

Achieving Continuity of Operations

Understanding & Implementing Continuity of Operations Plans

Continuity of Operations (COOP) planning has always been part of the fundamental mission of agencies throughout the Federal Government. For years, COOP planning had been an individual agency responsibility primarily in response to emergencies within the confines of the organization. The content and structure of the COOP plans, operational standards, and interagency coordination, if any, were left to the discretion of the agency.

The changing threat environment post-September 11 and recent disasters, including acts of nature, technological emergencies, military or terrorist related attacks and accidents have shifted awareness to the need for COOP capabilities that enable agencies to continue their mission-critical functions across a broad spectrum of emergencies. The objective of the COOP plan includes: ensuring the continuous performance of an agency's essential functions during an emergency; protecting essential facilities, equipment, records and other assets; reducing or mitigating disruptions to operations; reducing loss of life, minimizing damage and losses and achieving a timely and orderly recovery from an emergency and resumption of full service to citizens. Therefore, a broad COOP strategy was developed in order to ensure that individual departments and agencies are able to maintain minimum essential functions across a wide range of potential emergencies. There are three key components that have driven the development of the COOP plan: Presidential Decision Directive 63, Federal Preparedness Circular 65 and Presidential Decision Directive 67.

PRESIDENTIAL DECISION DIRECTIVE 63

The Presidential Decision Directive (PDD) 63, also known as the Critical Infrastructure Protection Directive, calls for a national-level effort to assure the security of the increasingly vulnerable and interconnected infrastructures of the United States. A major component of the directive involves the development and implementation of a plan by each department and agency of the Federal Government to protect its own critical infrastructure including cyberbased systems. There are three major asset categories that the PDD 63 covers: telecommunication

and telephony, information technology, and physical infrastructure. All three areas need to be accounted for in order to ensure the critical infrastructure is protected. VERITAS Software can assist agencies by ensuring their data and applications within the information technology (IT) environment are protected and available.

FEDERAL PREPAREDNESS CIRCULAR 65/ PRESIDENTIAL DECISION DIRECTIVE 67

As organizations began developing their Continuity of Operations Plan (COOP), they realized that coordinating the different teams that had been formed was essential. The Federal Preparedness Circular (FPC) 65 and the Presidential Decision Directive (PDD) 67 outlined the key elements in order to develop a viable and executable contingency plan to achieve continuity of operations.

The PDD-67 requires that a viable COOP must plan against all hazards that may affect the organization and that alternate facilities must be ready and available to return to operations within 12 hours after a disaster and that these operations can be sustained for up to 30 days.

OFFICE OF MANAGEMENT AND BUDGET CIRCULAR NO. A-130

Office of Management and Budget (OMB) Circular A-130 requires continuity of operations planning for every information system. The planning includes both contingency planning for short-term impacts to operations and continuity planning for longer-term impacts in order to rapidly and effectively handle potential disruption of mission-critical functions. To avert these disruptions, or minimize their damage, organizations must take proactive steps to develop a Continuity of Operations Plan (COOP). The Contingency portion of COOP focuses on minimal, day-to-day outages such as a localized short-term connectivity loss due to loss of a server, while the Continuity portion deals with long term or disaster scenarios. The COOP should contain operational recovery issues, ranging from arrangements for a

limited backup capability to relocation to a different facility in the event of a total failure. The goal is to protect lives, limit damage to property, and minimize the impact on operations, including information systems processing activities.

ELEMENTS OF A VIABLE COOP PLAN

The key elements to a viable COOP can be summarized in five distinct areas:

- The COOP must be maintained at a high level of readiness, meaning that thorough planning and implementation must occur prior to a disaster occurring.
- The COOP must be capable of implementation both with and without warning. Some disasters may provide a few hours of warning in order to allow the agency to react while other disasters may not provide any warning and call for the COOP to be implemented immediately.
- The COOP must be operational no later than 12 hours after activation.
- After a disaster has occurred and COOP has been initiated, operations must be able to be sustained for up to 30 days at the alternate facility.
- While agencies are developing their COOP plans they should take maximum advantage of existing agency field infrastructures.

There are many elements associated with delivering a viable COOP within an agency. VERITAS Software can assist agencies with their COOP by:

- Identifying mission-critical functions and recommending the appropriate technology to achieve the desired level of availability based on function.
- Protecting viable records and databases.
- Ensuring the operations of critical functions at alternative facilities.
- Provide for attaining operational capability within 12 hours.

- Establish and implement reliable technologies to allow agencies to continue essential functions and sustain operations for up to 30 days.
- Provide Disaster Recovery Plans, implementation and testing.
- Outline a decision process for determining appropriate actions in implementing COOP plans and procedures.
- Implement appropriate technology to meet COOP objectives.
- Test COOP plan.

All agencies must illustrate alignment with the mission of the Federal Government, part of which is a commitment to information sharing within and across agencies. Critical to the success of this mission is a reliance on the availability of accurate and timely information to support a broad range of government initiatives. Because virtually all mission-critical information is processed by computers, an agency's COOP plan must outline an overall risk management program to respond to unplanned and adverse situations that may destroy, damage, degrade, or compromise information systems data or computer processing capabilities so that essential operations may continue. The ability to quickly and easily access critical information is a major function of COOP.

IDENTIFYING MISSION-CRITICAL FUNCTIONS

As part of the planning process of COOP, agencies need to identify the essential functions that enable Federal agencies to provide vital services, exercise civil authority, maintain the safety and wellbeing of the general populace, and sustain the industrial/economic base in an emergency. In performing this process, agencies should identify important functions and then prioritize these functions in terms of mission-critical data and systems necessary to conduct essential functions. In addition, functions not deemed essential to immediate agency needs also need to be identified. Once the data is prioritized, understanding which technologies are necessary for particular data types is a much easier task. The first step to prioritizing data types is to understand the time frame allowable for data loss and recoverability of data. The key measure of disaster recovery technologies is based on recovery point objectives and recovery time objectives.

Recovery Point Objective (RPO) – Point in time to which applications data must be recovered to resume transactions.

Recovery Time Objective (RTO) – Maximum elapsed time allowed before lack of business function severely impacts an organization.

A complete disaster recovery plan is not delivered by any one technology, service, or vendor but rather a combination of products that are implemented in order to provide the needed RPO and RTO of an application. Performing this risk assessment can be a challenging task. To aid with this effort, the VERITAS Disaster Recovery Consulting Practice's team of leading disaster recovery certified, data availability professionals work with an agency's IT staff to map data and applications to the appropriate to the recovery point and recovery time objectives.

PROTECTING VITAL RECORDS AND DATABASES

The protection and availability of electronic and hardcopy documents, references, records and information systems needed to support essential functions under any disaster scenario is another critical element of a successful COOP plan. As outlined in FPC-65, the COOP plan should account for identification and protection of vital records, systems and data management software and equipment, to include any data necessary to perform essential functions and activities. In addition, agencies should pre-position and update duplicate records or backup electronic files to an alternate location on a regular basis.

The best way to ensure that vital records and databases are protected is by combining backup and replication technologies. Regular backups ensure all data can be recovered should a disaster occur. In addition, these tape backups need to be sent offsite on a regular basis to ensure they will be accessible should a disaster occur. The vaulting process should occur on a regular basis and be tracked by the agency.

For vital records and databases that may need to be accessed during a disaster scenario, VERITAS replication technology can be used to replicate the data to the disaster recovery site. This provides the ability to access the data immediately even during a disaster so that the vital records and database are protected.

In order to achieve maximum database availability clustering technology can be used to automate the

process of failing over applications and databases to an available server if there is a failure within an application, database, server or network environment. This software technology can dramatically reduce downtime associated with applications, databases and servers.

ENSURING THE OPERATIONS OF CRITICAL FUNCTIONS AT ALTERNATIVE FACILITIES

In addition, all agencies are required designate alternative operating facilities as part of their COOP plans and prepare their personnel for the possibility of unannounced relocation of essential functions and/or COOP contingency staffs to these facilities. Facilities may be identified from existing agency local or field infrastructures, or external sources but should be far enough away so it won't be impacted by the same disaster at the primary site. For example, if your primary data center is located in New York City and your secondary data center is located in Jersey City, both facilities may be impacted by the same disaster. Therefore, careful site planning but be followed to ensure that facilities are far enough away from each other so not to be impacted by the same disaster. Facilities shall be capable of supporting operations in a threat-free environment, as determined by the geographical location of the facility, a favorable assessment of the local threat, and/or the collective protection characteristics of the facility. Alternative facilities should provide the immediate capability to perform essential functions under various threat conditions. In addition, sufficient space and equipment must be available to sustain the relocation of the organization. Since the need to relocate may occur without warning, or access to normal operating facilities may be denied, agencies should maintain minimal essential equipment for continued operations at the alternative operating facilities. These alternate facilities should be prepared to sustain operations for a period of up to 30 days.

There are many site strategies that an organization can use in order to maintain the continuity of operations. The main site strategies are cold sites and hot sites.

Cold Site – A cold site is just a building available and ready should a disaster occur. In the event of a disaster situation, the affected agencies would need to acquire the appropriate hardware, software and communications necessary to conduct operations. Acquiring the appropriate technologies necessary to return to operations may be cost effective in the short term, as the agency does not have to maintain a duplicate environment. However, if an outage occurs it may be very expensive and time consuming to acquire the necessary hardware,

software and communications needed in order to begin operations in a new facility. In addition, there may be data security concerns, as special precautions must be taken to ensure that all data that system in a secure environment. A cold site strategy may be used if there are not stringent recovery point and recovery time objectives on the organization's data and applications.

Hot Site – A hot site, or redundant site, is a building already equipped with the processing capability and other services needed in order to immediately recover from a complete site outage. The site is normally equipped and configured similar to the primary site. Typically in hot site environments organizations are backing up their data at the primary site and using clustering technologies to provide application availability at the primary location.

Determining the appropriate location and type of site requires an understanding of the possible disasters that may occur in the area and fully understanding the essential functions of the agency so that recovery can occur during the required recovery point and recovery time objectives.

DISASTER RECOVERY PLANS, TESTING AND TRAINING

Developing a COOP plan, implementing technologies, learning the capabilities of the new technologies and testing the plan are essential to the viability of any COOP plan. Implementation and testing of the COOP capabilities is essential to demonstrating and improving the ability of agencies to execute their COOP plans during disaster scenarios. Periodic testing also ensures that equipment and procedures are maintained in a constant state of readiness. Training on the technologies associated with COOP plans familiarizes contingency staff members with the essential functions of the technologies and highlights processes they may have to follow during an emergency. With VERITAS Cluster Server Simulator and Disaster Recovery Fire Drill, administrators can freely test disaster recovery plans and application failover/migration scenarios in production, without disruption, to ensure availability in the event of an outage.

CENTRALIZED MANAGEMENT TO INCREASE AVAILABILITY AND EFFICIENCY

The ability to manage heterogeneous and geographically dispersed assets through a single web-based console that can be accessed anywhere not only increases availability by providing a holistic view of the IT environment, but also creates operational efficiencies via the standardization of tasks. By monitoring the environment and providing extensive reporting capabilities for clusters and replication, potential issues related to downtime can be proactively addressed and corrected.

ACHIEVING CONTINUITY OF OPERATIONS WITH VERITAS SOFTWARE

Achieving Continuity of Operations by ensuring Federal agencies will be up and running even during an outage is a critical function within any agency. VERITAS Software, the leading independent provider of storage software, provides a complete and integrated disaster recovery software solution to meet the various RPO and RTO objectives of the agency. Whether data and applications require backup, clustering or replication technology, VERITAS delivers a proven, integrated software solution, enabling agencies to recover their IT environment even if a disaster occurs. In addition, the VERITAS Disaster Recovery Services team will work with the agency's IT staff to create and maintain a viable COOP strategy.

For additional information about building a comprehensive COOP Plan and VERITAS Software Solutions designed to assist you, please call our offices or visit our Web site at www.veritas.com/government.

**VERITAS Software Corporation
Government Area**
2350 Corporate Park Drive, Suite 300
Herndon, VA 20171
800-327-2232, Option 2