Global Information Assurance Certification Paper

CONTINGENCY PLAN

For a

Medium sized LAN residing on a Government WAN

"Appendix L of THE BASICS OF APPLYING THE DITSCAP TO DIVISION/CLASS C AND BELOW LEVEL SYSTEMS"

Prepared by:

John A. Keen

March 2003

Table of Contents

Abstract:

This paper will focus on Appendix L (Contingency Plan) of the basics of applying the Department of Defense (DoD) Information Technology Security Certification and Accreditation Process (DITSCAP) to DIVISION/CLASS C and below level systems. Systems that fall into Class C enforce a more thorough discretionary access control through user responsibility, logon procedures, etc.

The fictitious network that this Contingency Plan describes will be referred to as "XZY." XYZ is able to process sensitive but unclassified (SBU) data, and is comprised of 14 servers.

This contingency plan attempts to meet the Option 1 requirement as I feel a sound contingency plan must be in place to secure operations and information on a network. I also feel that this is an ongoing problem and must be addressed for the importance of showing the need for a good contingency plan.

1. Introduction

The systems comprising the XYZ network are designed to provide cradle to grave support for Air Traffic Control and Landing Systems in Military Operational Environments. In-Service engineering tasking provides the means that ultimately reduces life-cycle cost while providing a smooth and continuous flow of advanced technology to the fleet. Program support includes concept definition, system development, test and evaluation, acquisition, logistics, software development and product improvements.

In order to limit the loss of essential capabilities provided by the XYZ systems, a comprehensive contingency plan must be in place. This plan must spell out disaster procedures to be followed to regain and sustain the mission-essential capabilities of these systems in the event of a disaster or other contingency. All such procedures must be easy to understand and disseminated to all personnel essential to the recovery process.

A disaster is defined as an event that causes distress or sudden misfortune. A disaster, by definition, is a contingency. A contingency, however, is not necessarily a disaster. A contingency could simply be an undesirable event. While a contingency could disrupt XYZ mission-essential capabilities, a disaster could destroy those capabilities in a specific region. The central theme of the plan is to minimize the effect any contingency disaster will have upon ongoing operations. This Contingency Plan will be comprehensive and functional regardless of what type of event occurs. This plan contains the phone numbers of essential team members. It represents a dynamic process that is kept up-to-date through periodic scenario testing and reviews. As recommendations are received or new areas of concern are recognized, the Contingency Plan will be updated to address any emerging needs.

2. Purpose

The purpose of this contingency plan is to minimize the effects of an operational disruption by applying a strategy for the prompt recovery of XYZ mission-essential capabilities either locally or off-site in case of an undesired event.

3. Scope

This contingency plan applies to the impairment or disruption of normal operations of XYZ. It applies to situations ranging in severity from those that temporarily suspend operations to disasters that have widespread and lasting effect. In such an event, it addresses the personnel, preparations, backup resources, emergency reactions, and restoration procedures that are to be used to reestablish services.

4. Document Locations

This Contingency Plan will be printed and distributed to personnel essential to the recovery process. Copies of this plan should be safeguarded both at the office and the residences of personnel essential to the recovery process. When stored at an individual's home, the Contingency Plan shall be kept in a protected location to prevent its unauthorized disclosure. An adequate number of copies should be maintained on site. Additional copies (both on paper and diskette) should be located at the offsite storage facility.

XYZ Data Processing Environment Location(s):

- XYZ_NT1- Building 125
- XYZ_NT2- Building 125
- XYZ_Backup- Building 125
- XYZ_NT5- Building 125
- XYZ_Util- Building 125
- XYZ_NT6- Building 125
- CSS1- Building 125
- XYZ_LSTF- Building 125
- XYZ_NT3- Building 125

- N00421M132445- Building 125
- N00421M132497- Building 128
- H6DCS- Building 128
- 125 Monitor- Building 128
- XYZ_CSS- Building 128

5. Plan Initiation

All buildings that house XYZ servers are within military base confines. In a contingency event, building personnel shall contact one of the individuals listed below. These individuals are the only personnel who can initiate this Contingency Plan.

System Administrator 1……..301-123-0001
System Administrator 2……301-123-0002
Government POC A……301-123-0003
Government POC B……301-123-0004

Each XYZ site is required to keep a current recall roster on hand at all times in the event of any contingency scenario. It is the responsibility of the individuals above to determine, based on the severity of the event, whether the recall roster should be initiated.

6. Recovery Priorities

In the event a recovery scenario arises, XYZ_NT1, which is the Primary Domain Controller, (PDC) should be recovered first and foremost.

7. Essential Personnel Necessary to Restoring Operations

The following group of individuals has been identified as essential to restoring operations of the XYZ system. During a contingency event, these individuals shall be contacted to recover their respective systems.

Name	Specialty	Telephone Number
Mr. A	ISSO	301-123-0003
Mrs. B	System Administrator	301-123-0001
Mrs. C	System Administrator	301-123-0002

Only essential personnel are allowed on base in the event of a closure. The personnel listed above, along with any future additions, shall be designated, and identified through

the Webster Field Pass Office, as Key Essential personnel. This designation will ensure the access to Webster Field in order to initiate critical system recovery.

8. Contingency Events

Contingency events refer to varying degrees of loss across six major asset categories: Data, Software, Communications, Hardware, Personnel, and Facility. The primary concern with the contingency plan is the degree of loss, impact on the mission and techniques for coping with it.

A. Loss of Data

To protect against the event of data loss, XYZ performs daily full backups of system data.

DailyFull Back-Ups - Full backups are performed for all production machines each working business day. The tapes are stored at Building 125 and Building 128. Each Wednesday, the buildings swap backup data tapes in case of emergency.

Non-System Specific Data – The operating system (OS) is automatically backed up every two weeks.

Emergency Repair Disks – Emergency repair disks/intelligent disaster recovery disks are periodically updated for NT Servers.

B. Loss of Software

XYZ team members perform routine maintenance of all software. In the event of a loss of software other than routine, XYZ will reinstall and/or restore the software from the latest backup. XYZ maintains licensing rights to all software needed to restore the system; therefore a software vendor list does not apply.

C. Loss of Hardware

XYZ team members perform routine maintenance of hardware. In a contingency event, a decision shall be made, based on the type(s) of hardware failure, whether the affected hardware can be repaired or should be replaced. Items covered under warranty should be replaced at no cost to the Government. The estimated time for procurement of replacement hardware is one month. The XYZ project manager shall authorize any procurement of replacement hardware.

D. Loss of Communication

A loss of network communications shall be reported to the XYZ Help Desk at 301-123-2300. XYZ Help Desk support will respond accordingly.

Loss of communications can also apply to voice as well as data communications. If the telephone service for any XYZ function fails, personnel can contact the Base Telephone Office at 301-342-3104. The Base Telephone Office is physically located in Building 409, Room 104.

E. Loss of Key Personnel

Loss of key personnel as a result of illness, transfer, death, family emergency or a host of other events can have a serious impact on normal system operations. In the advent of a loss of personnel during a contingency event, written standard operating procedures (SOPs) exist on-site to complete an emergency shutdown of XYZ. The Emergency Shutdown Standard Operating Procedures for XYZ shall be co-located with this Contingency Plan (Enclosure 2).

As a long-term solution to loss of key personnel, XYZ shall hire and/or re-train in-house personnel to perform the tasks of those lost. As the focus of a contingency plan is primarily for the short term, alternate personnel will be assigned to key positions if there is a loss. In the event many key personnel are lost, it may be necessary to temporarily enlist other Government personnel or use contractor support. The use of SOPs will be critical in this contingency scenario.

F. Loss of Facility

Facility loss is typically due to some catastrophic action such as fire, flood, storm, earthquake, etc. Situations can range between temporary loss of power, failure of the air conditioning system, or loss of water to an event that renders the facility uninhabitable. It may be possible to simply wait out a short-term contingency such as a power failure or other minor interruption, or to accept the loss of a hardware component for the period of time required to obtain another through normal channels.

9. Implementation of Temporary Operations

In a contingency event, a "control center" may need to be established. System Administrators and management team members will initiate the steps necessary to reinstate operations from the new location. Ideally, the team would keep a log to aid in the preparation of status reports and to document the event for historical purposes. Working from procedural and recovery checklists (copies of which should be maintained with the back-up tapes and a copy of this contingency plan), they would proceed to:

- Assemble and verify availability of all necessary hardware, software, and resources at the back-up site.
- Install and test systems and applications software.
- Arrange for and test/verify full recovery of communications capabilities.
- Determine starting point for recovered operations.
- Restore latest back-up files.
- Alert the user community to status and potential gaps in data and/or changes in procedures (i.e., need to re-enter lost data, etc.).
- Restore operations and begin processing (with most critical applications first)
- Monitor and verify restoration is complete and that data integrity and continuity have been re-established.
- Resume full processing schedule.

10. Hot Backup Facility

XYZ currently has no Hot Backup Facility in place but does have the capability to back up the system if needed.

11. Restoration of Normal Operations

See #10 Above

12. Physical Security

During an undesired event, normal operating procedures may be significantly altered. Personnel and systems will be expected to function under conditions that would not be tolerated during normal circumstances. Security remains a requirement, but techniques must be altered to fit the contingency. At a minimum, the following will need to be accomplished:

- Arrangements shall be made to protect system equipment from unauthorized access.
- Accountability will need to be maintained for full back-up tapes.
- An inventory shall be conducted of functioning hardware and equipment.
- Transportation will need to be arranged for hardware and equipment to an alternate location.

13. Magnetic Swipe-Cards

Magnetic swipe cards are not required to gain entrance to any buildings housing XYZ servers. All server rooms that house XYZ resources are secured. An escort, usually the systems administrator is needed to gain access.

14. Testing the Plan

A. Monitoring

The following actions shall be accomplished whenever new systems are implemented, significant modifications occur, or annually. These actions shall be monitored as they relate to the contingency plan.

- Review critical applications to ensure integrity.
- Review alternate storage/operating requirements and procedures.
- Review and update roles and responsibilities of essential personnel.

B. Test and Evaluation

Contingency scenarios should be periodically simulated and this plan tested for accuracy and effectiveness. At a minimum:

- Collect back-up files and perform a recovery using them.
- Try operating with a minimum hardware configuration.
- Try operating with a minimum complement of personnel.
- Simulate using key files, programs, or services to see if the system can be recovered.

C. Update

As this plan matures and is tested over time, XYZ shall periodically review and make modifications to ensure its accuracy and efficiency. The contingency plan must be kept current to serve its intended purpose.

15. List of Enclosures

Enclosure 1 - Contingency Scenarios
Enclosure 2 - Emergency Shutdown SOP for XYZ Production Systems
Enclosure 3 – Bomb Threat Procedures
Enclosure 4 – Fire Safety and Procedures

Enclosure 1 - Contingency Scenarios

The following scenarios are presented to help reduce losses to or downtime of XYZ mission-critical data systems. During the initial stages of a disaster, it is essential that every employee, whether it be military, government, or contractor, know their role and is able to respond accordingly.

1. Scenario 1

Scenario 1 is damage but not destruction of XYZ buildings and/or equipment and the systems housed therein. Among the many events that could cause damage or negative impact to the systems includes:

- Air Conditioner Failure
- Fire
- Flood and Water Damage
- Power Outages
- Structural Damage

A. Air Conditioner Failure

A graphic temperature-and-humidity monitor or thermostat is located in all server rooms and operates 24 hours a day. The temperature should be checked each morning and periodically throughout the day. All buildings have air-conditioning units, the fans in these units will normally operate at all times to maintain the proper air flow. If one unit fails, another unit can usually carry the load for most processing, but only for a limited amount of time. The failing unit must be repaired as soon as possible.

The standard temperature for a computer room should be no more than 76 degrees. If the temperature rises above 76 degrees, take the following precautions.

1) Advise the Operations Supervisor that the temperature is above the normal operating range. The Operations Supervisor will need to notify the Maintenance Department (301-342-5117) for corrective action.

2) If the temperature rises above 84 degrees, the Maintenance Department must be notified immediately of the condition.

3) The System Administrators must commence powering down non-critical computers/servers per the guidance of the Emergency Shutdown SOP (Enclosure 2).

4) Computers and servers should not be powered-up without the approval of a System Administrator.

B. Fire Suppression

All XYZ sites are equipped with overhead water sprinklers and or hand held fire extinguishers that can detect and suppress fires within the first few seconds. Upon system activation, the Base Fire Department is automatically notified and will respond.

On-site staff shall notify essential recovery personnel. An assessment of the damage shall determine a contingency action.

Enclosure 4 contains fire safety procedures.

C. Flood and Water Damage

Flood and water damage can be caused from the discharge or leak in the sprinkler system, broken pipes, bathroom facilities, the flow of water into the computer room from another area because of fire, etc. The following steps should be followed if there is a water problem.

- Power down all computers, starting with the most critical, in accordance with the Emergency Shutdown SOP's.

- Cover all hardware with plastic covers stored in the computer room. All personnel shall know the location of these covers. If the covers are not immediately available, plastic trash bags will suffice.

An assessment of the damage shall determine a contingency action. The assessment will also indicate whether vendors need to be contacted for replacement equipment. The equipment should not be powered up without the approval of the System Administrator.

D. Power Outage

Two dimensions of downtime impact system availability during a power outage: frequency and duration. Power failures are the most common cause of abrupt system failures. Due to the likelihood of power outages from circumstances beyond XYZ control, XYZ has been equipped with an Uninterruptible Power Source (UPS), which are located on each server.

E. Physical Damage

Physical Damage to XYZ buildings can occur from hurricanes, tornados, terrorists, etc. The major risks are loss of power and damage to hardware that could result in the loss of data. The generator shall be brought online during loss of power due to physical damage. For hardware failures, The XYZ project

manager shall authorize any procurement of replacement hardware. Vendors may be called day or night to repair hardware. Lost data will be recovered from the locally stored, nightly backup tapes. In the event that local backup tapes are destroyed, backup tapes will be retrieved from the offsite storage facility.

2. Scenario 2

Scenario 2 is a chemical or biological disaster with no ability to access XYZ buildings.

In accordance with the Base Disaster Preparedness Office, any chemical or biological disaster is considered a HAZMAT situation. In the event of an actual or suspected HAZMAT situation, evacuate all personnel to at least 2000' feet upwind of the building and call the Fire Department (301-342-3911). The Fire Department will initiate appropriate HAZMAT procedures.

Once all the building occupants are evacuated, notify the personnel essential to recovery to determine if the system should be remotely administered or establishing new operations for XYZ.

3. Scenario 3

Scenario 3 is a natural disaster or terrorist action with destruction of XYZ sites but where personnel are still at full manning capability.

In this scenario, preparation of a new backup site operations center will begin immediately. Essential personnel shall be responsible for establishing a local control center and contacting all XYZ staff with instructions for alternate work locations.

4. Scenario 4

Scenario 4 is the destruction of any of the XYZ sites with loss of key personnel.

Enclosure 2 - Emergency Shutdown SOP for XYZ Production Systems

If an emergency situation arises, XYZ key personnel, time permitting, begin emergency shutdown procedures by first notifying all XYZ users of an imminent emergency shutdown. This is done in one or more of the following ways:

1. Building page
2. E-mail all XYZ users
3. Via the net send function which is provided by Windows NT 4.0

After XYZ users have been notified of the shutdown, key personnel begin powering down the XYZ network. There is no order in which servers are shut down and depending upon the estimated time of the outage Uninterruptible Power Supply (UPS) backup may need secured as well.

Enclosure 3 – Bomb Threat Procedures

Attached here would be bomb threat procedures as provided by the Base Command

Enclosure 4 – Fire Safety and Procedures

Attached here would be fire safety and procedures as provided by Base Command

References:

1.) DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP). December 30, 1997

2.) Plan for the Worst: Things that go bump in the night.
URL: https://public.afca.scott.af.mil/public/02jan/19jan.html

3.) Naval Surface Warfare Center. 3/25/03
URL: http://www.nswc.navy.mil/ISSEC/Form/DITSCAP/SSAA_Template.doc

4.) Department of the Navy (DoN)
URL: http://www.navres.navy.mil/navresfor/directivesCD/cnrf/52393.pdf

5.) Developing your contingency plan.
URL:
http://www.amc.army.mil/amc/ci/matrix/documents/white_papers/contingencyplan.pdf

6.) Symantec: Guide to Contingency Planning
URL: http://www.symantec.com/symadvantage/015/planning.html

7.) Streamlining DITSCAP Documentation
URL: http://www.tcs-sec.com/services/c_and_a/tcs_ditscap.pdf

8.) General Automated Data Processing (ADP) Manual
URL: http://www.tricare.osd.mil/Adp/C1S1.PDF

Last Updated: October 24th, 2017

Upcoming Training

SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event