A WHITE PAPER

Federal Continuity of Operations

Part 8 of 10: Protect the Information and Communication Technology (ICT) Infrastructure

Topic Summary:

- Tie approach between commercial, federal, Department of Defense, and Army
- Information, Communications, and Technology (ICT) Planning, Implementation, and Testing
- Summary and Recommendations for next steps

Table of Contents

Illustration Index

Table Index

1.0 Introduction

Business Continuity Management (BCM) recognizes the mission-critical nature of Information Technology (IT) systems within the organization, and uses Information, Communications, and Technology (ICT) Continuity Planning to ensure that IT systems remain available, secure, and functional in disaster scenarios. Within the federal government and the Department of Defense (DOD), BCM is implemented as Continuity of Operations (COOP) and IT systems provide the backbone enabling agencies to ensure Continuity of Government (COG) just as in the private sector.

However, high-level federal and DOD policy concentrate ITC Continuity Planning on "national essential functions" (NEFs) that exist to support COG; this emphasis on "big systems" can sometimes lead smaller agencies and programs to forego the benefits of a COOP Program. This paper analyzes how organizations of all sizes, including small Army Programs that are not normally considered to be NEFs, can benefit from a policy-based and cost-efficient ICT Continuity Plan as part of an overall COOP Plan. Such plans do not need to exceed the Program's budget and can provide significant assurance that the Program can accomplish its mission despite a disaster scenario.

This paper advocates that the ICT Continuity Plan should be a separate sub-plan within the Program's overall COOP Plan. Moreover, the Program should follow a standard System Development Lifecycle (SDLC) to ensure that the ICT Continuity Plan is effective without being wasteful. The paper provides practical suggestions aimed at its Army Program use case that apply to the larger federal IT community, and closes with a summary of its findings.

2.0 Approach and Policy Guidelines

ICT Continuity Planning is a holistic approach to IT Disaster Recovery (DR); whereas IT DR concentrates on restoring the IT infrastructure, ICT Continuity Planning encourages a proactive approach to ensure overall organizational resiliency (for example, operating at an acceptable albeit degraded IT performance level even in the face of a large-scale disaster). This paper's approach to ICT Continuity Planning is to review how capabilities and processes within the organization, combined with applicable policy statements, help to inform a complete COOP Plan and to provide the organization with the best possible value.

2.1 Capabilities and Processes for ICT Continuity

The IT Infrastructure Library (ITIL) defines a *capability* as "the ability of an Organisation, person, Process, Application, Configuration Item or IT Service to carry out an Activity. Capabilities are intangible Assets of an Organisation" (ITIL, p 8). A *process*, on the other hand is defined as "a structured set of Activities designed to accomplish a specific Objective. A Process takes one or more defined inputs and turns them into defined outputs. A Process may include any of the Roles, responsibilities, tools and management Controls required to reliably deliver the outputs. A Process may define Policies, Standards, Guidelines, Activities, and Work Instructions if they are needed" (ITIL, p 36).

Within ICT Continuity Planning, capabilities refer to the specialized expertise that the organization has in ensuring that the IT infrastructure remains available and useful to decision makers. These capabilities are implemented within the organization by using processes and procedures grounded in system policy and aligned

with high-level system goals and objectives.

2.2 Policy

Policy for ICT Continuity Planning exists at the commercial level via British Standard (BS) 25999-1:2006 ("Business Continuity Management: Part 1: Code of Practice"), the DOD level via DOD Directive 3020.26 ("Department of Defense Continuity Programs"), the U.S. Army via Army Regulation (AR) 500-3 ("U.S. Army Continuity of Operations Program Policy and Planning").

2.2.1 BS 25999-1:2006

The standard provides two sections that address ICT Continuity Planning. Section 7.5 ("Technology") specifies that organizations should base their strategies upon the nature of the technology used and the services either delivered to the organization or provided by a third-party. These strategies could include "geographically spreading" the technology to ensure that a failure in one location does not impact the delivered service or function, holding older equipment as spares in the event of a system rebuild, and ensuring that replacement equipment is available to meet Recovery Time Objectives (RTOs). (The RTO is the longest time the business can do without a critical function before significant impact occurs).

Section 7.6 ("Information") specifies that strategies should exist to ensure that information is available within the timeframes established during the Business Impact Analysis (BIA). Specifically, the organization could ensure that information is stored at alternate locations, have arrangement with a third-party for escrowed storage of critical data such as vital contracts or private cryptographic keys, and ensuring that all necessary data is backed up per a policy-specified schedule.

2.2.2 DOD and Army Policy

DOD Directive 3020.26 does not address ICT Continuity Planning at the policy level directly. Rather, it states that "mission essential functions" (MEFs) must be identified by each organization via an impact analysis similar to the commercial BIA function and including a risk assessment to gauge the appropriate disaster response. Upon a COOP activation, identified MEFs must respond within a short time period (12 hours per the Directive). Vital records must be preserved; additionally, policy requires organizations to "Maximize the use of technological solutions to provide information to leaders and other users, facilitate decision making, maintain situational awareness, and issue orders and direction. Technology, information systems and networks must be interoperable, robust, reliable, and resilient" (p 2). DOD requires each implementing organization to define how this will be implemented.

2.2.2.1 Army Policy

Army policy via 500-3 is slightly more specific; it requires organizations to interact with the Chief Information Officer (CIO) of the G-6 to make maximum use of information technology (p 9). Additionally, "prepositioned information and duplicate emergency files" must be available within an emergency (such as remote storage of files and database replication). AR 500-3 refers the reader to AR 25-1 ("Army Knowledge Management and Information Technology") for more information; that publication refers the reader wishing to know more about IT Contingency Planning to review Department of the Army (DA) Pamphlet (Pam) 25-1-2 ("Information Technology Contingency Planning").

Once found, Pam 25-1-2 provides a rich source of material to the COOP practitioner seeking to define a policy-based ICT Continuity Plan and is of special interest to the Army Program use case highlighted by this series of

COOP planning papers. Major points from the Pamphlet include:

Table 1: DA Pam 25-1-2 Major Points

Major Point	Discussion
Tie into COOP Planning and BIA	The ICT Continuity Plan is not an independent document but a supporting structure to ensure that identified MEFs can continue their function.
Identify mitigation controls	These preventive, detective, and corrective controls avoid, reduce the impact, or reduce the duration of an outage either through an automated response or a generated alert for human response.
Define contingency strategies	Ensure that decision-makers understand their mitigation options so that the most cost-effective choices can be made.
Training and Test Schedules	A contingency plan that is not verifiably effective via trained team members is a negative asset to the organization due to the false sense of security it provides.
Establish backup procedures	Data must be available to meet RPO requirements.
Implement mitigation controls	Once selected, preventive, detective, and corrective controls must be verified to meet requirements. This is often done by establishing a baseline and performing an audit to check whether a particular control is meeting organizational expectations.
Establish alternate site	An alternate site can either be for quick failover (such as a "mirror" site that can respond instantly, or a "hot" site that can be activated in minutes to hours) or designed for slower response but long-term usage (such as a "cold" site that must have equipment trucked in and systems rebuilt before it can begin providing IT support functions). The goal is to reduce the organization's risk from a disaster to an IT processing center.
Exercises	All test plans, training courses, mitigation controls, and alternate sites must be exercised regularly and improvements noted.

2.2.2.2 Army Policy driven by Federal Policy

DA Pam 25-1-2 was not written in a vacuum; in keeping with this series' emphasis on both federal and DOD the reader must bear in mind that DA Pam 25-1-2 is an Army-tailored revision of the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-34 ("Contingency Planning Guide for Federal Information Systems"). In this author's opinion, the NIST publication is more current and more complete than the Army Pamphlet. Additionally, the key points from the Army Pamphlet above are specified almost identically in the NIST publication. This paper correlates both publications to help federal COOP practitioners in applying these papers to the wider federal community.

2.3 System Lifecycle

The Army and NIST both define ICT Continuity Planning in terms of the System Development Life Cycle (SDLC) as shown in the figure below:

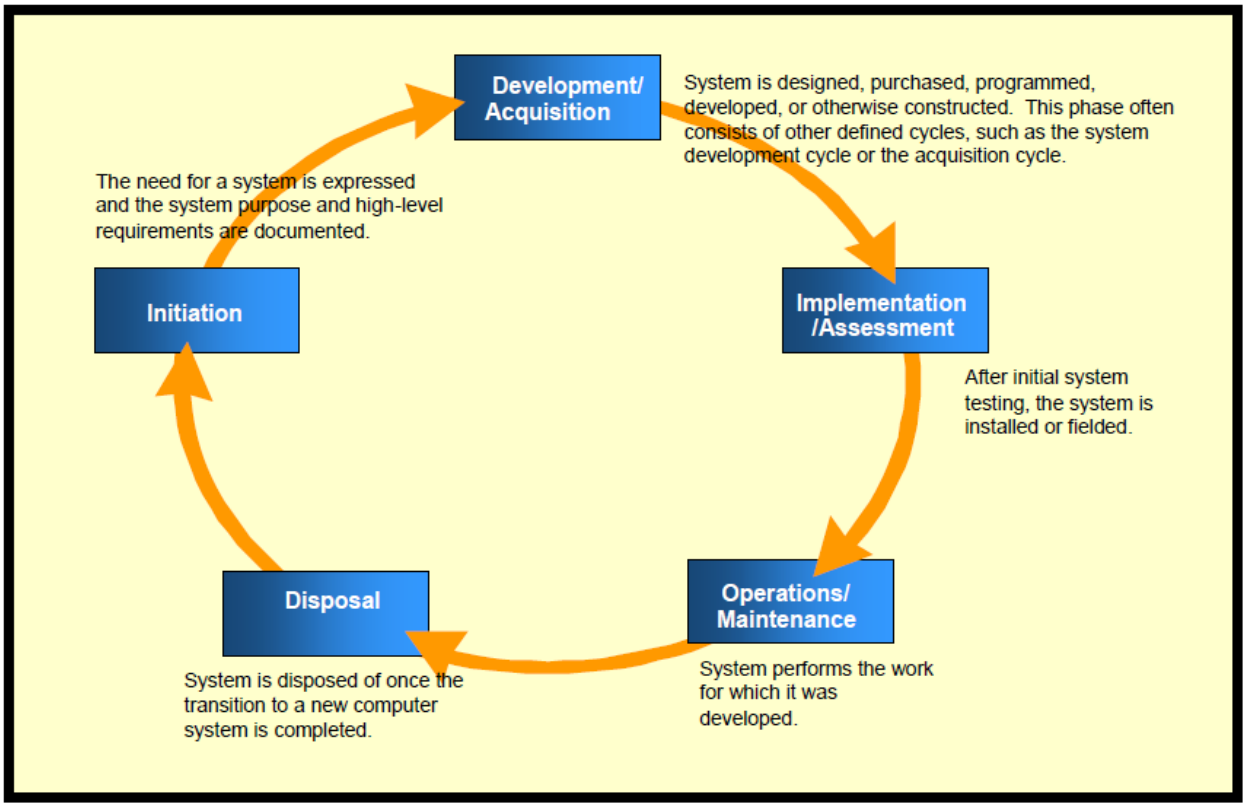

Figure 1: NIST SP 800-34 SDLC[1]

The DA Pamphlet applies the SDLC slightly differently than NIST (primarily in regards to referring to other Army resources), and it is useful to contrast the different phases between the two:

Table 2: SDLC Differences between NIST and Army[2]

Phase	NIST SP 800-34	DA Pam 25-1-2
Initiation Phase	Mission/business processes that the new information system will support should be evaluated to determine the users' recovery time requirement. High information system	Systems requirements are identified and matched to their related operational processes; the new IT system also is evaluated against all other existing and planned IT

[1] Source: SP 800-34, p 139.

[2] References are paraphrased from the documents. Within NIST SP 800-34, see "Appendix F: Contingency Planning and the System Development Life Cycle (SDLC)." Within DA Pam 25-1-2, see "Section 2-2: Information technology contingency planning and system development life cycle."

Phase	NIST SP 800-34	DA Pam 25-1-2
	availability requirements may indicate that redundant, real-time mirroring at an alternate site and failover capabilities should be built into the system design. Virtual applications may need to have "self-healing" capabilities.	systems to determine its appropriate recovery priority
Development / Acquisition Phase	Specific contingency solutions may be determined. The design should incorporate redundancy and robustness directly into the system architecture and ensure that contingency planning controls are appropriately addressed by the recovery strategy.	Where applications and systems are developed by a program manager, a standard method for contingency planning is provided to customers (see AR 70-1 and AR 70-75 for survivability requirements). Alternate site requirements are addressed in this phase.
Implementation Phase	The recovery strategy selected is now documented into the formal Information System Contingency Plan in coordination with the System Test and Evaluation effort. Tests / exercises may prompt modifications to the recovery procedures and the contingency plan.	Contingency strategies must be tested to ensure that technical features and recovery procedures are accurate and effective (requires a documented test plan).
Operation / Maintenance Phase	Users, administrators, and managers should maintain a test, training, and exercise program which continually validates the contingency plan procedures and technical recovery strategy via regularly scheduled tests.	Users, administrators, and managers maintain a training and awareness program that covers the contingency plan procedures. This includes regular tests, regular data backups, and updating the ICT Continuity Plan to reflect lessons learned.
Disposal Phase	Until the new system is operational and fully tested (including its contingency capabilities), the original system should be maintained in a ready state for implementation. As legacy systems are replaced, they may provide a valuable capability as a redundant system if a loss or failure of the new information system should occur. In some cases, equipment parts (e.g., hard drives, power supplies, memory chips, or network cards) from hardware that has been replaced can be used as spare parts for new operational equipment.	Until the new system is fully tested, accredited, and operational (including its contingency capabilities), the original system's contingency plan remains ready for implementation. The original system provides a valuable continuity backup capability!

As can be seen, the Army has very few differences from NIST's approach (mainly in the inclusion of the stricter accreditation processes inherent in running an information system on a military network). The Army COOP practitioner would be wise to use both references when determining an ICT Continuity Plan strategy.

3.0 ICT Continuity Plan Considerations

This section uses the major ICT Continuity Planning points from "Table 1: DA Pam 25-1-2 Major Points" to present a series of targeted analyses applicable to the Army Program use case. The careful reader will notice that the paper follows the SDLC identified both by DA Pam 25-1-2 and NIST SP 800-34, but that the Disposal phase is not addressed. A future paper will target this phase in more detail.

3.1 Plan (Initiation & Development / Acquisition Phases)

This section provides analysis on ICT Continuity Planning strategies of use to the COOP practitioner.

3.1.1 Tie into COOP Planning – BIA

The COOP Plan exists to ensure overall organizational *resilience* – the ability to quickly adapt and recover from any known or unknown changes to the environment (SP800-34, p 19). As the organization performs the BIA, it must be sure to include the information systems that support identified MEFs and the undergirding IT infrastructure for those information systems.

The Army Program needs to include subject matter experts (SMEs) with sufficient technical expertise such that the technical infrastructure can be fully identified along with the MEFs.

3.1.2 Identify Mitigation Controls

NIST recommends that COOP practitioners include the set of "CP" (Continuity Planning) controls from SP 800-53 ("Recommended Security Controls for Federal Information Systems and Organizations"). Within DOD, security controls are identified by Instruction 8500.2p ("Information Assurance (IA) Implementation") that defines 144 controls across 8 subject areas; these map to NIST's 205 control across 18 control "families." Although DOD does not currently use the NIST security controls, the Committee on National Security Systems (CNSS) published Instruction 1253 ("Security Categorization and Control Selection for National Security Systems") that instructs implementers to "refer to and use NIST SP 800-53, Section 3.3 for initial guidance on tailoring controls" (p 14) rather than the DOD 8500.2 controls.

The DOD and NIST Information Assurance (IA) controls can be mapped to each other, and this paper takes that approach in Section 3.3 Test (Operations and Maintenance Phase).

3.1.3 Define Contingency Strategies

NIST SP 800-34 defines six specific ICT Continuity Planning strategies for the COOP practitioner to consider:

- Define backup and recovery needs.
- Categorize systems based on Federal Information Processing Standard (FIPS) 199. This relates to the security categorization based on the system's impact to the nation and corresponds approximately to DOD's Mission Assurance Category (MAC) levels.
- Identify roles and responsibilities.

- Address alternate site needs based on RTO and RPO requirements.
- Identify equipment and cost considerations.
- Integrate into system architecture. This last is key to the Army Program as DA Pam 25-1-2 points out: "Agencies develop their IT contingency capabilities using a multiyear strategy and program management plan… A well-defined IT portfolio management and evaluation methodology for assessing continuity of operations and contingency planning as related to the existing baseline enterprise architecture should be well defined and understood. A lack of this understanding could result in a ***lack of funding***…" (p 11).

3.1.4 Training (Test) Schedules

DA Pam 25-1-2 exhorts COOP practitioners to implement training and test schedules into the ICT Continuity Plan: "Tests and exercises serve to validate, or identify for subsequent correction, specific aspects of IT contingency plans, policies, procedures, systems, and facilities used in response to an emergency situation. Periodic testing also ensures that equipment and procedures are maintained in a constant state of readiness. All agencies must plan and conduct tests and training to demonstrate viability and interoperability of IT contingency plans" (p 14).

Likewise, NIST SP 800-34 has similar language regarding Training, Testing, and Evaluation (TT&E): "Organizations should conduct TT&E events periodically, following organizational or system changes, or the issuance of new TT&E guidance, or as otherwise needed. Execution of TT&E events assists organizations in determining the plan's effectiveness, and that all personnel know what their roles are in the conduct of each information system plan" (p 41).

3.2 Implement (Implementation Phase)

This section provides analysis on how the COOP practitioner should implement the ICT Continuity Plan.

3.2.1 Establish Backup Procedures

Backup procedures should include:

- *Power* backup in addition to *data* backup; appropriately sized uninterruptible power supplies (UPS) to provide short-term backup power to all system components (including environmental and safety controls);
- Heat-resistant and waterproof containers for backup media and vital non electronic records;
- Offsite storage of backup media, non-electronic records, and system documentation;
- Frequent scheduled backups including where the backups are stored (onsite or offsite) and how often they are recirculated and moved to storage.
- NIST SP 800-34 goes further and provides implementation advice based upon the system's categorization level (impact to the nation upon failure):
- *Low-priority system (DOD MAC III; any outage with little impact, damage, or disruption to the organization).* Backup: Tape backup; Strategy: Relocate or Cold site.
- *Moderate-priority system (DOD MAC II; any system that, if disrupted, would cause a moderate problem*

to the organization and possibly other networks or systems). Backup: Optical backup, WAN/VLAN replication; Strategy: Cold or Warm site.

- *High-priority system (DOD MAC I; Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces).* Backup: Mirrored systems and disc replication; Strategy: Hot site.

3.2.2 Implement Mitigation Controls

The COOP practitioner must ensure that mitigation controls can be implemented cost-effectively and with available controls. This also may affect the control selection; for example, selecting a high-end intrusion prevention system that requires advanced configuration knowledge may not be practical from either a cost or a knowledge point of view.

Controls should be applied based on the model selected; within the federal space, this translates to using NIST SP 800-53 while in DOD (and the Army) it is DOD 8500.2p. Despite the control differences, the goal of any mitigation control is to ensure that disruptions are avoided if at all possible. For example, failures from electrical spikes can be avoided by inserting a power conditioner; failures from a downed power substation can be avoided by having two independent power lines entering the facility. Where a risk cannot be avoided, mitigating controls can reduce the impact of an occurrence (consider the case of automatic failover upon a disk crash). If an event occurs, then a selected control should be able to send an alert to a human being who can determine if escalation is warranted. Finally, corrective controls such as IT system auditing can ensure that continuous improvement is possible.

3.2.3 Establish Alternative Site

By far the most common conception of COOP is of a separate site (generally called "the COOP Site") that is designed to handle IT processing load upon a failure in the main site. Such a view is simplistic in the extreme as it looks only at the IT infrastructure aspect of failover and does not consider the organization as a whole. For example, what about the finance department, human resources department, or even the entire management structure? In a manufacturing model, a COOP site would of necessity either require its own manufacturing capability or alternate manufacturing sources would need to have been defined prior to the disaster.

Despite this common misperception of the COOP Site being "just about IT," the fact remains that no ICT Continuity Plan is complete without a careful analysis of the alternative IT infrastructure site options. DA Pam 25-1-2 defines five types of alternative sites as defined in the figure below:

Alternate site criteria selection

Site	Cost	Hardware equip-ment	Telecommunica-tions	Setup time	Location
Cold Site	Low	None	None	Long	Fixed
Warm site	Medium	Partial	Partial/full	Medium	Fixed
Hot site	Medium/high	Full	Full	Short	Fixed
Mobile site	High	Dependent	Dependent	Dependent	Not fixed
Mirrored site	High	Full	Full	None	Fixed

Figure 2: DA Pam 25-1-2 Alternate Site Types and Criteria[3]

[3] Source: PAM25-1-2, p 45.

DA Pam 25-1-2 defines these site alternatives as follows:[4] Cold sites typically consist of a facility with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support the IT system. Warm sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources. Hot sites are office spaces appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel. Mobile sites are self-contained, transportable shells custom-fitted with specific telecommunications and IT equipment necessary to meet system requirements. Mirrored sites are fully redundant facilities with full, real-time information mirroring; they are identical to the primary site in all technical respects.

The NIST publication uses the same five alternative site types and the same definitions. The choice of which site to use depends upon the cost-benefit analysis, and NIST provides a simple graphic to illustrate this:

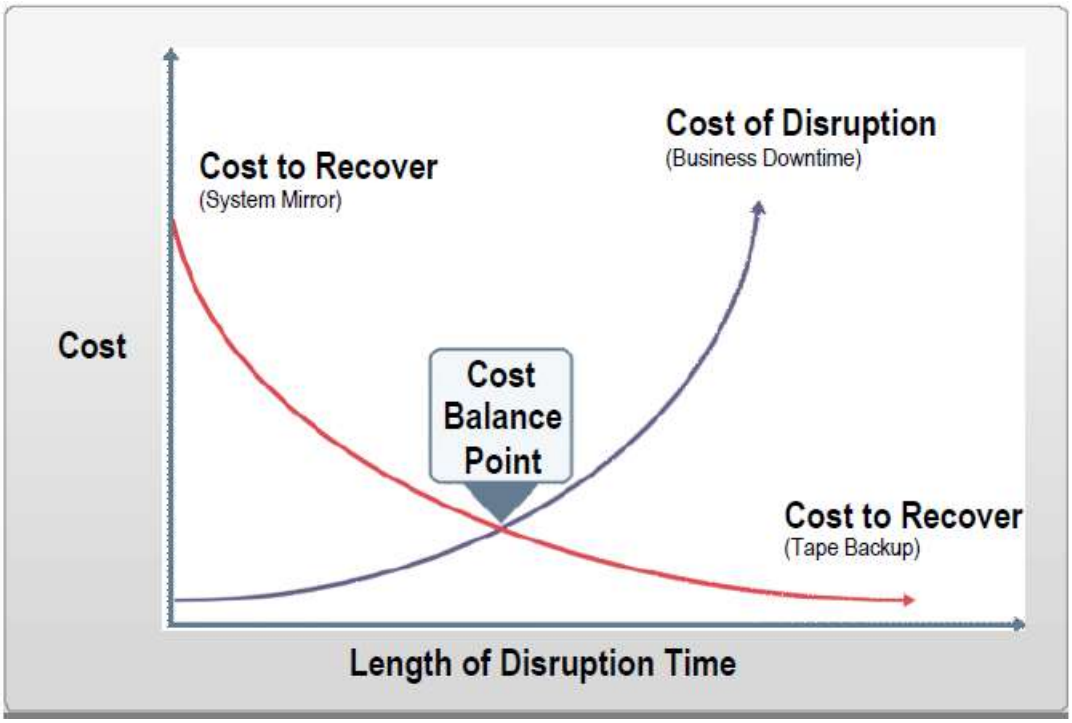

Figure 3: NIST SP 800-34 Cost Balancing for Alternative Sites

3.3 Test (Operations and Maintenance Phase)

This section provides analysis on how the COOP practitioner should test the ICT Continuity Plan.

3.3.1 Training

Within the Army Program use case, training familiarizes contingency staff members with the MEFs they may have to perform in an emergency (which also assumes that the ICT Continuity Plan has included contingency

[4] Adapted from the Pamphlet, p 45-46.

staff members). In fact, training must be regularly scheduled and run according to the ICT Continuity Plan requirements. DOD (and NIST) both require covered organizations to perform COOP training in general and IT DR training in particular at least once a year or at any significant change in the business. From the DA Pamphlet: "Team training should be conducted at least annually for IT contingency staffs on their respective IT contingency responsibilities" (p 14).

Training depends upon learning, and the DA Pamphlet has this to say (p 16):

- *Perform contingency training within a computer laboratory.* Virtual machine technology can be used to keep the cost down, and specific scenarios can be setup to emulate machine or facility failure.
- *Cross-train the contingency response team.* In an emergency, if the database expert is not available then it is not acceptable to lose the database. The way to avoid that is to ensure that redundancy exists not only in the hardware but also in the human beings making up the contingency plan. As an example, have network administrators build servers using the rebuild and recovery documents created by members of the server recovery team.

NIST emphasizes a slightly different view, with a focus on ensuring that recovery personnel understand their mission and roles. SP 800-34 identifies six different training goals (p 42):

- Understand the purpose of the plan;
- Facilitate cross-team coordination and communication;
- Establish reporting procedures;
- Define security requirements;
- Create team-specific processes (Activation and Notification, Recovery, and Reconstitution Phases); and,
- Define individual responsibilities (Activation and Notification, Recovery, and Reconstitution Phases).

The COOP practitioner can combine these approaches to create a thorough training approach and implementation.

3.3.2 Testing Controls (Exercise)

Both the NIST and the Army documents closely tie training with exercising the continuity strategy and implemented controls. In fact, a recognized training model is to perform a continuity exercise; most people have participated in this combined training / exercise model by way of the familiar fire drill.

NIST identifies two types of exercise techniques:

- *Tabletop.* This discussion-based technique has personnel meet in a classroom setting or in breakout groups. Led by a facilitator who presents a scenario, the participants answer questions related to the scenario and initiate a discussion related to roles, responsibilities, coordination, and decision making.
- *Functional.* This operational technique allows personnel to validate their operational readiness for emergencies by performing their duties in a simulated operational environment (thus, a *fire drill* is a functional exercise). This approach exercises procedures related to one or more functional aspects of a plan (e.g., communications, emergency notifications, system equipment setup). Functional exercises vary in complexity and scope, from validating specific aspects of a plan to full-scale exercises that address all plan elements.

Interestingly enough, the DA Pamphlet does not use the same terminology. It breaks up testing into the following (p 23): *table top* (similar to NIST); *system testing* (utilizing only a portion of the contingency response team and is limited to a specific system or process; useful for instituting new systems); *contingency rehearsal* (a full test of the installation's ability to manage a disaster scenario, and is time intensive and costly); and, *alert and notification* (call tree activation scenario; verifies telephone and cell phone numbers as well as the ability of each contingency team element to respond). This paper breaks up *contingency rehearsal* into its own category ("Section 3.2.3: Alternate Processing Site Recovery"), and the COOP practitioner should remember that the DA Pamphlet's communication structure (email and phone) does not include social networking alternatives such as Twitter, Facebook, or Army Knowledge Online.

3.3.3 Alternate Processing Site Recovery

The DA Pamphlet identifies *contingency rehearsal* as the most time-consuming and costly exercise. Within NIST SP 800-34, this same type of test is referred to only indirectly within its comments upon the SP 800-53 security control CP-4 ("Contingency Planning Testing and Exercises"). That security control applies the traditional commercial moniker: *full-interruption test* (p 133). Regardless of the terminology chosen, such a test is fraught with danger and is the gold standard of ICT Continuity Planning. In effect, the organization is emulating a complete disaster scenario *against production systems* to prove that failover and resilience exist to meet RTO and RPO requirements.

The DA Pamphlet applies this type of test primarily to the local Directorate of Information Management (DOIM) that provides network access to Army organizations (such as the Army Program use case specified by this paper). In the commercial world, a full-interruption test is caveated this way: "Not usually recommended as an appropriate testing approach because it requires interruption of actual production activities on a real-time basis."[5] In fact, neither NIST nor the Army goes into sufficient detail on the different types of exercises (checklist, structured walk-through, simulation, parallel, and full-interruption) so the COOP practitioner would do well to consider these exercise plans.

4.0 Concluding Remarks

4.1 Summary

This paper has analyzed how an ICT Continuity Plan can be implemented to support the organization's IT infrastructure. Within the federal government and the DOD, IT plays a critical part in delivering value to the Warfighter. Even relatively minor failures that affect the IT infrastructure can prevent the organization from accomplishing its mission.

This paper advocates for ICT continuity to be embedded as its own sub-plan within the overall COOP Plan as recommended by commercial, federal, and DOD policy as well as Army doctrine. By presenting a complete implementation strategy following the SDLC, even a small Army Program can receive cost-effective benefits from this approach and vastly improve continuity capabilities.

[5] Harold F. Tipton and Kevin Henry, "Business Continuity and Disaster Recovery Planning," *Official (ISC)2 Guide to the CISSP CBK*, Boca Raton, FL: Auerbach Publications: 2007 (pg. 385).

4.2 Recommendations

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

Table 3: Recommendations

Recommendation	Rationale
Make the ICT Continuity Plan a separate sub-plan within the COOP Plan	The COOP Plan should be arranged such that it is neither unwieldy nor hard to use in an emergency situation. It should clearly lead the reader into the required detail plan (for example: "Does the event affect computers? Then refer to the ICT Continuity Plan"). This allows better governance and easier change management by not bottlenecking all content through a single master plan.
Create ICT Continuity as a "capability"	Demonstrated expertise in managing disasters can provide a key differentiator for organizations within the public sector (not just the private sector). Scarce funding will be allocated to those groups who show that they have a solid plan in place for dealing with and recovering from problems.
Use the SDLC as the ICT Continuity Plan model	The SDLC represents the best-practice as defined both by the Army and NIST for preparing for IT disasters. Although not a hard requirements, the COOP practitioner would do well to apply the same model to ICT Continuity Plan development.
Refer to NIST SP 800-53 for mitigating controls	Although DOD has not *officially* migrated Instruction 8500.2p to the NIST family of security controls as specified within SP 800-53, that change is coming soon. Numerous DOD documents and online resources verify that the change to the NIST model will occur either in 2011 or 2013 at the latest. The wise COOP practitioner will prepare for this change ahead of time.
Do not forget to categorize systems	Within the federal space, the FIPS 199 categories on impact to the nation (low / moderate / high) should be used. Within DOD, systems should be categorized based upon their MAC level (I – least impact to deployed forces to III – significantly impacts deployed forces). The chosen level definitely affects the IT continuity and disaster recovery plan choices.
Consider that testing and training go hand-in-hand	Just as school fire drills both instruct individuals on how to react in an emergency situation as well as exercising the organization's ability to perform actions successfully, IT drills such as unplugging key routers or disabling critical databases combine response capabilities with the opportunity to educate team members on the continuity processes.

4.3 Next Steps

For a COOP Plan implementation to be successful, the COOP practitioner must manage team members from across the organization to produce the needed result: a verified and living COOP Program that uses feedback to improve continuously. This can be challenging because the COOP team members will have separate reporting lines of authority apart from their COOP duties; this can lead to friction and a lack of organizational efficiency. The next paper in this series examines how, within a small Army Program, the problems facing the COOP practitioner in leading the distributed COOP team can be addressed.

Appendix A: Acronyms and Abbreviations

AKO	Army Knowledge Online
AR	U.S. Army Regulation
BCM	Business Continuity Management
BIA	Business Impact Analysis
BS	British Standard
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
COOP	Continuity of Operations
CP	Continuity Planning
DA	Department of the Army
DOIM	Directorate of Information Management
DOD	Department of Defense
DR	Disaster Recovery
FIPS	Federal Information Processing Standard
G-6	Responsible for the information management function for the Department of the Army.
IA	Information Assurance
ICT	Information, Communications, and Technology
IT	Information Technology
MAC	Mission Assurance Category
NIST	National Institute of Standards and Technology
Rev.	Revision
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SME	Subject Matter Expert
TT&E	Training, Testing, and Evaluation
U.S.	United States

About the Author

Andrew Bruce is a Cloud Architect for D&SCI in the Army Programs group out of Aberdeen Proving Ground, MD. D&SCI 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 datacenter consolidation and cloud virtualization enterprise portfolio 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 as well as a Master's Degree in Information Assurance from Norwich University.

Reference List

[AR25-1] DA. October 24, 2007. Army Regulation 25-1: Army Knowledge Management and Information Technology. <http://www.apd.army.mil/pdffiles/r25_1.pdf>. Accessed: July 6, 2011. 142 p.

[AR25-2] DA. October 24, 2007 (Rapid Action Revision Issue Date: March 23, 2009). Army Regulation 25-2: Information Assurance. <http://www.apd.army.mil/pdffiles/r25_2.pdf>. Accessed: June 12, 2011. 103 p.

[AR500-3] DA. 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.

[BS25999] BSI. November, 2006. Business Continuity Management: Part 1: Code of Practice. London. 50 p.

[CNSS-1253] Committee on National Security Systems. October, 2009. CNSSI Instruction No. 1253: Security Categorization and Control Selection for National Security Systems. <http://www.cnss.gov/Assets/pdf/CNSSI-1253.pdf>. Accessed: July 7, 2011. 73 p.

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

[ITIL] ITIL. May 30, 2007. Glossary of Terms and Definitions. <http://www.get-best-practice.co.uk/glossaries.aspx>. Accessed: July 7, 2011. 55 p.

[PAM25-1-2] DA. November 16, 2006. Pamphlet 25-1-2: Information Technology Contingency Planning. <http://www.apd.army.mil/pdffiles/p25_1_1.pdf>. Accessed: July 6, 2011. 155 p.

[SP800-34] NIST. May 2010. SP 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems. <http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf>. Accessed: June 21, 2011. 149 p.