A WHITE PAPER

Federal Continuity of Operations

Part 6 of 10: Business Continuity Management (BCM) Response Plan Requirements

Topic Summary:

- Review the elements of a BCM response
- Analyze commercial and public sector guidance for BCM response
- Practical applications for a BCM response to a small Army Program
- Summary and Recommendations for next steps

Table of Contents

Illustration Index

Table Index

1.0 Introduction

Business Continuity Response planning identifies the necessary actions and resources to enable an organization to manage disruptions regardless of the cause. Within the commercial world, this response planning enables a complete Business Continuity Management (BCM) solution to provide organizational resilience and the ability to safeguard its reputation, brand, stakeholders, and value producing ability.

In the public sector, a Continuity of Operations (COOP) Program accomplishes much the same as BCM, with the aim of ensuring continuity of overall governmental functions rather than ensuring an agency's value-add capabilities. This paper analyzes how the equivalent of Business Continuity Response planning can be performed in the context of a small Army Program to demonstrate the opportunities that even small Department of Defense (DOD) and federal programs can leverage to help ensure their ability to accomplish their mission despite crisis conditions. The paper then summarizes its findings and presents practical recommendations for the reader.

2.0 Commercial and Public Sector BCM Response Practices

According to British Standard (BS) 25999-1:2006 ("A Code of Practice for Business Continuity Management"), which is used as a BCM standard throughout the world, the BCM Response consists of "various plan (s)… to identify, as far as possible, the actions that are necessary and the resources which are needed to enable the organisation to manage an interruption whatever its cause" (GPG08-4, p 4). This set of plans defines a full spectrum of disaster planning and coverage to prevent an organization, its people, its stakeholders, and its brand from harm even in the face of a serious disaster. This section highlights what these elements are and how they are interpreted within the commercial and public sector worlds.

2.1 The Elements of a Business Continuity (BC) Response

The BCM Response as described by BS 25999-1:2006 consists of a framework of individual plans that provides a tailored, executable, and verifiable organizational strategy to react to possible disruptions. However, this framework is not set in stone; take, for example, the interesting problem of the Incident Response Plan as compared to the Crisis Management Plan. Within BS 25999-1:2006, these plans are treated as synonyms (GPG08-4, p 5) and the use of the term *crisis* is even deprecated for its "negative connotations." As an alternative view still based strongly in good practice, The International Consortium for Organizational Resilience (ICOR) clearly delineates between Crisis Management (which should provide an overall emergency management structure) and Incident Management (which should execute as an operational function underneath Crisis Management). Neither ICOR nor BS 25999-1:2006 are strictly "wrong" or "right;" rather, they simply address the same problem (handling and containing a potential crisis) using different techniques.

This paper proposes the use of ICOR's interpretation as a baseline; the ICOR reading provides a reasonable and defensible approach that addresses all of the requirements identified by BS 25999-1:2006 in a straightforward manner. The following figure highlights the ICOR's interpretation of BS 25999-1:2006:

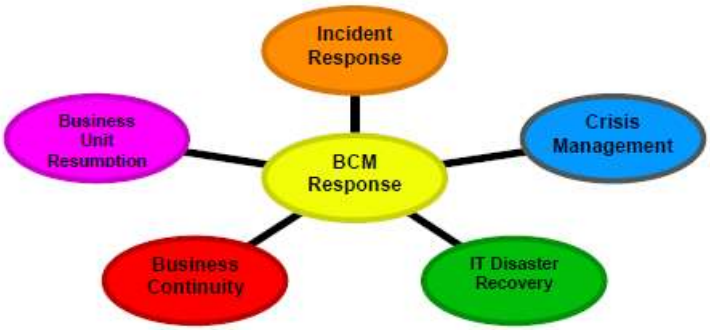

Figure 1: Elements of the BCM Response[1]

ICOR's five plan elements making up the BCM Response include:[2]

- *Incident Response Plan (IRP).* Also known as an Incident Management Plan (IMP) and within BS 25999-1:2006 identified as synonymous with the Crisis Management Plan (CMP), this plan specifies "how the strategic issues of a crisis affecting the organisation would be addressed and managed by the Executive."
- *Crisis Management Plan (CMP).* As implemented by ICOR, an authoritative plan that identifies a team composed of leaders from the BCM Steering Committee. The IMP falls under the authority of the CMP, and during an incident the Incident Response Team (IMT) reports to and receives direction from the Crisis Management Team (CMT). In the event of a full-blown emergency or disaster, the CMP specifies escalation capabilities and guides the activation of other plans.
- *IT Disaster Recovery Plan.* "The management approved document that defines the resources, actions, tasks and data required to manage the recovery effort. Usually refers to the *technology* recovery effort."[3] The National Institute of Standards and Technology (NIST) defines these technology-focused efforts as *contingency* rather than *continuity*.[4]
- *Business Continuity Plan (BCP).* "Pulls together the response of the whole organisation to a disruptive incident by facilitating the resumption of business activities." Upon the declaration of a disaster, the organization implements the BCP in order to facilitate both the continuation of providing added value as well as to start the process to return to normal operations.
- *Business Unit (BU) Resumption.* Also referred to within the BS 25999-1:2006 as an "Activity (Operational level) Plan," this plan "cover[s] the response by each department or business unit to the incident." Just

[1] Source: ICOR-6, p 16.

[2] Adapted from GPG08-4; direct quotes have quotation marks.

[3] Emphasis added by the author.

[4] SP800-34, p 21: "*Continuity planning* normally applies to the mission/business itself; it concerns the ability to continue critical functions and processes during and after an emergency event. *Contingency planning* normally applies to information systems, and provides the steps needed to recover the operation of all or part of designated information systems at an existing or new location in an emergency" (sic).

as the overall BC Response provides tailored guidance for the organization, the individual BU responses concentrate on the specific needs that units may have. For example, a manufacturing BU may require the continued ability to manufacture and deliver goods during a disruption while an outsourced helpdesk firm may require only telephony infrastructure.

2.2 Guidance within Army, DOD, and the Federal Government

Within the public sector, BCM is provided by a Continuity of Operations (COOP) Program; the government's focus on maintaining a "steady-state" in mission execution trumps any discussion retaining revenue. The U.S. Army Program exists as a uniformed branch of the Department of Defense, itself a functioning arm of the Executive branch of the federal government. Within even a small Army program, therefore, policy and implementation guidance on the BC response plan elements arrive from all three of these levels.

- *Army* – Army Regulation (AR) 500-3 ("U.S. Army Continuity of Operations Program Policy and Planning") provides the main source of guidance for the COOP practitioner working within the Army space. This document is driven by and refers to its authoritative DOD policy driver. Each of the BC Response plan elements has a corresponding element within AR 500-3 as identified below.
- *DOD* – Directive 3020.26 ("Department of Defense Continuity Programs") provides a high-level list of responsibilities and policy statements to ensure that "mission essential functions" (MEFs) are maintained to ensure the proper "continuity of government" (COG).
- *Federal* – While numerous publications exist on COOP, AR 500-3 explicitly states that the Federal Emergency Management Agency's (FEMA) Federal Preparedness Circular (FPC) 65 ("Federal Executive Branch Continuity of Operations (COOP)") as providing the "general requirements" for an Army-specific COOP Program as well as being a "good subject matter outline that will assist planners and writers of COOP procedures" (p 16).

The following section of this paper identifies how COOP practitioners can use this guidance to create a tailored BC response within the federal space.

3.0 Practical Application

The COOP practitioner must perform a significant amount of work to create a BC response. This section provides practical implementation suggestions while also correlating the commercial, federal, and Army versions of each of the plans making up the BC response. Where applicable, guidance from NIST (applicable to the entire federal government) is also provided.

3.1 Business Continuity Plan

As the overall management plan for business continuity, the BC Plan requires a structured and methodical approach to ensure that business functions can be continued and normal operations resumed as soon as possible. Therefore, the COOP practitioner should create this plan first.

Table 1: Business Continuity Plan Practical Implementation

Policy and Nomenclature	
BS 25999-1:2006	Business Continuity Plan
FPC 65	COOP Plan; Essential Functions Plan; Vital Records and Databases; Test, Training and Exercises Plan
AR 500-3	Basic COOP Plan, Annex A (Task Organization), Annex J (Command and Relationships), Annex T (Training and Exercises), Annex Y (Glossary of Terms), Annex Z (Distribution)
Practical Application	
General Guidance	Applied to Army Program Use Case
Prepare, coordinate, and maintain at least every two years and align to higher-level organizational policy.	Ensure that COOP funding requests support resource needs to meet DOD Directive 3020.26 requirements.
Coordinate continuity efforts with other groups.	Contact the Force Protection, Antiterrorism, and Critical Infrastructure Risk Management programs to ensure to reduce resource requirements.
Ensure that the plan is exercised at least annually.	See Army Regulations 11-33 and 350-28 for suggestions on how to conduct tests; these may be tabletop, functional, or full-scale exercises as directed by the senior Army representative.
Leverage technology as part of planning effort with tools and techniques to automate the plan.	Refer to the Chief Information Officer (CIO)/G-6 for current technology solutions; assist the CIO/G-6 in maintaining Army-wide redundant data communications capabilities to support MEFs.
Ensure vital documents are stored in a secure offsite location with verifiable access during an emergency.	FPC 65 breaks Vital Records down into its own sub-plan (“Vital Records and Databases,” cf. p 7). AR 500-3 simply requires “identifying, storing, protecting, and maintaining COOP emergency files, vital records, materials, and databases required to execute MEFs” (p 22). Technically speaking, storing vital records within a DECC would suffice.

3.2 Crisis Management Plan

The Crisis Management Team (CMT) provides overall guidance on an evolving emergency, and is generally located at a centrally-located Emergency Operations Center (EOC) separate from onsite Incident Management Teams (IMTs). The Crisis Management Plan provides a framework for activating and standing down individual IMTs, determining when to escalate ongoing incidents based on measurable impacts to the organization (e.g. "network downtime to exceed 175 minutes constitutes a network emergency"), and provides for the activation of other plans contained within the overall BCM Plan.

Table 2: Crisis Management Plan Practical Implementation

Policy and Nomenclature	
BS 25999-1:2006	Incident Response Plan *(ICOR differentiates)*
FPC 65	Delegations of Authority Plan; Orders of Succession Plan; Interoperable Communications Plan; Devolution of Control and Direction Plan
AR 500-3	Annex B (Threats and Intelligence), Annex E (Personnel and Administration), Annex F (Public Affairs), Annex J (Command Relationships), Annex K (Communications and Information)
Practical Application	
General Guidance	Applied to Army Program Use Case
Fully identify possible crises so that leading trends can be identified.	Use Force Protection Conditions (FPCON) to identify five possible crisis states from NORMAL (routine security posture) to DELTA (a hostile attack has occurred or intelligence indicates one is imminent).
Identify audiences that must be informed of changes, such as public media or key stakeholders. Plan for resilient information delivery methods.	Review with the CIO/G-6 to ensure that redundant communications links exist for notification of key stakeholders. Investigate the cost of the Government Emergency Telecommunications Service (GETS) for key stakeholders.
Ensure that both escalation decisions and stand-down decisions can be made.	Populate the Crisis Management Team with leaders from the Steering Committee. AR 500-3 calls for defining the "rules and procedures designated officials are to follow when facing issues of succession and rules for promulgating the changes" (p 17).

3.3 Incident Response Plan

Operating under the command and control of the Crisis Management Team (CMT), the Incident Response Team (IRT) is responsible for providing the first line of defense to all identified significant incidents to ensure that the CMT is informed and can escalate evolving incidents in a proactive and timely manner. The Incident Response Plan (IRP) defines the IRT members, the activation sequence, the CMT reporting structure, and the stand-down process for IRT members to follow based upon directions specified within the Crisis Management Plan.

Table 3: Incident Response Plan Practical Implementation

Policy and Nomenclature	
BS 25999-1:2006	Incident Response Plan
FPC 65	Human Capital Plan
AR 500-3	Annex Q (Medical Services)
Practical Application	
General Guidance	Applied to Army Program Use Case
Ensure that human life is top priority in any incident.	AR 500-3 speaks only indirectly to the responsibility that the IRP has for ensuring human safety. The COOP practitioner can refer to AR 385-10 ("The Army Safety Program") for a full set of procedures.
Care for persons affected by the incident and report injuries or missing personnel to the Crisis Management Team immediately.	As an operational arm of the Crisis Management Plan, the IRP must account for emergency supplies supporting safety: "bottled water (if authorized),[…] security guard force services,[…] commercial feeding, and medical services" (AR500-3, p 28).
Trained members must lead the IRT.	While a function of the basic COOP Plan (via training programs), each IRT needs to provide demonstrable proof of their ability to perform their function during an incident.

3.4 IT Disaster Recovery Plan

From an operational standpoint, Informational Technology (IT) Disaster Recovery falls into what NIST identifies as "contingency planning" rather than "continuity planning;" that is, IT exists to support MEFs (critical business functions) and not the other way around. This section includes the relevant NIST Special Publication (SP) to allow the COOP practitioner a thorough set of guidance.

Table 4: IT Disaster Recovery Plan Practical Implementation

Policy and Nomenclature	
BS 25999-1:2006	IT Disaster Recovery
FPC 65	Alternate Operating Facility(ies) Plan
NIST SP800-34	Contingency Planning Guide for Federal Information Systems
AR 500-3	Annex Q (OPSEC)
Practical Application	
General Guidance	Applied to Army Program Use Case
Provide a secure alternate location from which critical IT infrastructure can operate.	AR 500-3 includes much of what BS 25999-1:2006 labels IT Disaster Recovery within the basic COOP Plan. The COOP practitioner does well to use the detailed guidance within NIST SP 800-34. As an example, Sections 2.2.4 ("Critical Infrastructure Protection (CIP) Plan") and 2.2.8 ("Occupant Emergency Plan (OEP)") provide a full set of best practices to mitigate IT outages.
Maintain the confidentiality, integrity, and availability of necessary information.	AR 500-3 explicitly identifies IT disaster recovery as an operational function that must maintain operational security (OPSEC). From the Regulation: "COOP planning, execution, and operation utilizes OPSEC techniques to categorize vulnerabilities, and employ applicable countermeasures" as well as "[i]ntegrate COOP planning…with current OPSEC education and awareness training" (p 19) with the goal of "denying adversaries information about…capabilities and intentions" (p 35).
Ensure that trained personnel exist to operate IT equipment and processes.	Perform specialist cross-training as part of the mandatory COOP Exercise requirements.

3.5 Business Unit Resumption Plan

Individual business units (BUs) must have the capability of returning to normal operations based on a well-defined timeline. In this phase, business continuity occurs tailored to the specific BUs making up the organization.

Table 5: Business Unit Resumption Plan Practical Implementation

Policy and Nomenclature	
BS 25999-1:2006	Business Unit Resumption Plan
FPC 65	Reconstitution Plan
AR 500-3	Annex C (Operations), Annex D (Logistics)
Practical Application	
General Guidance	Applied to Army Program Use Case
Damage limitation and salvage	AR 500-3's emphasis on operations and logistics supports the need to have an adequate environment. This means that specific recovery teams must be provided for specialized to the equipment operated by a particular unit or combat brigade.
Define and resume normal business functions	From the Regulation: "[a]ctions in this phase enable the relocating staff to assume and commence MEFs from the ERF. Priority is given to executing MEFs." (p 15).
Consolidate business functions and stand down all emergency response teams	AR 500-3 defines the need for an Emergency Relocation Facility (ERF); this facility provides "critical requirements and procurement needs for command, control, communications & intelligence" such as prepositioned files, vital records, documents, software, databases, or other resources. The ERF serves as the foundation for the actual relocation effort.

4.0 Concluding Remarks

4.1 Summary

This paper has looked at the different approaches to crafting a Business Continuity Response from public- and private-sector views. In the private sector, the need to protect the business' revenue-generating functions biases the practitioner due to the simple fact that the business cannot survive indefinitely without earnings. The public sector is more concerned with its ability to ensure that a stable form of government exists than

strictly with a comparison of how much value has been earned. This is not to say that the private sector does not value supporting functions, or that the public sector has no concern for the cost-benefit ratio of a given continuity plan; in fact, this is far from the case. However, the differences between the two sectors' continuity approach can help the practitioner make wise decisions.

Within the public sector, FEMA's FPC 65 provide the basis for DOD's and the Army's continuity strategy. This paper looked at specific requirements specified by FPC 65 and related them to the Army and to other guidance from within the federal government (such as the NIST Special Publications). This correlation allows the Army Program use case to be presented with specific recommendations and approaches based on sound policy.

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 6: Recommendations

Recommendation	Rationale
Human life and safety is the most important aspect of any continuity plan.	Continuity plans only activate in a disaster scenario; people may be at significant risk depending on the type of incident that has occurred (example: terrorists, criminal activity, and natural disasters). The continuity plan must include specific steps to follow to account for *all* people (to include visitors and contractors).
Separate the concept of Crisis Management (high-level) from Incident Management (operational)	Crisis management allows the organization to have a single management construct for tracking and responding proactively to evolving issues. The ICOR approach of having a higher-level and strategic management team in addition to one (or more) operational and executive teams provides a useful abstraction layer as well as helping to ensure a *single message delivery mechanism* to stakeholders.
Integrate with other organizations to create a management response	Within the Army, the CIO/G-6 provides widely-available technology and process assessments; this makes CIO/G-6 a useful continuity management planning resource. Within the wider defense community, the Defense Information Systems Agency (DISA) provides detailed assurance guides that assist in maintaining operational security (OPSEC) throughout an incident or disaster.
Exercise plans regularly with trained individuals.	No continuity management response is complete without a funded and verifiable program exercise capability. An untested continuity plan gathering dust on a shelf is actually worse than no plan at all due to the false sense of confidence it generates. Even worse is having a plan and IRTs but not investing in the training required for IRT leaders to know their functions; chaos quickly results.
Know your stakeholders and how to reach them.	Stakeholders include one's workers, one's customers, and one's chain of command. These stakeholders need to be thoroughly identified prior to an incident; a communications plan is only effective if it delivers information to the right people. Using social media (Tweets, multiple email addresses, text messaging, online portals, and public media where appropriate) can aid critical information transmission in a resilient way.

Recommendation	Rationale
Know when to stand down	The continuity management response needs to define what "normal" means; at some point, the goal is to ensure that normal operations resumes. Start the plan by defining "normal" and close the plan by presenting the processes necessary for incident response and crisis management teams to disband.

4.3 Next Steps

The next paper in this series will identify which documents and plans need to make up the organization's BCM Response to ensure that continuity can be maintained and normal operations resumed as soon as possible. Properly handled, many incidents can be contained and prevented from transforming into a full-blown disaster. At some point, however, an incident may be declared an emergency (and in some cases like flood or fire, may start as an emergency). No BCM or COOP planning process would be complete without a discussion of how the incident response team handles an emergency, and the next paper in this series addresses how emergency communications should be implemented (using the Army Program use case as a practical example). This emergency management helps to ensure that the organization's most valued resource – its people and stakeholders – are kept informed and safe.

Appendix A: Acronyms and Abbreviations

AoA	Analysis of Alternatives
AR	U.S. Army Regulation
BCI	Business Continuity Institute
BCM	Business Continuity Management
BCP	Business Continuity Plan
BS	British Standard
BU	Business Unit
CIO	Chief Information Officer
CMP	Crisis Management Plan
CMT	Crisis Management Team
COOP	Continuity of Operations
DECC	DOD Enterprise Computing Centers
DISA	Defense Information Systems Agency
DOD	Department of Defense
EOC	Emergency Operations Center
ERF	Emergency Relocation Facility
FPCON	Force Protection Conditions
GETS	Government Emergency Telecommunications Service
GPG	Good Practice Guidelines
ICOR	The International Consortium for Organizational Resilience
IMP	Incident Management Plan *(Synonymous with Incident Management Plan)*
IRP	Incident Response Plan
IRT	Incident Response Team
IT	Information Technology
NIST	National Institute of Standards and Technology
OPLAN	COOP Operations Plan (*AR 500-3*)
OPSEC	Operational Security
SIPRNet	Secure Internet Protocol Routing Network

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

[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.

[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.

[GPG08-4] 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.

[ICOR-6] ICOR. 2009. Essentials of Business Continuity Management Series: BCM Plan Writing & Maintenance (Week 6 Reading). Lombard (IL). 78 p.

[SP800-34] NIST. May 2010. Special Publication 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.