LOB #303:

DISASTER RECOVERY

Purpose

Disaster Recovery (DR) for IT is a capability to restore enterprise-wide technology infrastructure, applications and data that are interrupted from a disaster event such as natural disasters (storms), utility outages affecting the Data Center (power), explosives that may destroy the data center, or mass system failures. Since the County is highly reliant on technology to perform services for all programs, and in advent of 9-11 and in more recent years, the occurrence of natural disasters on a more frequent basis than in the past, having ability to be more resilient and avoid interruptions and to continue to operate supporting disasters, traditional disaster recovery is now known as high-availability and is an operational necessity. Along with technology recovery, agencies should have a Continuity of Operations Plan (COOP) to be able to function in any gap period or worse-case scenario.

Continuity planning is operational mission assurance that the required critical services, technology and resources are available when alternate methods of assuring prioritized essential functions and capabilities need to be sustained or quickly restored. The Fairfax County Continuity of Operations Program provides the County Executive, his leadership team, and the County's senior managers with the ability to continuously direct, manage and sustain essential government services and business functions regardless of threats or disruptions, and under potentially ongoing adverse conditions. COOP planning priorities include the deployment of resources to protect the lives and safety, property, and economic security of Fairfax County's residential and corporate citizens during disruptions or long-term/large-scale emergencies where County resources or other critical infrastructure may be compromised.

Description

Disaster Recovery (DR) is a discretionary, discrete program supporting the entire County government for all systems in the DIT Data Center, and FOCUS for FCPS. Also within the scope of the DR LOB, the County's COOP program is an essential partner function, aligned, thus herein represented. DIT has had DR as an essential part of its Data Center operations since its inception. In the 1990s, almost all County applications were on the mainframe environment, and in that era, DR was a process by where organizations had a contract to be able to load their applications at an off-site commercial data center and run for an interim period. This required staff to retrieve back-up tapes in a bonded commercial vault, go to the back-up site, load and activate the service. In the time that the County had this service, it never had to be formally activated as the County's processing technology was reliable and stable.

As technology evolved and most systems moved from the old mainframe environment to a variety of server and storage platforms, the traditional DR business model and contract structure was ultimately not well suited to meet the availability requirements of these newer environments. Such contracts while in normal disaster recovery scenarios would work, in reality, availability was built on science that suggested a small percentage of customers would need the service simultaneously, thus a shared environment with limited total available capacity.

In 2014, as the FOCUS project removed most of the last of the old mainframe based systems, and with its new technology and 24 x 7 availability, the business case was strengthened to move to a more modern approach for business continuity and system availability. As a result, in FY 2014, reinforced by a report of the Auditor to the Board, DIT established new disaster recovery capabilities in-line with contemporary business and technical specificities and developed a commercial-class production failover architecture that could be shared by all critical enterprise and county-agencies' IT services and applications. The new DR-'High Availability' service began implementation during FY 2014. It provides for near real-time availability from a third party off-site facility, a significant improvement over the legacy DR processes whereby system recovery would be achieved over several days. The failover environment includes a secure, certified off-site location, high-speed network connectivity between the Fairfax Government Center and the off-site location, and critical infrastructure (power, network, storage, servers, etc.) and state-of-the art replication and

recovery processes and tools. The process of planning, designing, and implementing an IT environment at a failover site to deliver the following services include: Services Failover / Application Recovery, High Availability / Redundancy, Data Backup / Archiving, Data Restore, Data Replication.

FOCUS was the initial application set-up, and the initial investment is being leveraged for and will continue to be expanded for agency applications housed in official County data centers through failover capability. There are over 600 applications in the DIT Data Center.

The task to move agencies' mission critical applications to the third-party off-site hosting/DR facility will take place throughout FY 2016. Staff in the Data Center, FOCUS Tech Team, Platform, and Network divisions of DIT are responsible for activating DR.

COOP

The continuity program coordinates the efforts of more than 110 (part-time assignment) staff, representing all 45 departments and agencies. Using this matrix model provides the County with a fiscally-responsible, yet robust continuity framework to address the important challenges of assuring each agency has a viable COOP Plan. The Program Manager is assigned to the Office of the County Executive, reporting directly to the Deputy County Executive for government operations. The program framework ensures every Agency COOP Plan adequately captures and reflects the structural interdependencies with other agencies, and identifies the requisite collaboration necessary with critical State or Federal partners, community stakeholders, corporate partners and private sector vendors – upon which many County services depend for successful continuity of operations.

Fairfax County Continuity of Operations Planning is conducted under the leadership and direction of the Office of the County Executive. Continuity planning is a collaborative and coordinated effort across all departments and agencies – empowered and guided by Federal, State and municipal laws and policy directives. Additionally, Fairfax County executive policy memorandums regarding prioritization of essential services; information technology systems priorities; and human resource policies dictate the parameters for creating and maintaining viable COOP Plans for each agency. Beginning in FY2014, the County Executive directed that each County agency, including numerous divisions and sub-units conduct tabletop exercises to evaluate the viability of their respective plans.

This comprehensive framework reflects the commitment of government leaders to fulfill their responsibility to protect the safety, property and economic security of Fairfax County during any type of emergency or catastrophic event that threatens or inhibits government operations. Continuity planning has been a function of County departments and agencies since 2001. Beginning in 2010, the County has been partnering with the Virginia Department of Emergency Management, Department of Homeland Security and Federal Emergency Management Agency (FEMA) to develop and share continuity plan templates, host regional workshops and training events, and provide planning and staffing resources. Many of these resources have been shared with neighboring jurisdictions in the National Capital Region (NCR), throughout the State and across the country. The County's continuity program has been offered as an example of a best practice for State, Territorial, Tribal and local government continuity of operations planning by FEMA's National Continuity Programs office.

The County's continuity of operations program has been managed as a very lean effort, with interruptions caused by staff turnover since its inception. In the past five years, the program has focused on revamping and enhancing the plan template used by the agencies (reducing the document from a cumbersome 70+ pages to a base template of 12 pages). Since 2014, the COOP Coordinator has worked closely with DIT on DR and Cyber matters.

Benefits

The benefits of instituting a DR capability will allow for reducing the possibilities of downtime to County operations through IT failover capabilities through a seamless, robust, and carefully designed DR capability. Additional benefits include:

- Fast and complete recovery.
- Selected applications and infrastructure services operational during a disaster or temporary outage at Government Center.
- Elimination of Government Center as a single point of vulnerability
- High availability enabling the County to continue operations and delivery of services in the event of a disaster.
- Stronger protection and integrity of data, hardware, software, and County IT services.
- Ability to build on scalable infrastructure.
- Minimal to no disruption to users or systems.
- Increased confidence from stakeholders, users and the public.

DR-High Availability is a high industry best practice, mostly implemented in major commercial corporations, not yet adopted in many governments due to cost and residual portfolios of obsolete technology systems. Having this capability strengthens the County's posture for financial rating and is a key element in audits.

COOP

Mission assurance and business continuity are good business practices. The 21st century challenge for local governments is continuing to sustain critically important services for its community. Whether the threat is cybersecurity, terrorism, or a significant weather event, local governments must maintain mission assurance. Continuity of operations and business continuity planning ensures resilient capabilities exist across the organization so essential services, critically important resources and competent staff are always available to provide for the community's safety, well-being and economic vitality.

Using the highly-efficient matrix staffing model, a single full-time program manager is funded by the County's General Fund. Coordinating this staffing structure from the Office of the County Executive demonstrates the value and importance of the continuity program, and the recognition of having the support of the organization's chief administrative officer. This empowers the program with the ability to work across all levels of the organization, coordinating with each of the other Deputy County Executives, the Chief Financial Officer, Chief Information Officer, and each department head. This program works closely with DIT in supporting DR and Cyber activities.

The continuity program directly supports every County agencies capability to perform the services and functions for which it was created, and assures the County elected leadership that each vision element.

Mandates

Disaster Recovery (DR)
This program is not mandated however, the requirement for a Disaster Recovery program was requested by the Fairfax County Board of Supervisors.

COOP
Federal, State and local statutes that provide legal authorities for the continuity program vary between departments and agencies. Many agencies are legally empowered and/or required to provide services, enforce Federal, State or county laws and ordinances. Other agencies are legally obligated to ensure the security of personal, financial, health and safety information. Examples of some laws, statutory regulations and/or guidelines include:

- United States of America
  - U.S. Constitution (1992)
  - U.S. Code (2011)
    - Title 6. Chapter 2. National Emergency Management
    - Title 10. Chapter 18. Military Support for Civilian Law Enforcement Agencies
    - Title 32. National Guard, Deployment
    - Title 42. Chapter 68. Disaster Relief
      - Robert T. Stafford Act, PL 93-288, as amended (2007)

- U.S. Code of Federal Regulations (2011-2012)
  - 6 CFR 29 – Domestic Security, Protected Critical Infrastructure
  - 36 CFR Part 1236 – Vital Records Management
  - 41 CFR 102-74 – Facility Management
  - 44 CFR – Emergency Management and Assistance

- National & Homeland Security Presidential Policy (NSPD, HSPD & PPD) Directives
  - HSPD 5 – National Incident Management System
  - HSPD 8 & PPD 8 – National Preparedness
  - HSPD 20 – Continuity of Operations

- U.S. Department of Homeland Security – FEMA
  - National Response Framework (2008)
  - National Infrastructure Protection Plan (2009)
  - National Preparedness Goal (2011)
  - Continuity Guidance Circular 1 (2009)
  - Continuity Guidance Circular 2 (2010)
  - Comprehensive Planning Guidance 101 v2 (2010)

- Commonwealth of Virginia
  - Virginia Constitution (1971)
    - Article VII – Local Government

- Code of Virginia (2011)
  - Title 15.2, Chapter 14; §15.2-1413
  - Title 44, Chapter 3.2; §44-146.13 – §44-146.29:1

- Virginia Emergency Operations Plan (2012)
  - Volumes I-VIII

- County of Fairfax
  - Fairfax County Code (2012)
  - County Executive Priority of Services Policy Memo (12 Mar 2010)
  - DIT Priority of Systems Policy Memo (13 Nov 2009)
  - Protection of Personal Information Policy Memo (11 Oct 2011)
  - Fairfax County Emergency Operations Plan (2015)
  - Fairfax County Pre-Disaster Recovery Plan (2012)

- Private, Non-Governmental Organizations
  - NIST – Business Continuity Guidance & Industry Standards
    - ISO 22301
    - ISO 27001

- National Fire Protection Association NFPA 1600 (2010)

Trends and Challenges

Disaster Recovery (DR)

Trends

- The County is on the leading edge of implementing high availability, near real time failover. The occurrence of disasters and business demands are increasing for Fairfax County which requires minimal downtime of systems/applications, and minimal inaccessibility of county data and services.
- Clouds – major Cloud infrastructure providers would most likely have at least a secondary site failover process, which should be in contracts.

Challenges

In today's increasingly complex data center environment, providing automated high availability and disaster recovery is a major challenge.

- Complex design and planning required for the number of systems, applications, infrastructure, and data required to failover over as part of County applications.
- Appropriate resource allocations (funding, resources, schedule) continue to be required.
- Competing Priorities – (Staff and Vendors) – County FTEs and vendors may not all be available due to other priorities from other approved projects, normal operations, or production emergencies.
- Funding– Possible delays in equipment/resources due to the approval/funding of any needed purchase orders.
- Functional Buy-In – Possible delays in implementation/testing due to required approvals by stakeholders for any work being performed which may impact their business (i.e. outages).

In times of budgetary constraints, coupled with a record of sustained reliability of the core systems and lack of actual disaster situations necessitating failover, maintaining commitment to funding a robust DR solution could be problematic.

COOP

The trend for COOP is expanding in government, and considered a best practice. County agencies should automatically have COOP embedded in their operations as a normal procedure. However, with years of budget reductions limiting available resources in agencies, finding time to modify plans along with deployment of new services and technology capabilities and exercise plans is an on-going challenge. Further, providing ongoing workshops and training opportunities to support staff across all 45 agencies with consistent guidance and full-time technical assistance is a challenge.

Resources

Category	FY 2014 Actual	FY 2015 Actual	FY 2016 Adopted
LOB #303: Disaster Recovery			
FUNDING			
Expenditures:			
Operating Expenses	$1,077,191	$1,989,905	$2,034,630
Total Expenditures	$1,077,191	$1,989,905	$2,034,630
Total Revenue	$0	$0	$0
POSITIONS			
Authorized Positions/Full-Time Equivalents (FTEs)			
Positions:			
Regular	0 / 0	0 / 0	0 / 0
Total Positions	0 / 0	0 / 0	0 / 0

Metrics

Metric Indicator	FY 2013 Actual	FY 2014 Actual	FY 2015 Actual	FY 2016 Estimate	FY 2017 Estimate
Percent Uptime of FOCUS ERP System	98%	99%	99.99%	99.99%	99.99%
Enterprise Production Applications with DR/Failover	4%	13%	21%	38%	92%

The County is on the leading edge of implementing high availability, near real time failover. The potential for disasters, less disruption tolerance to business operations, and more demand for supporting technology in all business areas are increasing for Fairfax County which requires minimal downtime of systems/applications, and optimal accessibility of county data and services.

There are over 600 Enterprise and Agency Open Systems Applications and databases in the DIT County Data Center. Prior to FY 2015, the only apps in the legacy DR model were those on the old mainframe environment. In FY 2015, the County awarded a contract for modern near-real time back-up recovery, with budget provided to cover the data center landscape. The process to implement the new strategy started with the core FOCUS system, and incrementally the inventory of data and compliant systems will be implemented. Careful planning and testing is required for each application and subsystem for the DR environment.