

BCP/ITDR/RISK OVERVIEW FOR IT MANAGERS

FRIDAY, October 20, 2006



DoIT IT Security Division Services

✦ **Pandemic - Continuity of Operations [COOP]**

- loss of people

1. Business Continuity Planning [BCP]

- loss of Data Center
- loss of Agency facility

2. Disaster Recovery [ITDR]

3. Risk Management

Other Services Offered:

- **CSS, DNS, Proxy**
- **Firewall Services**
- **Incident Response**
- **Information System Logging**
- **Intrusion Prevention & Monitoring**
- **Investigations**
- **Security Audits**
- **Technical Evaluations**

Avian Influenza / Pandemic Planning Statewide Task Force Background

- **Avian Influenza Statewide Task Force**
 - DPH, DEP, Agriculture, DEMHS, DMHAS, UCONN, DAS and DOIT
- **Avian Influenza**
- Wild Bird - DEP
- Domestic Bird - Agriculture
- Testing - UCONN
- **Pandemic Planning**
- DAS is the lead
- DOIT has played a significant role
- 1.) In May CIO Wallace sent out Communications to all agency heads
- Distributing a Powerpoint presentation providing them a methodology to develop their own plans
- 2.) Nuala coordinated the establishment of Flu Watch Web site
 - <http://www.ct.gov/ctfluwatch/site/default.asp?>
- 3.) Joe Lapierre and Brian Mills developed a Web based bird mortality reporting application
 - <http://cfwwildbirdmortalityreporting.stag.ct.gov/>
- 4.) Established a statement of work with IBM to conduct initial Pandemic Planning training sessions that will be kicked off next Friday.

COOP Introduction

Avian Influenza normally infects waterfowl and can be transmitted to commercial poultry, particularly chickens and turkeys, by migrating birds.

There are 16 known subtypes of the avian influenza. The one called H5N1 is of particular concern because it adapts rapidly and can mutate to infect humans with a particular virulent and deadly strain.

COOP Introduction, continued

Flu Viruses are always changing, with new strains emerging. In order to become a Pandemic, two events must first occur:

1. **An animal flu virus (usually avian (bird)) must mutate or mix with a human virus.**
2. **That virus must change to become able to spread from human to human.**

If the new flu virus is different from those seen before by the living population, people do not have any immunity (resistance) to it, so it can spread quickly and become a pandemic.

COOP Assumptions:

- **Staff levels may be significantly impacted due to high levels of illness**
- **Remaining workers may be psychologically affected by disease, economic concerns, or fear and require employee assistance**
- **Staff may be reduced by the need for some workers to attend to family illness or children remaining home due to school closures.**
- **Human resource reductions may be temporary or may be long term depending on the severity of the influenza strain**
- **Staff may be lost due to significant mortality associated with the disease**

Continuity of Operations Planning: Overview

- 1. Assign Agency COOP/Disaster Recovery Owner and Leaders**
- 2. Identify all Business Processes for each location**
- 3. Validate Procedure Documentation**
- 4. Determine Recovery Time Objectives (RTO) based upon “worst case”**
- 5. Assign Recovery Priority**
- 6. Identify Primary Resources Supporting Each Function**
- 7. Pre-select Resource Pools Supporting each function during staffing shortages of 10%, 20%, 30% 40% and State closure**
- 8. Conduct Cross-Training Programs**
- 9. Devise Alternate Work Strategies**
- 10. Analyze Technology Impacts to implementation of alternate work strategies**
- 11. Identify Critical External Service Providers and Supply Chains**
- 12. Create and test internal/external Communication Plan**
- 13. Publish Delegation of Authority Plan**
- 14. Announce Agency Succession Plans**
- 15. Address Availability of Vital Records Management**
- 16. Develop Alternate Site Strategies, as appropriate**
- 17. Return to Normal Operations After a Crisis**

COOP Planning: NIMS

- **Pandemic Response, as with any other State response to a crisis, is to align with the Governor's order to execute National Incident Management System (NIMS) protocols and responsibilities.**
- **NIMS will enable all agencies to interact effectively with:**
 - The State of Connecticut's Emergency Operation Center (EOC), which will be invoked by DEMHS should an Avian Flu epidemic strike and
 - Other Agencies which are cooperating in the response to the crisis
- **Key NIMS positions at each SITE include:**
 - "Incident Commander" – person in charge
 - "Operations Section Chief" – person responsible to oversee critical functions
- **Some NIMS positions will be handled at the Agency level:**
 - "Public Information Officer" (agency communications / media)
 - "Legal Counsel"
 - "Human Resources Officer"
 - "Finance Officer"
- **These NIMS positions will have a parallel partner at the EOC / State Level**

Business Continuity Planning [BCP]

Scenarios:



Loss of DoIT Data Center



Loss of Agency Building or Facility

“NIMS” Compliancy

Business Impact Analysis

BCP Template now available

<http://www.ct.gov/doitservices/cwp/view.asp?a=2693&Q=321714>



Plan Development

Plan Maintenance [HIPAA Agencies]

How to engage DoIT to develop your Business Continuity Plan (BCP)

Agency actions:

- Review DoIT-provided BCP template to better understand what a BCP is comprised of
- Request a sizing estimate from DoIT [currently billed at hourly rates]
- Assess estimate
- To proceed, determine Agency funding source
- Provide written request to DoIT IT Security requesting BCP service
 Conduct Business Impact Analysis
 Business Continuity Plan Development
 [current hourly rates ... subscription rates still to be determined]

DoIT actions:

- Draft an MOU for Agency signature
- Engage resources to conduct Agency BCP sizing estimate
- Provide resulting plan development estimate to Agency
- Engage resources to begin development of BCP
- Eventually amend the MOU with BCP Subscription pricing once it has been developed

Information Technology Disaster Recovery [ITDR]

“Facilitate the recovery of technical capabilities at an alternate site”

Our Disaster Recovery Plan Goes Something Like This...



DILBERT
By Scott Adams

Hot Site Subscription

IBM Business Continuity and Resiliency Services at Sterling Forest, NY

DoIT owned and administered [at DoIT]

Mainframe

Enterprise Storage & Backup

Exchange

Network Infrastructure [testing only]

Firewalls

DNS

Distributed Systems [requiring enhanced Infrastructure]

Agency owned and DoIT administered [at DoIT]

Agency owned & Agency administered [at DoIT]

Agency owned & Agency administered [at Agency]

How to participate in Distributed Systems Hot Site testing

Send in written request to DoIT IT Security specifying:

- (a) the application(s) you wish to test
- (b) the hardware/software configuration required for the test
- (c) your Agency's agreement to cover:
 - associated hot site subscription charges,
 - commitment to subscribe to ITDR services, which require having the following completed prior to commitment for activated ITDR support:
 - 1) Completion of a recovery assessment
 - 2) Development of a comprehensive ITDR plan

DoIT will then:

- (a) obtain subscription pricing for components
- (b) draft an MOU for Agency signature
- (c) engage resources to begin ITDR development for the agency
- (d) eventually amend the MOU with ITDR Service pricing once it has been developed

Risk Management

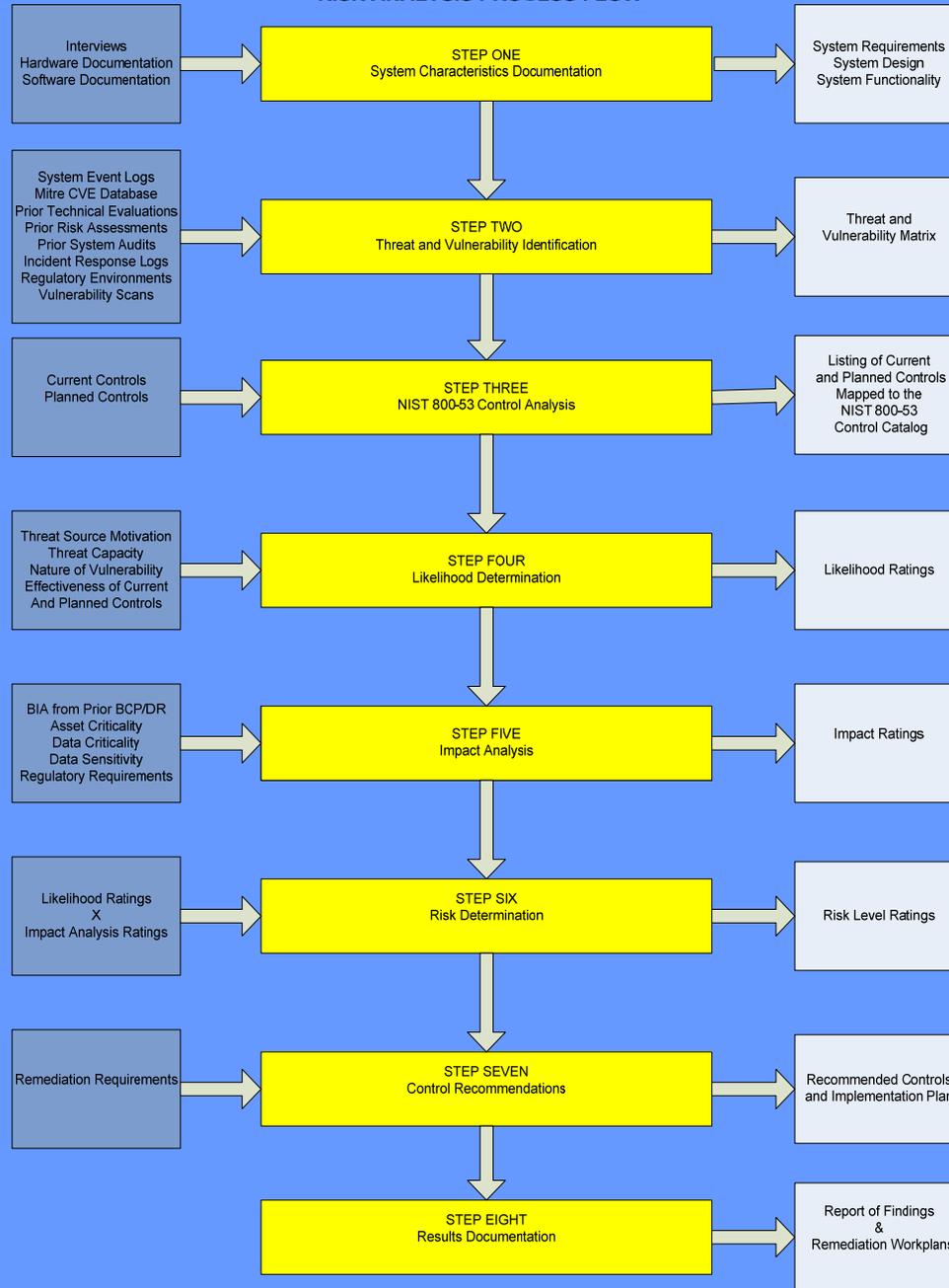
IT Security Risk Management:

- Organizations manage risk on a daily basis
- IT Security is a Risk Management discipline
- Cornerstone of RM is a systematic Risk Analysis
- An IT Risk Analysis is a collaborative initiative (not an audit)

Risk Analysis Process:

- Identify all threats and related vulnerabilities
- Document all current and planned controls
- Evaluate the effectiveness of these controls
- Highlight the success of specific control investments
- Establish the impact of a threat occurring
- Determine the overall risk level for each threat
- Determine whether to remediate, transfer or accept specific risks

RISK ANALYSIS PROCESS FLOW



IT Risk Analysis

Risk Analysis Benefits:

- Provides organizations with a relative measure of their current IT risk profile
- ITSD Risk Analysis methodology scales from a single system to the entire enterprise
- IT Security budgetary decisions are framed within a comprehensive cost-benefit paradigm
- Provides an effective measure of the overall impact of specific IT security initiatives
- An iterative life cycle process providing meaningful benchmarks and progress tracking

Risk Management Partnerships:

Risk Analyses undertaken in a collaborative manner, leverages the synergistic potential of Risk Management Partnerships between IT Security Professionals and their client agencies

This in turn creates an environment whereby the return on investment for all IT Security initiatives can be maximized