A WHITE PAPER

Federal Continuity of Operations

Part 5 of 10: Continuity Strategies

Topic Summary:

- Continuity strategy defined
- Practices for determining continuity strategies
- Tailoring a continuity strategy to a customer's needs
- Summary and Recommendations for next steps

Table of Contents

Illustration Index

Table Index

1.0 Introduction

Within the federal government and the Department of Defense (DOD), the Business Continuity Management (BCM) Program finds its equivalent in a Continuity of Operations (COOP) Program. The COOP Program exists to ensure that continuity of government (COG) can occur even in the face of a national disaster. Federal, DOD, and Army policy all reflect this emphasis on what must be done to ensure that our government can continue to provide leadership and direction to the nation and the world regardless of the circumstances.

This paper, the fifth in a series of ten, analyzes how a small Army Program can define appropriate continuity strategies as part of the larger COOP Program implementation. Such continuity strategies must ensure that the Army Program can accomplish its mission and provide the guidance necessary for the COOP Practitioner to create the COOP Plan. This paper provides concrete recommendations and prepares the way for the practitioner to identify the specific planning documents that make up a complete continuity response.

2.0 Practices for Determining a Continuity Strategy

A tailored *Continuity Strategy* provides the basis for the successful BCM Program. An organization must understand what functions it performs and – more importantly – *why* it performs those functions for a continuity plan to be reliable and comprehensive. The continuity strategy informs the plan by forcing the organization to consider its approach objectives; this strategy is always unique to the organization.

Consider an outsourced helpdesk firm which must ensure that it can continue to receive calls and provide assistance to its customers or face Service Level Agreement (SLA) penalties and potential lost business. Such a firm need not concern itself with concerns over damage to its physical shipping capabilities (such as trucks) as a manufacturing firm must. Rather, the helpdesk firm needs to concentrate on making sure that it has properly trained people to speak to customers and the technical infrastructure to send and receive phone calls within the (SLA) timelines. Likewise, an insurance company responding within a disaster area must have trained staff with excellent interpersonal skills and equipped to communicate with each other and the home office in the absence of a functioning power grid. The helpdesk firm, manufacturing firm, and the insurance company each needs a distinct continuity strategy to address its specific concerns.

Within the federal government, DOD, and the Army the need for continuity strategy is just as strong. While the emphasis is different than the commercial world's need to retain their customer base while not being penalized for non-performance, the goal to ensure continuity of government and military functions provides a clear mandate for a well-articulated continuity strategy. This section looks at guidance both from the Army and the commercial world for creating a tailored continuity strategy.

2.1 Army Guidance

The Army provides Army Regulation (AR) 525-26 ("Infrastructure Risk Management (Army)"); despite the overly information technology (IT) sounding name, this guide treats "infrastructure" as critical components making up "agriculture and food, water, public health, emergency services, defense industrial base, telecommunications; energy; banking and finance; transportation; chemical industry and hazardous materials, and postal and shipping" (p 10). This larger concept of infrastructure certainly includes the data communication services provided by the Army Program use case presented by this series of papers, so AR 525-26 makes a good starting

point to determine the specific continuity strategies that the COOP Practitioner should consider when preparing to craft the COOP Plan.

AR 525-26 calls for the practitioner to consider:

- Assess whether the nonperformance of identified critical functions within the program could threaten an Army core competency. For these competencies, practitioners should refer to the Army's Strategic Readiness System (SRS) and assets identified by the higher-level major command (MACOM).
- Determine the risk to physical and cyber (public and private) infrastructure.
- Ensure that assets supporting that infrastructure have redundancy and alternate locations.
- Ensure that trained personnel are available to execute the program's critical functions within alternate locations.
- Define necessary communication paths during COOP activation.
- Analyze trend information of prior threat or hazard occurrences to help prioritize COOP Plan components.
- Align the program's risk management strategies with higher-level MACOM and Army goals and objectives.

AR 525-26 refers the reader to the Army's overall risk management and COOP planning, which leads back to AR 500-3 ("U.S. Army Continuity of Operations Program Policy and Planning"), DOD Directive 3020.26 ("Department of Defense Continuity Programs") and DOD Instruction 3020.42 ("Defense Continuity Plan Development") which have been covered in previous papers.

2.2 Commercial Guidance

While the Army guidance is sound and based upon general principles, the commercial world provides the COOP Practitioner with a specific set of tools and techniques to determine the best tailoring of continuity strategies to the target program. The Business Continuity Institute (BCI) has provided a Good Practice Guide (GPG) with a thorough analysis of the international standard for BCM: British Standard (BS) 25999-1:2006. The GPG defines the following strategies to consider when building a BCM Program.

Table 1: BS 25999-1:2006 BCM Strategies Mapped to the Army Use Case[1]

BS 25999-1:2006 Continuity Strategy Component *Component*	**Applied to Use Case (Army Program)**
Recovery Time Objective (RTO) – the organization will not want simply to recover an interrupted activity in time to prevent system collapse, but will want "a margin in case of unforeseen difficulties with recovery or if its original measurement" was inaccurate.	Basing COOP planning strictly on how long the most demanding customer can tolerate data outage is not sufficient; the practitioner must build in a weighting factor to allow for slippage.

[1] Adapted from the GPG (GPG08-3, p 5-18).

BS 25999-1:2006 Continuity Strategy Component	Applied to Use Case (Army Program)
Resilience – "something can suffer a failure and yet still continue operations"	Build a COOP facility; Use virtual images on redundant hardware within the hosting facility
Reliability – Contract with a third-party to ensure that services are available when needed.	DOD functions are hosted within Defense Information Systems Agency (DISA) Enterprise Computing Centers (DECCs) and have less recourse. The DISA also must implement a COOP Program, so the COOP Practitioner should refer to the hosting facility's plan to ensure the reliability level.
Cost / Benefit – "Manufacturing and service industries who supply other businesses may be able to demonstrate increased sales or better margins can be achieved by demonstrating BCM capabilities (i.e. improved reliability) to their customers - and thus show a benefit to be compared to costs."	Within the DOD, and especially given the current emphasis on cost reduction, ensuring that the required continuity levels can be achieved based on a defensible analysis of alternatives (AoA) improves the COOP Program's chances for full implementation.
Verifying capabilities of third-party recovery sites – The ability of the recovery site to scale to an actual emergency (for example, providing dedicated facility access or not accepting multiple customers from the same defined geographic location).	A COOP site for the Army Program needs to be within a DISA DECC just as the standard hosting site. These DECCs are located around the country and already have defined levels of capacity; the COOP Practitioner needs to refer to the DECC'S availability policy for more information.
Training to enable the "protection of the organisation's knowledge and skills…[and]…protection against loss or absence of key staff."	Thorough documentation to meet the Army's existing formal requirements, in conjunction with a *defined knowledge transfer process* can help to ensure that trained staff members exist to execute a COOP declaration.
Arranging for "ship in" contracts where key equipment or materials can be provided quickly during a COOP declaration.	For the Army Program use case this is of less applicability; appropriate knowledge transfer to geographically diverse staff in conjunction with a COOP facility provide much of this capability.
Telephony – "The logistical problem of handling telephone calls during an interruption, once they have been redirected, needs to be addressed."	Within the Army Program, this would be handled by having a phone tree of all essential staff in conjunction with the ability to redirect incoming customer calls to a predefined remote site.
Information – The GPG speaks to *confidentiality* (information is not disclosed), *integrity* (information does not change), *availability* (decision makers can access information when needed), and *currency* (in-flight transactions are protected).	The Army Program processes classified data, which imposes special restrictions on storage and access requirements. Classified data must be provided on the Secure Internet Protocol Routing Network (SIPRNet). In-flight transactions are less important because there data consumers make individual

BS 25999-1:2006 Continuity Strategy Component	Applied to Use Case (Army Program)
	Web service calls.
Stakeholders, Partners, and Contractors – "The organisation's level of responsibility (both legal and moral) for these groups should be understood."	The Army Program must ensure that customers can be notified in the event of a COOP declaration. This can be accomplished by ensuring that a defined customer notification plan exists.

3.0 Continuity Strategy for Army Program Use Case

The Army Program use case must have its own specialized continuity strategy; this section provides specific tools and techniques for creating this strategy.

3.1 Determine RTOs / RPOs

Of the 150 users that currently access the Army Program, two require access every day by 9am EST. Any failure beyond that time must be communicated within three hours to avoid technical violations. No customers report danger to their mission for outages less than one week except at fiscal year-end time. The Recovery Point Objective ("the point to which information must be restored to enable an activity to operate once it is resumed")[2] is not applicable except for defined data loads from data providers. The Recovery Time Objective (RTO), or "the period of time within which systems, applications, or functions must be recovered after an outage"[3] is therefore one week.

Strategy: Provider data loads must be transaction driven to avoid integrity problems if a problem occurs, while customer data consumption capabilities become critical only after one week.

[2] GPG08-2, p 6.

[3] NFPA, p 23.

3.2 Resilience and Reliability, Third-Party Recovery Sites

The Army Program is defining a cloud model to ensure that failures in one center can be transferred automatically to another center (a "dynamic cloud" model) as shown below:

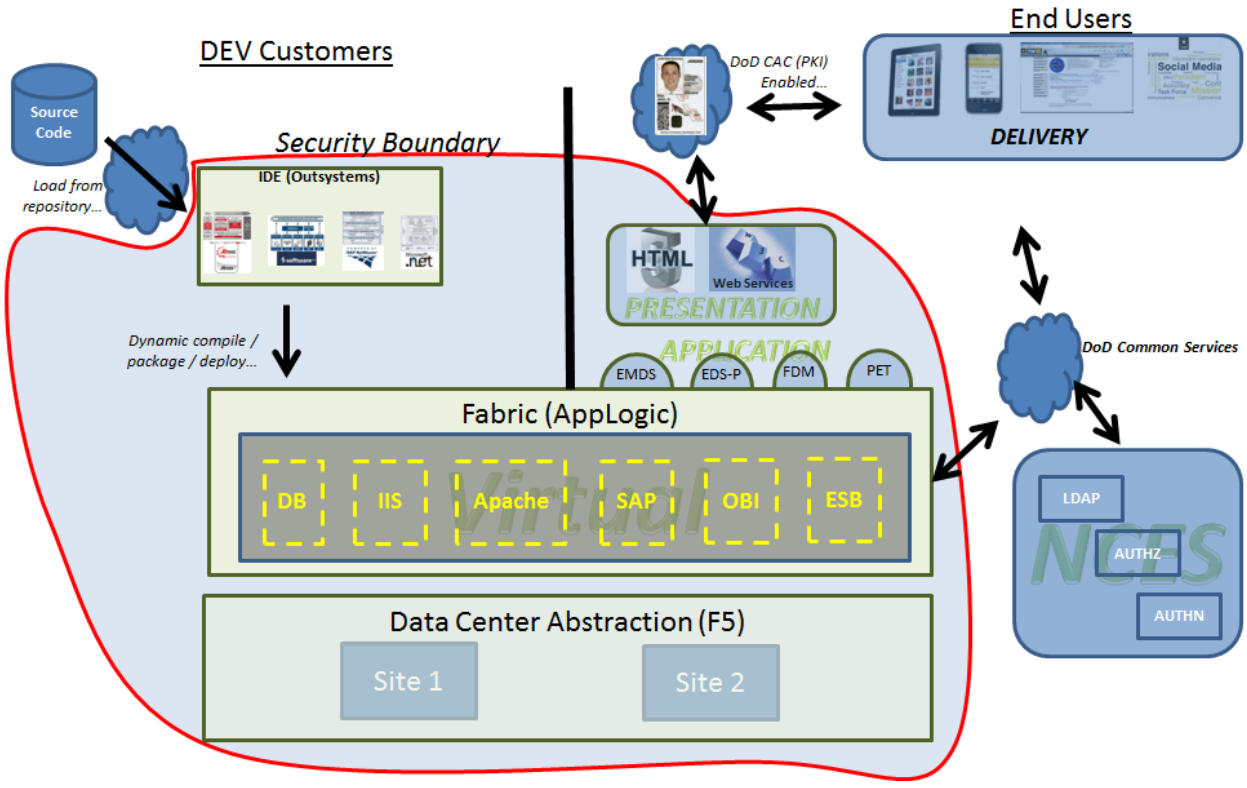

Figure 1: Cloud model to provide resilience[4]

The COOP Plan identifies this cloud computing model as an essential aspect. The COOP Site for this program is enabled automatically by the hosting provider as shown within the "Data Center Abstraction" layer.

Strategy: Build the COOP Plan based upon a highly-available infrastructure maintained by the hosting provider.

3.3 Cost Benefit and Training

The hosting provider already provides a significant economy of scale for technical redundancy. The training requirements can be cost-optimized by including an ongoing employee training module within the COOP Program. Using distance-based learning to train dispersed personnel on customer notification procedures will further reduce costs, while system administration functions can be delegated to trusted remote personnel to enable virtual management.

Strategy: Enable distance learning and training programs as part of the COOP Plan, and specify a means for system documentation to be securely available to remote administrators.

[4] Source: Redacted architectural diagram from the Army Program use case.

3.4 Communications and Stakeholder Relations

Upon a COOP declaration or any significant outage, communications occurs via a phone tree with key customer points-of-contact (POCs). These POCs must also be available in paper form so that, during an emergency, designated communication personnel within the Army Program can have access to this information. A current printed contact list must be provided for within the COOP Plan, as well as at least three different communications paths. For example, automated email broadcast notification systems in conjunction with the printed phone list, supplemented by a common announcement board provided by the highly-available hosting provider. Employee communications can be provided for in the same way; the COOP Plan must include regularly-updated resource contact information.

Strategy: Require contact information to be collected from all program employees, and specify that a collaboration portal is available (itself highly available). Investigate email broadcast capabilities with the program's primary email provider, and verify the email provider's COOP strategy / plan. Email contact information must include at least two email addresses per employee, along with pager / cellphone contact details.

3.5 Program Information Strategy

Because the Army Program houses classified data on the SIPRNet, the hosting provider must provide a "SIPR Vault" to house the physical servers and databases that contain this information. Additionally, access to the data systems must be carefully controlled regardless of whether a COOP declaration is in force or not. Unauthorized consumers may never access classified data, even in an emergency.

The COOP Plan must provide a clear succession strategy to ensure that, if program officials are not available, a chain of command can be provided. This chain of command needs procedures for ensuring that required data can be accessed, including the processes by which emergency data access authorization can be granted.

Strategy: Identify chain of command succession as part of an overall information management process. Ensure that all hosting facilities (primary and backup) provide support for classified data storage.

4.0 Concluding Remarks

4.1 Summary

This paper has demonstrated how continuity strategy tools and techniques can be taken from both public and private sources to create a tailored strategy. Within the Army, AR 525-26 provides a good starting point for determining these strategies: determining how long a function can nonperform before its absence becomes critical; ensuring redundancy of infrastructure supporting a program; training personnel to provide customer and stakeholder communications; reviewing trends within the industry; and, aligning specific strategies to higher-level policies and objectives.

BS 25999-1:2006 serves as the commercial guidance for COOP strategy planning, and this paper highlighted a number of key factors that the standard identifies with implementation notes for each factor. One important note is for the practitioner to keep in mind that building a function to restore within a defined RTO is not sufficient, as the recovery process may have problems being executed. Each recovery strategy must include a cost / benefit analysis component; in a recovery situation every resource dollar is precious because the organization is *already in a funds-draining environment*. Third-party recovery sites need to be looked at

carefully to ensure they can meet organizational requirements; the COOP practitioner should investigate the COOP plans for these third-parties to verify that they will suffice in an emergency. Communications and data must be protected; communications so that stakeholders and employees can be notified of instructions during an emergency; and, data so that decision makers can securely access the information they need in a timely manner.

4.2 Recommendations

This paper has provided a tailored continuity strategy to its Army Program use case and has provided a number of recommendations as shown in the table below:

Table 2: Recommendations

Recommendation	Rationale
Remember that the line of business affects the continuity strategy.	Continuity is not a one-size-fits-all model. Within the federal government and DOD, continuity ensures that the organizational mission can be accomplished while the commercial world emphasizes the ability to preserve revenue and customers. In either case, the focus of the business provides the context needed for creating the best continuity strategy.
Assess the threat of nonperformance first.	The RTO and RPO requirements for the products and / or services offered by the organization heavily impact the continuity strategy to pursue. For example, a service-oriented company needs a continuity strategy that prioritizes service delivery capabilities.
Ensure that COOP strategies of third-party providers are verified.	A successful COOP Program does not exist in a vacuum, especially for smaller organizations attempting to implement a COOP Program within a constrained budget. External entities will provide backup capabilities, alternate work facilities, and even recovery / salvage expertise. The COOP practitioner must review these third-parties' COOP posture as part of COOP strategy development.
Provide for reliable communications mechanisms.	During a disaster, normal methods of communications may not exist. The company phone directory, for example, may not be available. The key to disaster communications lies in planning ahead: printed lists provided to key communication facilitators; alternate email delivery and usage of mobile text messaging can help to ensure that the organization's message is delivered during an emergency.
Plan for an orderly succession.	If a key decision maker is not available during an incident, then valuable time can be lost where proper authority does not exist. The COOP strategy needs to ensure that authorized deputies are identified for each defined function so that actions can be taken to contain an emergency situation as soon as possible.

4.3 Next Steps

The next paper in this series will identify which continuity planning documents will be required in order to ensure that the final COOP Plan will be complete. Planning documents such as the Incident Response Plan, the

Incident Communications Plan, the IT Disaster Recovery Plan, and other plans make up the overall BCM Program and ensure that it can be executed successfully. Additionally, the due diligence required to understand the business functions leading up to these plans' creation helps to ensure that the organization fully appreciates the various activities that it performs on a regular basis. This increased awareness and understanding provides a sound foundation for the COOP Program.

Appendix A: Acronyms and Abbreviations

AoA	Analysis of Alternatives
AR	U.S. Army Regulation
BCI	Business Continuity Institute
BCM	Business Continuity Management
BS	British Standard
COOP	Continuity of Operations
DECC	DOD Enterprise Computing Centers
DISA	Defense Information Systems Agency
DOD	Department of Defense
GPG	Good Practice Guidelines
IA	Information Assurance
IT	Information Technology
MACOM	Major Command
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SIPRNet	Secure Internet Protocol Routing Network
SLA	Service Level Agreement
SRS	Army Strategic Readiness System
U.S.	United States

About the Author

Andrew Bruce is a Lead Scientist for Computer Sciences Corporation (CSC) in the Army Programs group of the North American Public Sector. CSC provides professional services to the Federal Government and the Department of Defense, specializing in customizing and developing architecture and governance models that enable tight integration to the Army's enterprise portfolio management initiatives. Mr. Bruce's job responsibilities include: working directly with customers and partners for new business development, supporting proposal efforts, overseeing Army customers' network infrastructure, working with project managers to ensure project completion, managing software development efforts throughout the entire system life-cycle, and leading new technology research and proofs-of-concept. After a career spanning three decades in shrink-wrap, commercial, and corporate software development, Mr. Bruce is focusing on Information Assurance to achieve his goal of building and managing large data centers providing cloud computing utility services for commercial and Government customers. Mr. Bruce holds the CISSP, PMP, and FITSP-D certifications and is currently pursuing a Master's Degree in Information Assurance from Norwich University.

Reference List

[AR525-26] Department of the Army. June 22, 2004. Army Regulation 525-26: Infrastructure Risk Management (Army). <http://www.apd.army.mil/pdffiles/r525_26.pdf>. Accessed: June 26, 2011. 23 p.

[AR500-3] Department of the Army. April 18, 2008. Army Regulation 500-3: U.S. Army Continuity of Operations Program Policy and Planning. <http://www.fas.org/irp/doddir/army/ar500-3.pdf>. Accessed: June 12, 2011. 39 p.

[DOD-3020.26] Department of Defense. January 9, 2009. DoDD 3020.26: Department of Defense Continuity Programs. <http://www.dtic.mil/whs/directives/corres/pdf/302026p.pdf>. Accessed: June 15, 2011. 10 p.

[DOD-3020.42] Department of Defense. February 17, 2006 (Certified current as of April 27, 2011). DODI 3020.42: Defense Continuity Plan Development. <http://www.dtic.mil/whs/directives/corres/pdf/302042p.pdf>. Accessed: June 21, 2011. 11 p.

[GPG08-2] Business Continuity Institute. 2007. Good Practice Guidelines 2008: A Management Guide to Implementing Global Good Practice in Business Continuity (Section 2). Caversham (UK). 14 p.

[GPG08-3] Business Continuity Institute. 2007. Good Practice Guidelines 2008: A Management Guide to Implementing Global Good Practice in Business Continuity (Section 3). Caversham (UK). 18 p.

[NFPA] National Fire Protection Association. 2010. NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs (2010 Edition). Quincy (MA). 52 p.