A WHITE PAPER

Federal Continuity of Operations

Part 4 of 10: The Risk Assessment

Topic Summary:

- Analyze Federal, Department of Defense, and Army risk assessment policy requirements
- Integrate commercial risk assessment practices
- Complete a simple risk assessment against a process from a small Army Program
- Summary and Recommendations for next steps

Table of Contents

Illustration Index

Table Index

1.0 Introduction

A Risk Assessment allows the Continuity of Operations (COOP) Practitioner to analyze the prioritized Mission Essential Functions (MEFs) identified by the Business Impact Analysis (BIA) and to determine how best to ensure that those MEFs operate continuously despite hazards and threats. The Department of Defense (DOD) and the Army do not make this assessment easy; beyond simply requiring that commanders implement risk assessments as part of any command decision, tools and techniques are noticeable by their absence. This paper analyzes how a small Army Program can perform a Risk Assessment using a good-practice approach.

This paper starts by reviewing DOD and Army policy guidance in conjunction with commercial practices to create an assessment strategy. Next, the paper applies this strategy to a representative use case drawn from an operational system to demonstrate how a risk assessment can help to ensure the overall COOP posture of the program in a cost-efficient manner. The paper closes by summarizing its findings presenting recommendations for the program manager (PM) to review.

2.0 Risk Assessment Policy Guidance and Implementation Strategy

The risk assessment takes the output from the BIA and provides context for the organization to account for the forces that may exert interruptive, destructive, or devastating consequences on the critical business activities whether those forces are *threats* (man-made, such as terrorists or criminals) or *hazards* (natural, such as storms or fire). The risk assessment also recommends necessary mitigation controls by comparing existing organizational controls to the threat reduction requirements; in effect, performing a gap analysis.

A rigorous approach based on sound organizational risk management policy ensures the efficacy of the risk assessment and this section proposes a practical implementation framework based on federal, DOD, Army, and commercial practices.

2.1 Federal and DOD Guidance

At the federal level, the Federal Emergency Management Agency (FEMA), which executes under the aegis of the Department of Homeland Security (DHS), issued Federal Preparedness Circular (FPC) 65 (“Federal Executive Branch Continuity of Operations (COOP)”). FPC 65 addresses risk assessment only indirectly as part of Annex B (“Essential Functions”); the Circular states that “agencies should prioritize…functions against likely COOP triggers” and that the agency must “establish…resource[s]…and…other supporting activities needed to perform these functions within 12 hours, or less, of COOP activation” (p 17). The process of identifying COOP triggers (threats and / or hazards) in conjunction with the “supporting activities needed to perform these functions” (the mitigation controls) effectively requires a formal risk assessment to implement.

Within the DOD, Directive 3020.26 (“Department of Defense Continuity Programs”) explicitly requires Components to implement “risk-management assessments to ensure that appropriate operational readiness decisions consider the probability of an attack or incident and its consequences” (p 2). Furthermore, DOD Instruction 3020.42 (“Defense Continuity Plan Development”) goes further and requires “[r]isk assessments to identify and assess potential hazards or limitations relative to the location of the facility” (p 6-7) when selecting an alternate facility as well as an “executive decision process that allows for assessment of a threat, or potential

threat situation" (p 8) when planning for COOP response and recovery.

Unfortunately, these policy and procedure guidelines do not provide a methodology for an organization to use to implement a risk assessment.

2.2 Army Guidance

The Army is a DOD Component organization and has its own policy derived from the federal and DOD high-level policy drivers. A COOP Program relies heavily on information assurance (IA) for its implementation and the COOP Practitioner should begin with Army Regulation (AR) 25-2 ("Information Assurance") to see where COOP falls under the wider realm of overall facility and data protection. AR 25-2 starts by requiring a COOP Plan for every program or project, including non-essential programs and projects (p 8). Additionally, risk assessment responsibilities permeate every level within the Army organization and begin with the acquisition program; acquisition contracts must include statements to "reflect an initial risk assessment and…specify the required protection level" (p 24). Personnel (especially foreign personnel) must be subjected to a risk assessment (p 37), and any detected security breaches within a program must generate a risk assessment for presentation to the commanding officer (p 50).

Army's COOP policy can be found in Regulation 500-3 ("U.S. Army Continuity of Operations Program Policy and Planning"), which requires evaluation and assessment of MEFs (AR500-3, p 23) as well as whether "the precise characteristics of [a] threat require the further refinement of preplanned protective measures" (p 24). AR 500-3 references Army Field Manual (FM) 5-19 ("Composite Risk Management") is the authoritative Army risk management methodology; FM 5-19 states that its Composite Risk Management (CRM) methodology provides a five-step risk assessment process as shown below:

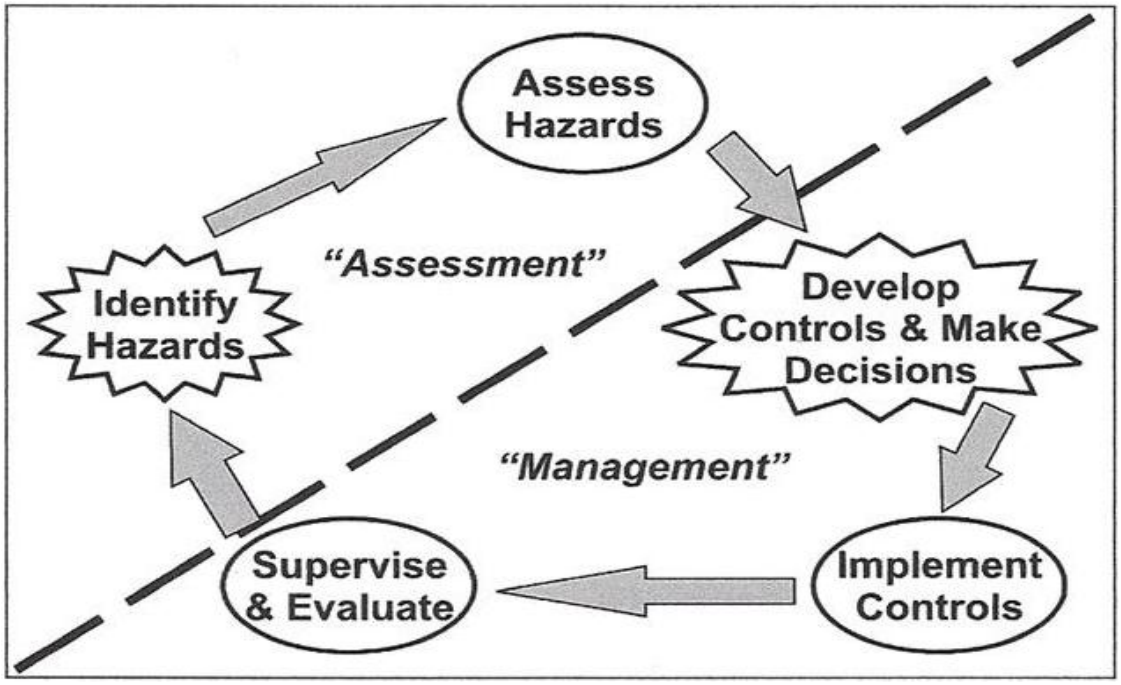

Figure 1: The Army's Five-Step CRM Process

These five steps within FM 5-19 follow a standard format: identify the hazards (BIA to identify the critical functions followed by initial hazard review by SMEs), assess the hazards (risk assessment), develop controls (also part of the risk assessment), implement controls (based on risk assessment results and approved changes), supervise and evaluate (to allow continuous improvement). FM 5-19 has a heavy focus on operational field activities to include enemy troop movements and possible actions which can at times be difficult to apply to purely administrative or support functions. To aid in this translation, the Manual provides a mapping facility between mission-specific activities vice general activities as shown in the table below:

Table 1: FM 5-19 Mapping between Mission-Specific and Nonmission-Specific Hazard Assessment[1]

Mission-Specific	Nonmission-Specific
Mission	Activity
Enemy	Disruptors
Terrain and Weather	Terrain and Weather
Troops	People
Time	Time
Civilian Considerations	Legal

One valuable artifact from FM 5-19 is the qualitative Risk Assessment Matrix shown below:

Table 2: FM 5-19 Qualitative Risk Assessment Matrix

RISK ASSESSMENT MATRIX						
		Probability				
Severity		Frequent A	Likely B	Occasional C	Seldom D	Unlikely E
Catastrophic	I	E	E	H	H	M
Critical	II	E	H	H	M	L
Marginal	III	H	M	M	L	L
Negligible	IV	M	L	L	L	L
E – Extremely High		H – High		M – Moderate		L – Low

FM 5-19's risk assessment matrix provides the COOP Practitioner with the guidance necessary to assess the impact ("I" to "IV" with "I" being catastrophic and "IV" being negligible) and the probability ("A" to "E" with "A" being frequent and "E" being unlikely).

[1] Adapted from the Manual by the author (FM 5-19, p 12).

2.3 Commercial Guidance

Within the commercial world, the British Standard (BS) 25999-1:2006 ("Business Continuity Management – Part 1: Code of Practice") has been widely used to ensure the Business Continuity Management (BCM) plans can be created and maintained to handle a wide range of possible threats and hazards. The Business Continuity Institute (BCI) publishes Good Practice Guidelines (GPG) that provide context and implementation specifications for the BS 25999-1:2006 standards; for risk assessment, these guidelines include an eleven-step process summarized in the table below:

Table 3: BS 25999-1:2006 Risk Assessment Mapped to the Army's FM 5-19[2]

BS 25999-1:2006 Risk Assessment Element		**Applied to Use Case (Army Program)**
Step	*Element*	
1	Tabulate a scoring system for impacts and probabilities and agree with project sponsor.	Based on FM 5-19, use the risk assessment matrix to agree with policy.
2	List threats to the urgent business processes determined in the BIA.	The MEFs serve as the "urgent business processes."
3	Estimate the impact on the organisation of the threat using a numerical scoring system.	Apply FM 5-19's risk assessment matrix to build a qualitative risk function.
4	Determine the likelihood (probability or frequency) of each threat occurring and weight according to a numerical scoring system.	Apply FM 5-19's risk assessment matrix to build a qualitative risk function.
5	Calculate a risk by combining the scores for impact and probability of each threat according to an agreed formula.	The completed FM 5-19's risk assessment matrix displays the threat matrix.
6	Optionally prioritise the risks according to a formula which includes a measure of the ability to control that threat.	FM 5-19's framework performs this in Step 3 ("Develop Controls and Make Risk Decisions"); it is a required step.
7	Obtain organisation sponsor's approval and sign-off of these risk priorities.	FM 5-19 states: "Risk decisions must always be made at the appropriate level of command or leadership based on the level of risk involved" (p 21). Within the Army Program use case, this is the local Commanding Officer or authorized deputy.
8	Review existing risk management control strategies noting where the assessed risk level is out of step with the current risk management strategies for that threat.	FM 5-19 identifies this step as "Reassess Risk" (p 20) and the goal is to develop a gap analysis after determining what controls should be implemented to enable the MEF to be fulfilled.

[2] Adapted from the GPG (p 13).

BS 25999-1:2006 Risk Assessment Element		Applied to Use Case (Army Program)
9	Consider appropriate measures to *transfer*, *accept*, *reduce*, or *avoid* risk.	FM 5-19 does not identify all of these strategies. The Commander is, by definition, accountable for a program's or project's MEF; that accountability cannot be transferred. Risks to an MEF can only be accepted based on higher-level guidance (p 48); furthermore, risk avoidance is an option only if the MEF will not be compromised in any way. This effectively leaves only risk reduction by means of mitigating controls.
10	Ensure that planned risk measures do not increase other risks. For example, outsourcing an activity may decrease some types of risk by increase others.	Commanders must ensure that supporting external functions as well as stakeholder organizations are identified and that risks are communicated.
11	Obtain the organisation sponsor's approval, a budget and sign-off for the proposed risk management control (s).	Relevant to the Army Program use case, FM 5-19 does not use the same wording or meaning. In the case of MEFs, risk decisions must be made based upon the chain of command. Simply put: an MEF must continue to function during a declared COOP. However, the cost-benefit analysis implied by the commercial approach should certainly be performed within the context of FM 5-19. Controls to ensure that an MEF continues functioning compete for funding with all other program requirements.

As can be seen, the commercial practices from BS 25999-1:2006 provide slightly more detailed steps than FM 5-19, but both methodologies can be used to construct a powerful risk assessment model for the COOP Practitioner to use.

2.4 A Practical Implementation Approach

For the purposes of the risk assessment performed by this paper a combination of BS 25999-1:2006 and FM-19 is used. The salient points become:

- Use the FM 5-19 risk assessment matrix for scoring risks.
- Identify threats and hazards to the MEF under investigation using subject matter experts (SMEs). Review available literature to determine the probability of the threat and / or hazard.
- Risk becomes a function of impact (levels 8, 4, 2, 1 to provide weighting) multiplied by probability (values from 1 to 5). Prioritize these risks based on their score.

- Determine existing controls that reduce or avoid the risk where the MEF is not compromised. Provide recommendations and costs for additional controls as necessary. Analyze the selected gap controls to ensure that they provide the best possible value.
- Submit the completed assessment to the Commanding Officer or authorized deputy.

These risk assessment steps, based upon solid policy and good-practice foundations, provide the COOP Practitioner with a straightforward and repeatable process that lends itself well to a standard spreadsheet representation.

3.0 Risk Assessment Applied

This paper performs a simple risk assessment on a single selected process to demonstrate the recommended steps. The output from this assessment is a completed spreadsheet; this spreadsheet is provided as a separate deliverable for the paper.

3.1 The Process to Assess

For this risk assessment, the process being assessed is the Change Control Board. This process is essential to the correct functioning of the Army Program because of the customer-facing nature of the work being performed. Three activities are addressed within the Change Control Board (CCB):

- CCB expertise to analyze changes
- The location where the CCB meets
- The communication between CCB members

The selected activities are not necessarily mission-essential, but they do represent how the risk assessment spreadsheet can be applied. As the project manager for the Army Program noted, "[t]his program has an active customer base which expects that agreed-upon changes occur based on what the commander said. The program's customers are not tied to the program; if they don't get the response and feedback they want then they start looking for other data providers. Good change management makes for happy customers."[3] The close reader will note the lack of Maximum Tolerable Downtime (MTD) as well as the lack of Recovery Time Objective (RTO) and Recovery Point Objective (RPO); for a true MEF these different values all begin to approach zero. (Otherwise the MEF would not be mission essential.)

[3] Source: Personal interview with the contractor's project manager, July 6, 2011.

3.2 Example Risk Assessment for CCB Activities

Example 1: Expertise loss due to loss of critical personnel (resignation, illness, death).

MEF	**CCB**						
Risk	**Expertise loss due to loss of critical personnel**						
Stakeholders	**Project management, Hosting facility**						
Risk Assessment Matrix			Probability				
			Frequent	Likely	Occasional	Seldom	Unlikely	
	Severity		A	B	C	D	E	**SCORE**
	Catastrophic	I	L	L	L	L	L	15
	Critical	II	L	L	L	M	L	17
	Marginal	III	L	L	M	L	L	18
	Negligible	IV	L	M	L	L	L	19
		E - Extremely High	H - High	M - Moderate	L – Low			
Existing Controls	**Cross-training and documentation to facilitate replacement**						
Additional Controls	**Appoint one "at-large" CCB member to be available on demand**						
Cost	**$2,400** 2 hours, 1x per month, 24 hours @ $100 / hour						

In this example, the stakeholders include project management because of the loss of effective change management as well as the hosting facility because approved changes cannot be promoted through the Development-Test-Production environment. The risk acceptance matrix indicates that it is most likely that this risk is negligible, but that it could be marginal (have some impact on operations). Some controls exist via cross-training and documentation; this could easily be enhanced by having an extra ("at-large") CCB member appointed to ensure continuity of the team if the risk occurs. A minimal cost is involved based on the expense of the additional CCB member for two hours per month.

Recommendation: Apply the control and appoint one additional CCB member.

Example 2: CCB cannot meet due to facility access issues.

MEF	**CCB**						
Risk	**Primary facility unavailable (classified material means remote work disallowed)**						
Stakeholders	**Project management, Hosting facility, Facilities personnel**						
Risk Assessment Matrix			Probability				
			Frequent	Likely	Occasional	Seldom	Unlikely	
	Severity		A	B	C	D	E	**SCORE**
	Catastrophic	I	L	L	L	L	L	15
	Critical	II	L	L	L	L	L	15
	Marginal	III	L	L	L	M	H	20
	Negligible	IV	L	L	L	M	M	18

		E - Extremely High	H - High	M - Moderate	L – Low		
Existing Controls	**None**						
Additional Controls	**Issue multi-level thin client CD that allows access to classified remote material; this technology available from DISA now (see http://www.trustedcs.com/documents/SOTrustedWorkstationSolTOv.pdf)**						
Cost	**$7,500** 5 CCB members, VPN setup, machine verification ($1,500 per member)						

Because the Army Program use case works with classified data, loss of venue for the CCB (for any reason) effectively means that change management stops within the program. This impact is marginal, but has been known to occur; not necessarily because the facility is unavailable but also because CCB members may not be able to access the facility. No controls currently exist to mitigate this risk; a simple solution featuring thin-client technology to create "virtual trusted workstations" can allow CCB members to establish an online quorum from trusted PCs running a completely private and secure remote workstation (see the link for more details). The cost is primarily in setting up the virtual private network (VPN) and to purchase the hardened CD-based virtual desktop image.

Recommendation: Due to the low impact and slightly higher cost, do not implement this control.

Example 3: CCB cannot communicate change instructions to the hosting facility.

MEF	**CCB**						
Risk	**Communications unavailable for notifying hosting facility of approved changes**						
Stakeholders	**Hosting facility**						
Risk Assessment Matrix			Probability				
			Frequent	Likely	Occasional	Seldom	Unlikely	
	Severity		A	B	C	D	E	**SCORE**
	Catastrophic	I	L	L	L	L	L	15
	Critical	II	L	L	M	M	L	20
	Marginal	III	L	L	L	H	L	21
	Negligible	IV	L	L	L	L	L	15
		E - Extremely High	H - High	M - Moderate	L – Low		
Existing Controls	**None**						
Additional Controls	**Provide duplicate collaboration portal that can be reviewed by hosting facility**						
Cost	**$12,500** Provision SharePoint VM on SIPRNet, define simple change mgmt list						

In this scenario, the CCB can establish a quorum and changes can be approved but communications with the hosting facility are not available. This has been known to happen; for example, when the designated point of contact within the hosting facility is not available. Due to the contractual nature of the hosting facility relationship to the Army Program within the use case, adding additional staff (or even cross-training) within the hosting facility is not an option. As mitigation, the Army Program can setup a collaboration portal where change

instructions can be issued using a business workflow; this ensures that approved changes are not overlooked simply because personnel to handle the change are not readily available within the hosting facility.

The higher price ($12,500) represents the license fee to setup the collaboration portal; as a side benefit, the Army Program can use this collaboration portal for other purposes unrelated to the CCB and gain return on investment due to increased overall productivity.

Recommendation: Despite the higher cost, if the Army Program can benefit from the collaboration portal then implement this change. The mitigated risk of communications with authorized points-of-contact within the hosting facility is a side-benefit that, by itself, would not merit the control.

4.0 Concluding Remarks

4.1 Summary

This paper has analyzed risk assessment requirements from the federal, DOD, and Army policy levels. Additionally, risk assessment techniques from the Army (FM 5-19) and the commercial world (BS 25999-1:2006) have been compared and applied to the Army Program use case. A straightforward and repeatable risk assessment process has been presented for use by the COOP Practitioner and demonstrated against a specific process within the Army Program use case.

The key to a successful COOP Program implementation within a smaller program lies in the ability of the COOP Practitioner to execute the elements (BIA, risk assessment, control implementation, and so on) into affordable mini-projects. Because smaller programs in DOD and the federal government rarely have an excess of funds to expend on formal COOP planning, the COOP Program must proceed incrementally. This demands discipline and tenacity on the part of the COOP Practitioner, but the results are well worth the effort when major problems do occur.

4.2 Recommendations

This paper has examined several methodologies for performing a Risk Assessment within the context of a COOP Program for a small Army Program and has provided a number of recommendations as shown in the table below:

Table 4: Recommendations

Recommendation	Rationale
Combine commercial and federal / DOD risk assessment methodology.	The commercial world's emphasis on cost-benefit analysis applies well to the public sector. Funding for mitigating controls competes for scarce resources in the larger program context, so delivering mitigation for the least cost is critical.
Establish a standard method by which to judge relative priority for risks based on impact and probability.	FM 5-19 provides a risk assessment matrix that can easily be used within a spreadsheet program to provide a straightforward weighting algorithm based on SME evaluation of specific risks.

Recommendation	Rationale
Always include cost in the risk assessment criteria.	The combination of impact, probability, and cost determine whether a particular risk is worth an identified control. The examples provided as part of this paper demonstrated how these three elements could be used in concert to determine whether a particular control should be recommended to mitigate a given risk.
Be cognizant of whether MTD, RTO, and RPO apply within the BIA and the risk assessment.	In the federal sector, an identified MEF must be continuously available; in effect, MTD, RTO, and RPO begin to approach zero. This is far different than in the commercial space where functions must specify how long they can be left unperformed before the organization is effected; within DOD, if an essential function is unavailable then in many cases it is assumed that the function is missed instantly. However, where that is not the case then the MTD, RTO, and RPO values are used within the BIA to establish the relative functional priority; this priority must be multiplied by the weighted risk assessment to ensure that mitigated risks demonstrate the greatest cost-benefit.

4.3 Next Steps

The next paper in this series will identify how the small Army program can use the output from the Business Impact Analysis and the Risk Assessment processes to construct a set of sound continuity strategies. The DOD in general and the Army in particular serve as executable agents on behalf of the nation's governmental functions; thus, an Army Program's prime directive must be its ability to execute its mission continuously.

Appendix A: Acronyms and Abbreviations

AKO	Army Knowledge Online
AR	U.S. Army Regulation
BCI	Business Continuity Institute
BCM	Business Continuity Management
BIA	Business Impact Analysis
BS	British Standard
CCB	Change Control Board
CO	Commanding Officer
COOP	Continuity of Operations
DHS	Department of Homeland Security
DOD	Department of Defense
FCD	Federal Continuity Directive
FEMA	Federal Emergency Management Agency
FM	Field Manual
FPC	Federal Preparedness Circular
GPG	Good Practice Guidelines
IA	Information Assurance
IT	Information Technology
MEF	Mission Essential Function
MTD	Maximum Tolerable Downtime
NIST	National Institute of Standards and Technology
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SME	Subject Matter Expert
U.S.	United States
VPN	Virtual Private Network

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

[AR25-2] Department of the Army. 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.

[AR385-10] Department of the Army. August 23, 2007 (Rapid Action Revision Issue Date: June 14, 2010). Army Regulation 385-10: The Army Safety Program. <http://armypubs.army.mil/epubs/pdf/R385_10.PDF>. Accessed: June 25, 2011. 138 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.

[FM5-19] Headquarters, Department of the Army. August, 2006. FM 5-19: Composite Risk Management. <https://armypubs.us.army.mil/doctrine/DR_pubs/dr_aa/pdf/fm5_19.pdf> (requires AKO login). Accessed: June 25, 2011. 108 p.

[FPC-65] Federal Emergency Management Agency. June 15, 2004. FPC 65: Federal Executive Branch Continuity of Operations (COOP). <http://www.fema.gov/pdf/library/fpc65_0604.pdf>. Accessed: June 25, 2011. 50 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.