning Coordinator will:

(1) Identify and coordinate with internal and external points of contact for each major system to characterize the ways that they depend on or support the IT system. Ensure that data back up is implemented daily of critical files or tapes and stored off-site in the event of an incident or disaster;

(2) Identify disruption impacts and allowable outage times. Identify the maximum allowable time that a resource may be denied before it prevents or inhibits the performance of an essential function;

(3) Develop and prioritize recovery strategies that personnel will implement during contingency plan activation. Consider issues such as cost, allowable outage time, security, and integration with larger organization-level plans;

(4) Coordinate with officials to establish contingency teams and team leaders for damage assessment and recovery teams; and

(5) Ensure that plans are review and updated biannually.

-END-