

The George Washington University
Office of Public Safety and Emergency Management
Continuity of Operations Planning Checklist

Continuity of operations planning serves to identify critical job functions and identify alternative methods to maintain operations in the event of a disruption. Continuity planning should specifically address what the functions are, how they are done normally, realistic alternatives, recovery goals and processes, assumptions, communication methods and a system for implementing the plan.

A continuity of operations plan is a complement to a contingency plan, which serves to protect life safety. A large component of continuity planning lies in documenting "corporate memory". A continuity of operations plan is essential to the restoration and maintenance of an element's critical operations.

1. ORGANIZATION	YES	NO	COMMENTS
Does the plan state who it is designed to protect (department(s), number of persons, personnel names)?			
Is the plan organized and easy to understand, implement, and apply (uses headings, logical sequence, plain language)?			
Does the plan include, at a minimum, the elements included in this checklist?			
Is the plan an accurate reflection of the operations/functions it was written to protect?			
Does the plan include the date of revision?			
Does the plan align with the University's priorities of people, property, and vital interests?			
2. FUNCTIONS	YES	NO	COMMENTS
Does the plan identify the critical/key functions of the department?			
Does the plan break these tasks down to the most basic level and list them sequentially for restoration?			
Does the plan prioritize these functions?			
Are seasonal priorities taken into account? If not, is this stated?			
Has the plan accounted for personnel, work space, specialized equipment, and any department-specific considerations? <i>*A How-To Guide for assessing your IT readiness is available on the GW Campus Advisories page (Planning Guidance tab)</i>			
3. DEPENDENCIES & INTERDEPENDENCIES	YES	NO	COMMENTS
Does the plan account for services provided by other departments (e.g. ISS) and to other departments?			
Are there alternatives for these interdependencies?			

Have important contacts, vendors, contracts, etc. been identified to facilitate restoration and contact information included in the plan? <i>*Including vendor contact information is recommended as applicable</i>			
4. ALTERNATIVES	YES	NO	COMMENTS
Does the plan identify alternative methods for performing key functions in case of disruption?			
Are the alternatives realistic, (i.e. not cost or time prohibitive) and feasibly implemented?			
Does the plan indicate how long the department could continue operations without its usual resources (under ideal circumstances)?			
Are alternative methods to support operations identified in case there is a longer period of disruption?			
Are these alternatives also realistic?			
Does the plan include time estimates for restoration of functions in the short- and long-term? Are "short-term" and "long-term" defined?			
Has VPN access been established for critical personnel so that they can work remotely if needed, or alternatively, has data been backed-up and stored at a remote location (e.g. when appropriate, on a flashdrive at home)?			
5. RECOVERY	YES	NO	COMMENTS
Does the plan include steps (1 st , 2 nd , 3 rd etc.) for restoration of each key function?			
Does the plan identify those aspects of its key functions that can be restored in parts, if applicable?			
Have specific personnel been designated to handle restoration, and have back-ups been assigned?			
Has a process for procuring any necessary resources been identified?			
6. ASSUMPTIONS	YES	NO	COMMENTS
Does the plan include a complete list of (or otherwise clearly state) its assumptions?			
Are the assumptions realistic?			
If needed, have assumptions been made about the availability of key personnel during an incident?			
Does the plan avoid over-reliance upon unstated assumptions about another department or service?			
7. COMMUNICATIONS	YES	NO	COMMENTS
Do communication plans indicate methods for communicating both internally and externally?			

Are requirements for incident/emergency communication methods identified (<i>e.g.</i> a phone tree requires a contact sheet, working telephone, external phone line, and voice)?			
Have incident/emergency communication methods been comprehensively identified step-by-step (<i>e.g.</i> detailing a specific list-serv)?			
8. FINANCIAL COMPONENTS	YES	NO	COMMENTS
Does the plan identify procedures for financial management documentation in case of an incident? <i>*Refer to Annex X of the Incident Manual.</i>			
Does the continuity plan engage financial issues?			
If appropriate, has a cost estimate for restoration been conducted?			
9. IMPLEMENTATION	YES	NO	COMMENTS
Does the plan state a process for dissemination (<i>e.g.</i> discussion of plan at staff meetings, plan sent by departmental listserv, incorporated into new employee orientation)?			
Does the plan incorporate an annual schedule or system for review and updating (<i>e.g.</i> March of beginning of fall semester)?			
Does the plan assign responsibility to specific personnel for updating and maintaining the plan?			

ADDITIONAL NOTES: