



# **DEVELOPMENT OF INFORMATION SYSTEM CONTINGENCY PLANS**

## **A White Paper**

January 2011

This page intentionally left blank.

# Table of Contents

<b>1</b>	<b><u>INTRODUCTION.....</u></b>	<b><u>2</u></b>
1.1	ISCP Plan .....	2
1.2	Developing the ISCP Plan.....	2
<b>2</b>	<b><u>CONCLUSION .....</u></b>	<b><u>3</u></b>

## **1 INTRODUCTION**

---

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34 revision 1 was approved and signed this past May. This revision provides far more guidance for contingency plan development than its predecessor.

When developing an Information System Contingency Plans (ISCP) it is critical to remember that the purpose of this type of plan is to organize the recovery policies, requirements, and procedures for a single system into a single easy to follow document. Referencing other documents, spreadsheets, diagrams, etc., will make your plan difficult to use and, if the referenced documents reside on your network, they may not be available when you need them. Your ISCP should be easy to read, break down all tasks into manageable and traceable steps, and contain all of the information that you need to implement it.

### **1.1 ISCP PLAN**

The ISCP is a plan for the recovery of a single IT system. The following items must be included:

- Who will be in charge and devolution of authority should succession of authority become necessary;
- Facility characteristics and security;
- Criteria for plan activation;
- Actions to be taken; and
- Exercising/ Training

### **1.2 DEVELOPING THE ISCP PLAN**

The process for developing an ISCP is made up of six (6) steps:

1. Develop the contingency plan statement. This should already be in place and provide the authority and guidance for the development of all recovery-related plans. If your organization hasn't developed a Recovery Planning Statement, it would be a good idea to develop one and submit it up the chain for signature. The executive responsible for the overall recovery capability should sign the policy statement.
2. Conduct a Business Impact Analysis (BIA). Your organization should have conducted an overall BIA to identify and prioritize all functions performed, associated systems and enabling resources. A single system BIA should be used to:
  - Verify the system prioritization identified in the organization-wide BIA;
  - Prioritize system users to identify "power users"; and
  - Identify all essential components for recovering the system to its minimal operational configuration. (e.g., what is the least number of servers, infrastructure, workstations, etc., necessary to provide enough capability to "get by")

3. Identify preventive controls. Measures that you can take to either eliminate the risk of system loss or reduce the possibility that a threat will be able to either take down your system or degrade its capability below acceptable levels.
4. Determine Strategies. When selecting the strategy to implement, it's important to remember – “the shorter the Recovery Time Objective, the fewer strategies there are, and the more expensive those strategies are.” When selecting recovery strategies, planners should take into consideration recovery requirements for other systems and implement single strategies for multiple systems wherever possible.
5. Testing Training and Exercises. First, I recommend organizations refrain from using the term “testing”. Testing has the connotation of a pass/fail situation. The purpose of exercising the plan is to identify weaknesses in the plan and not if your staff can recover systems. If during an exercise it is determined that system recovery did not meet requirements, a flaw in the plan/documentation provided with the plan is apparent. Exercises should be conducted at least annually with a minimal reliance on table top discussions. You will never know if your plan will truly work when you need it if you don't actually implement your recovery capability. It is better to know what won't work then to place your faith in a “capability” that has never been truly exercised.
6. Plan Maintenance. Plans have a shelf-life of approximately 90 days. People are reassigned, organization missions change, equipment and software are recapped, operating environments change, and strategies change. Each of these situations will require an update to the plan. Implement tight version control and aggressive maintenance programs to ensure your plan will work when you need it.

## 2 CONCLUSION

---

Remember, the following key points:

- Keep it simple and easy to follow
- Don't assume you will be able to answer “TBD's” at the time of a disaster
- Make it one-stop-shopping for all of the information necessary to implement the plan
- Make it checklist centric to minimize confusion and maximize usefulness
- Keep it current
- Exercise it!