Continuity of Operations Planning

A step by step guide for business

What is a COOP?

A Continuity Of Operations Plan (COOP) is a MANAGEMENT APPROVED set of agreed-to preparations and sufficient procedures for responding to a disaster.

Why is a COOP important?

The threats exist - 24hrs per day
You can't prepare AFTER a disaster happens
Your business cannot remain "idle"

Who needs to be involved?

EVERYONE

The COOP Process:

Pre-Planning

Project Initiation, Funding and Management.
Risk Assessment & Control
Business Impact Analysis

Planning

Develop Business Continuation Strategies
Plan Emergency Operations Site
Develop Continuity of Operations Plan

Post Planning

Training & Awareness
Exercising & Audit Plan
Maintain the Plan

I. Pre-Planning

Step One - Project Initiation, Funding & Management

Appoint project leader, if the leader is not the CEO.

- Identify and convene planning team representing each major area of the company.
- At the business unit level, set:
  Scope - the area covered by the disaster recovery plan
  Objectives - what is being worked toward and the course of action that the unit intends to follow
  Assumptions - what is being taken for granted or accepted as true without proof
- Set project timetable
- Draft project plan, including assignment of task responsibilities and resource requirements (people, equipment and $$'s if any)
- **Obtain CEO's approval of scope, objectives, assumptions and project plan**

Step Two – Risk Assessment & Control

To conduct a risk assessment, do the following:

- **Identify Vulnerabilities** for your facility or business (such as flood, tornado, hurricane, terrorist attacks, Hazmat event etc.)
- Review physical security (e.g. building access, ID requirements etc.)
- Review Insurance Coverage for identified major risks
- For hardware & software systems/activities supporting mission critical functions:
  - Assess probability of system failure or disruption
  - Review backup and power protection systems
  - Review data security and software backup procedures
  - Prepare risk and security analysis
  - Develop mitigation strategy for each major risk

Step Three –Business Impact Analysis

To complete a Business Impact Analysis, perform the following steps:

- Review Business Mission Statement
- Identify mission-critical business facilities, activities, functions, processes and hardware and software systems and identify personnel necessary to perform mission-critical tasks
- Identify mission-critical vendors & suppliers
- Analyze results to determine impact on Revenues or Service Delivery of loss of critical facilities, systems, applications, business processes or personnel and **prioritize results**

Vulnerability Analysis Chart

Your most vulnerable areas will be those with the highest total.

Type of Disaster	Human Impact	Property Impact	Business Impact	Internal Resources	External Resources	Total
	5 High Impact - 1 Low Impact			5 Weak - 1 Strong		
Prolonged Loss of AC Power						
Loss of Environmental Controls						
Hurricane						
Flood						
Tornado						
Earthquake						
Internal Structure Fire						
Wildfire						
Electrical Storm						
Breach of Security						
Interruptions of Internal Communications						
Interruptions of External Communications						
HazMat incident						
Transportation Accident (if within 5 miles of an airport)						
Terrorist Incident						

Business Impact Analysis Form

Department Name:

Activity:

What is the purpose of this activity?

Primary Contact Name for Function: **Phone:**

How would you classify this function or system?

Critical **Essential** **Necessary** **Desirable**

The categories detail the length of time that an activity can remain disrupted:

Critical *< 1 day -* ***Essential*** *2 - 4 days -* ***Necessary*** *5 -7 days -* ***Desirable*** *>10 days*

If this function were not performed following a disaster, would there be an impact on the following:

Operating Revenue	Contract Obligations	Client Satisfaction	Human Life
Laws Broken	Supply chain	Company Reputation	Jobs

For each column enter a score 1 through 4 and add to view total impact

	Revenue Loss	**Other Cost Impacts**	**Impact on Customers or Reputation**	**Impact on Company Personnel/Jobs**	**Total Impact**
1 Hour					
1 Day					
2 Days					
3 Days					
1 Week					
1 Month					

Business Impact Priority Worksheet

CRITICAL RESOURCE	Total Impact Assessment	Priority For Action	NOTES

II. Planning

Step Four - Develop Business Continuation Strategy

For each high-risk business area or facility:

- Identify vital records and plan to secure, relocate or replace them
  - HR
  - Clients
  - Contracts
  - Vendors
  - Etc. etc.
- Identify the minimum requirements to perform the critical function during a severe disruption
- Locate an alternative supply for critical inventory items
- Prepare a list of alternate vendors/suppliers of critical items outside immediate area
- Prepare a **Succession Plan** clear lines of authority
- Identify One Minute & Thirty Minute "**grab lists**" for each office

Step Five – Emergency Operations Site

For each business unit select a "hot" location, other than the normal facility, used to conduct critical business functions in the event of a disaster. Hot location must serve the highest priority business needs in the event that primary facility is not able to be occupied for whatever reason.

- Determine resource requirements for alternate facility
- Review cost/benefit of relocation versus temporary suspension of operations
- Identify potential alternative facilities and establish costs
- Evaluate and make recommendations
- Make selection and contract with hot relocation site

Step Six – Develop COOP

1. **Objective**
2. **Plan Assumptions**
3. **Criteria for invoking the plan**
   - Document emergency response procedures to occur during and a fter an emergency (i.e. ensure evacuation of all individuals, call the fire department, after the emergency check the building before allowing individuals to return)
   - Document procedures for assessment and declaring a state of emergency
     - Document notification procedures for alerting unit and university officials
     - Document notification procedures for alerting vendors
     - Document notification procedures for alerting unit staff and notifying of alternate work procedures or locations.
4. **Roles Responsibilities and Authority**
   - Identify unit personnel
   - Recovery team description and charge
   - Recovery team staffing
   - Transportation schedules for media and teams
5. **Procedures for operating in contingency mode**
   - Process descriptions
   - Minimum processing requirements
   - Determine categories for vital records
   - Identify location of vital records
   - Identify forms requirements
   - Document critical forms
   - Establish equipment descriptions
   - Document equipment - in the recovery site
   - Document equipment - in the unit
   - Software descriptions
   - Software used in recovery
   - Software used in production
   - Produce logical drawings of communication and data networks in the unit
   - Produce logical drawings of communication and data networks during recovery
   - Vendor list
   - Review vendor restrictions
   - Miscellaneous inventory
   - Communication needs - production
   - Communication needs - in the recovery site
6. **Resource plan for operating in contingency mode**
7. **Criteria for returning to normal operating mode**
8. **Procedures for returning to normal operating mode**
9. **Procedures for recovering lost or damaged data**
10. **Define a Testing and Training Regimen**
    - Document Testing Dates

- Complete disaster/disruption scenarios
- Develop action plans for each scenario

11. **Plan Maintenance**
    - Document Maintenance Review Schedule (yearly, quarterly, etc.)
    - Maintenance Review action plans
    - Maintenance Review recovery teams
    - Maintenance Review team activities
    - Maintenance Review/revise tasks
    - Maintenance Review/revise documentation

12. **Probable Appendices**
    - inventory and report forms
    - maintenance forms
    - hardware lists and serial numbers
    - software lists and license numbers
    - contact list for vendors
    - contact list for staff with home and work numbers
    - contact list for other interfacing departments
    - network schematic diagrams
    - equipment room floor grid diagrams
    - contract and maintenance agreements
    - special operating instructions for sensitive equipment
    - cellular telephone inventory and agreements

III. Post Planning

Step Seven – Training and Awareness

1. Share Details of the plan with key personnel on a need to know basis.
2. Share checklists and public information with all staff

Step Eight - Test and Audit the Plan

1. Develop test strategy
2. Conduct tests
3. Modify the plan as necessary
4. Establish periodic review and update procedures

Step Nine - Maintain and Update the Plan

1. Review changes in the environment, technology, and procedures
2. Develop maintenance triggers and procedures
3. Submit changes for systems development procedures
4. Modify unit change management procedures
5. Produce plan updates and distribute