

TEL2813/IS2820
Security Management

Contingency Planning

Jan 13, 2005



Contingency Planning

Things which you do not hope happen
more frequently than things which you do
hope.

-- PLAUTUS. (C. 254–184 B.C.), *MOSTELLARIA*,
ACT I, SCENE 3, 40 (197)



Introduction

- Planning for the unexpected event, when the use of technology is disrupted and business operations come close to a standstill
- Procedures are required that will permit the organization to continue essential functions if information technology support is interrupted
- Over 40% of businesses that don't have a disaster plan go out of business after a major loss



What Is Contingency Planning?

- The overall planning for unexpected events is called contingency planning (CP)
- It is how organizational planners position their organizations to prepare for, detect, react to, and recover from events that threaten the security of information resources and assets
- Main goal: restoration to normal modes of operation with minimum cost and disruption to normal business activities after an unexpected event



CP Components

- Incident response planning (IRP) focuses on immediate response
- Disaster recovery planning (DRP) focuses on restoring operations at the primary site after disasters occur
- Business continuity planning (BCP) facilitates establishment of operations at an alternate site



CP Components (Continued)

- To ensure continuity across all CP processes during planning process, contingency planners should:
 - Identify the mission- or business-critical functions
 - Identify resources that support critical functions
 - Anticipate potential contingencies or disasters
 - Select contingency planning strategies
 - Implement selected strategy
 - Test and revise contingency plans



CP Operations

- Four teams are involved in contingency planning and contingency operations:
 - CP team
 - Incident recovery (IR) team
 - Disaster recovery (DR) team
 - Business continuity plan (BC) team



Contingency Planning

- NIST describes the need for this type of planning as

"These procedures (contingency plans, business interruption plans, and continuity of operations plans) should be coordinated with the backup, contingency, and recovery plans of any general support systems, including networks used by the application. The contingency plans should ensure that interfacing systems are identified and contingency/disaster planning coordinated."

Contingency Planning

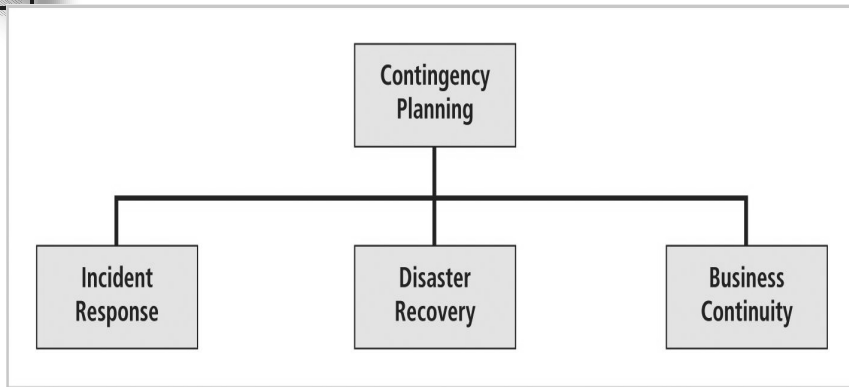


FIGURE 3-1 Contingency Planning Hierarchies

Incident Response Plan

- IRP:
 - Detailed set of processes and procedures that anticipate, detect, and mitigate the impact of an unexpected event that might compromise information resources and assets
- Incident response (IR):
 - Set of procedures that commence when an incident is detected



Incident Response Plan (Continued)

- When a threat becomes a valid attack, it is classified as an information security incident if:
 - It is directed against information assets
 - It has a realistic chance of success
 - It threatens the confidentiality, integrity, or availability of information assets
- It is important to understand that IR is a reactive measure, not a preventive one



During the Incident

- Planners develop and document the procedures that must be performed during the incident
- These procedures are grouped and assigned to various roles
- Planning committee drafts a set of function-specific procedures



After the Incident

- Once the procedures for handling an incident are drafted, planners develop and document the procedures that must be performed immediately after the incident has ceased
- Separate functional areas may develop different procedures



Before the Incident

- Planners draft a third set of procedures, those tasks that must be performed in advance of the incident
- Include:
 - Details of data backup schedules
 - Disaster recovery preparation
 - Training schedules
 - Testing plans
 - Copies of service agreements
 - Business continuity plans

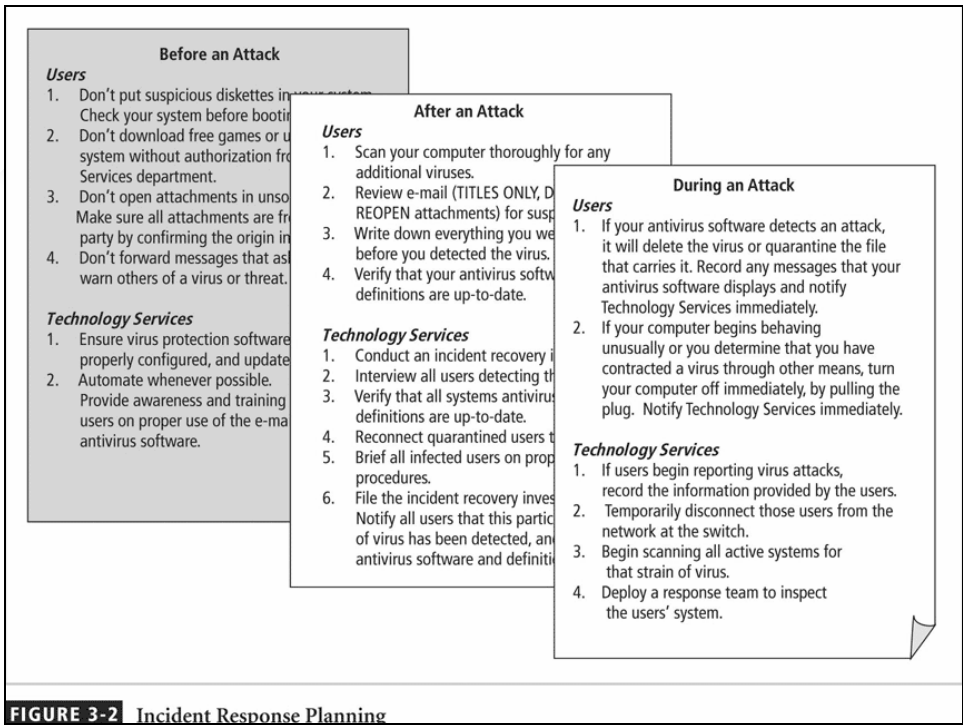
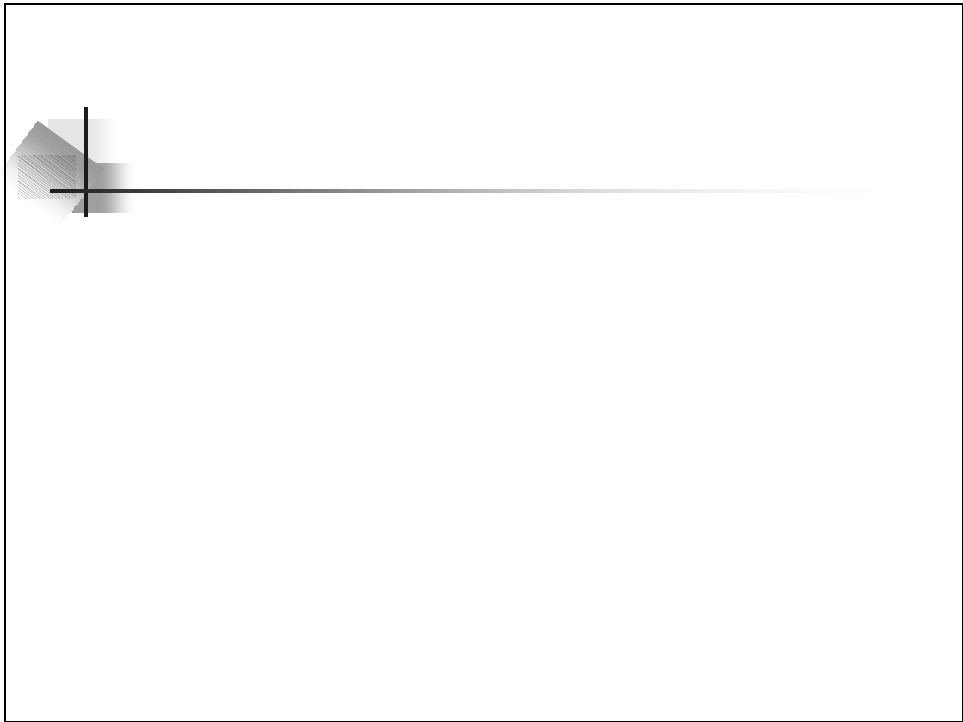


FIGURE 3-2 Incident Response Planning



Preparing to Plan

- Planning requires detailed understanding of information systems and threats they face
- IR planning team seeks to develop pre-defined responses that guide users through steps needed to respond to an incident
- Pre-defining incident responses enables rapid reaction without confusion or wasted time and effort



Preparing to Plan (Continued)

- IR team consists of professionals capable of handling information systems and functional areas affected by an incident
- Each member of the IR team must:
 - Know his or her specific role
 - Work in concert with each other
 - Execute the objectives of the IRP



Incident Detection

- Challenge is determining whether an event is routine system use or an actual incident
- Incident classification: process of examining a possible incident and determining whether or not it constitutes actual incident
- Initial reports from end users, intrusion detection systems, host- and network-based virus detection software, and systems administrators are all ways to track and detect incident candidates
- Careful training allows everyone to relay vital information to the IR team



Incident Indicators

- Probable Indicators
 - Presence of unfamiliar files
 - Presence or execution of unknown programs or processes
 - Unusual consumption of computing resources
 - Unusual system crashes
- Probable Indicators
 - Activities at unexpected times
 - Presence of new accounts
 - Reported attacks
 - Notification from IDS
- Definite Indicators
 - Use of dormant accounts
 - Changes to logs
 - Presence of hacker tools
 - Notifications by partner or peer
 - Notification by hacker



Occurrences of Actual Incidents

- Loss of availability
- Loss of integrity
- Loss of confidentiality
- Violation of policy
- Violation of law



Incident Response

- Once an actual incident has been confirmed and properly classified, the IR team moves from detection phase to reaction phase
- In the incident response phase, a number of action steps taken by the IR team and others must occur quickly and may occur concurrently
- These steps include notification of key personnel, the assignment of tasks, and documentation of the incident



Notification of Key Personnel

- As soon as incident is declared, the right people must be immediately notified in the right order
- Alert roster: document containing contact information of individuals to be notified in the event of actual incident either sequentially or hierarchically
- Alert message: scripted description of incident
- Other key personnel: must also be notified only after incident has been confirmed, but before media or other external sources learn of it



Documenting an Incident

- As soon as an incident has been confirmed and the notification process is underway, the team should begin documentation
 - Should record the who, what, when, where, why and how of each action taken while the incident is occurring
- Serves as a case study after the fact to determine if right actions were taken and if they were effective
 - Can also prove the organization did everything possible to deter the spread of the incident



Incident Containment Strategies

- Essential task of IR is to stop the incident or contain its impact
- Incident containment strategies focus on two tasks:
 - Stopping the incident
 - Recovering control of the systems



Incident Containment Strategies

- IR team can stop the incident and attempt to recover control by means of several strategies:
 - Disconnect affected communication circuits
 - Dynamically apply filtering rules to limit certain types of network access
 - Disable compromised user accounts
 - Reconfigure firewalls to block problem traffic
 - Temporarily disable compromised process or service
 - Take down conduit application or server
 - Stop all computers and network devices



Incident Escalation

- An incident may increase in scope or severity to the point that the IRP cannot adequately contain the incident
- Each organization will have to determine, during the business impact analysis, the point at which the incident becomes a disaster
- The organization must also document when to involve outside response



Initiating Incident Recovery

- Once the incident has been contained, and system control regained, incident recovery can begin
- IR team must assess full extent of damage in order to determine what must be done to restore systems
- Immediate determination of the scope of the breach of confidentiality, integrity, and availability of information and information assets is called incident damage assessment
- Those who document the damage must be trained to collect and preserve evidence, in case the incident is part of a crime or results in a civil action



Recovery Process

- Once the extent of the damage has been determined, the recovery process begins:
 - Identify and resolve vulnerabilities that allowed incident to occur and spread
 - Address, install, and replace/upgrade safeguards that failed to stop or limit the incident, or were missing from system in the first place
 - Evaluate monitoring capabilities (if present) to improve detection and reporting methods, or install new monitoring capabilities



Recovery Process (Continued)

- Restore data from backups as needed
- Restore services and processes in use where compromised (and interrupted) services and processes must be examined, cleaned, and then restored
- Continuously monitor system
- Restore the confidence of the members of the organization's communities of interest



After Action Review

- Before returning to routine duties, the IR team must conduct an after-action review, or AAR
- AAR: detailed examination of events that occurred
- All team members:
 - Review their actions during the incident
 - Identify areas where the IR plan worked, didn't work, or should improve



Law Enforcement Involvement

- When incident violates civil or criminal law, it is organization's responsibility to notify proper authorities
- Selecting appropriate law enforcement agency depends on the type of crime committed: Federal, State, or Local
- Involving law enforcement has both advantages and disadvantages:
 - Usually much better equipped at processing evidence, obtaining statements from witnesses, and building legal cases
 - However, involvement can result in loss of control of chain of events following an incident

Incident Response and Disaster Recovery

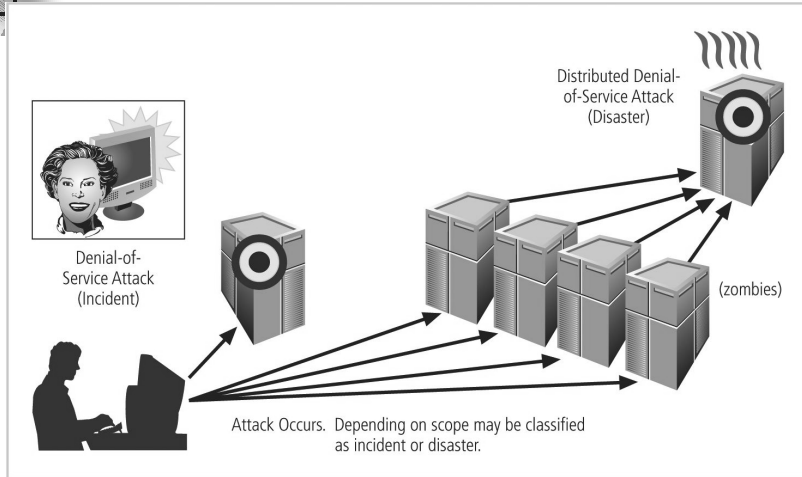


FIGURE 3-3 Incident Response and Disaster Recovery

Disaster Recovery

- preparation for and recovery from a disaster, whether natural or man made
- In general, an incident is a disaster when:
 - organization is unable to contain or control the impact of an incident
 - OR
 - level of damage or destruction from incident is so severe, the organization is unable to quickly recover
- Key role of DRP: defining how to reestablish operations at location where organization is usually located



Disaster Classifications

- A DRP can classify disasters in a number of ways
- Most common method: separate natural disasters from man-made disasters
- Another way: by speed of development
 - Rapid onset disasters
 - Slow onset disasters



Planning for Disaster

- Scenario development and impact analysis are used to categorize the level of threat of each potential disaster
- DRP must be tested regularly
- Key points in the DRP:
 - Clear delegation of roles and responsibilities
 - Execution of alert roster and notification of key personnel
 - Clear establishment of priorities
 - Documentation of the disaster
 - Action steps to mitigate the impact
 - Alternative implementations for various systems components



Crisis Management

- Set of focused steps taken during and after a disaster that deal primarily with people involved
- Crisis management team manages event:
 - Supporting personnel and their loved ones during crisis
 - Determining event's impact on normal business operations
 - When necessary, making a disaster declaration
 - Keeping public informed about event
 - Communicating with outside parties
- Two key tasks of crisis management team:
 - Verifying personnel status
 - Activating alert roster



Responding to the Disaster

- Actual events often outstrip even best of plans
- To be prepared, DRP should be flexible
- If physical facilities are intact, begin restoration there
- If organization's facilities are unusable, take alternative actions
- When disaster threatens organization at the primary site, DRP becomes BCP



Business Continuity Planning (BCP)

- Ensures critical business functions can continue in a disaster
- Most properly managed by CEO of organization
- Activated and executed concurrently with the DRP when needed
- Reestablishes critical functions at alternate site (DRP focuses on reestablishment at primary site)
- Relies on identification of critical business functions and the resources to support them



Continuity Strategies

- Several continuity strategies for business continuity
 - Determining factor is usually cost
- Three exclusive-use options:
 - Hot sites
 - Warm sites
 - Cold sites
- Three shared-use options:
 - Timeshare
 - Service bureaus
 - Mutual agreements



Exclusive Use Options

- Hot Sites
 - Fully configured computer facility with all services
- Warm Sites
 - Like hot site, but software applications not kept fully prepared
- Cold Sites
 - Only rudimentary services and facilities kept in readiness



Shared Use Options

- Timeshares
 - Like an exclusive use site but leased
- Service Bureaus
 - Agency that provides physical facilities
- Mutual Agreements
 - Contract between two organizations to assist
- Specialized alternatives:
 - Rolling mobile site
 - Externally stored resources

Off-Site Disaster Data Storage

- To get any BCP site running quickly, organization must be able to recover data
- Options include:
 - Electronic vaulting: bulk batch-transfer of data to an off-site facility
 - Remote Journaling: transfer of live transactions to an off-site facility
 - Database shadowing: storage of duplicate online transaction data

Disaster Recovery and Business Continuity Planning

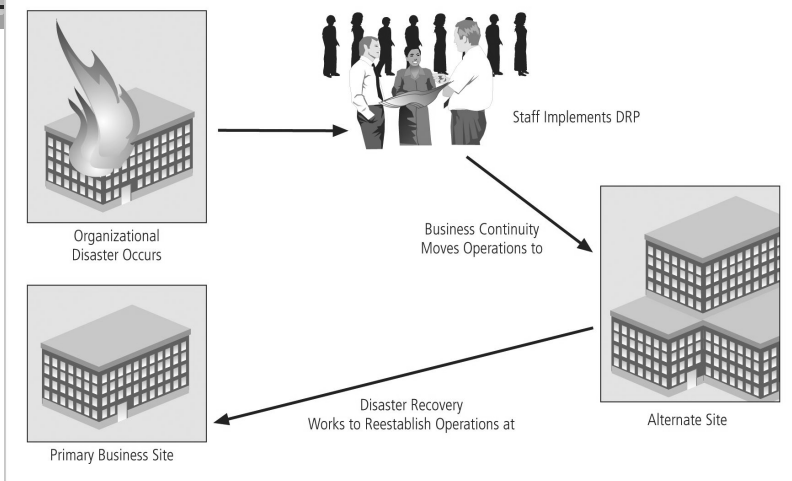


FIGURE 3-4 Disaster Recovery and Business Continuity Planning

Contingency Plan Implementation Timeline

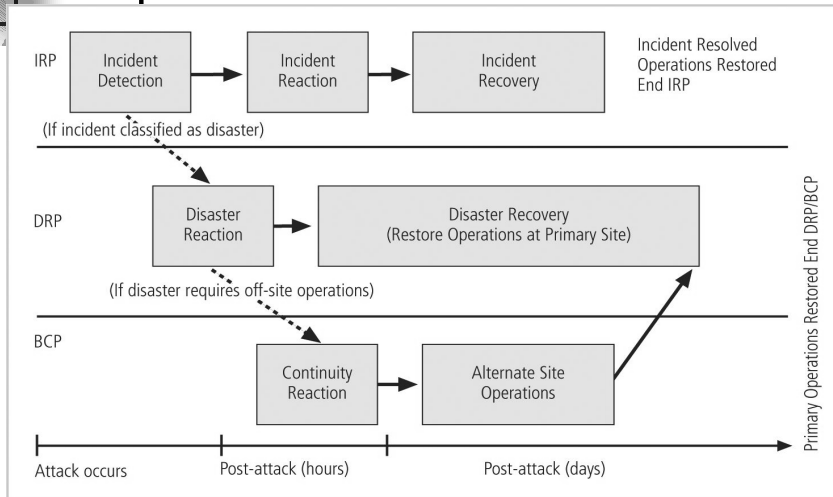


FIGURE 3-5 Contingency Plan Implementation Timeline

Putting a Contingency Plan Together

- The CP team should include:
 - Champion
 - Project Manager
 - Team Members
 - Business managers
 - Information technology managers
 - Information security managers

Major Tasks in Contingency Planning

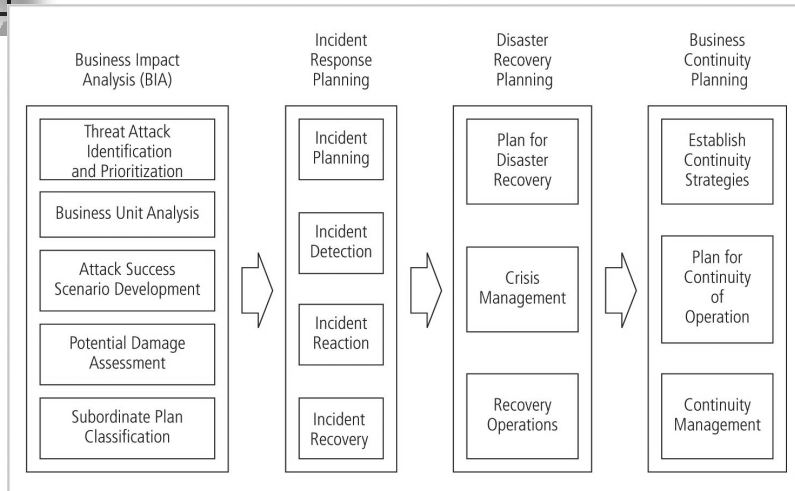



FIGURE 3-6 Major Tasks in Contingency Planning

Business Impact Analysis (BIA)

- BIA
 - Provides information about systems/threats and detailed scenarios for each potential attack
 - Not risk management focusing on identifying threats, vulnerabilities, and attacks to determine controls
 - Assumes controls have been bypassed or are ineffective and attack was successful
- CP team conducts BIA in the following stages:
 - Threat attack identification
 - Business unit analysis
 - Attack success scenarios
 - Potential damage assessment
 - Subordinate plan classification



Threat/Attack Identification and Prioritization

- An organization that uses risk management process will have identified and prioritized threats
- These organizations update threat list and add one additional piece of information -- the attack profile
- Attack profile: detailed description of activities that occur during an attack



Business Unit Analysis

- Second major BIA task is analysis and prioritization of business functions within the organization



Attack Success Scenario Development

- Next create a series of scenarios depicting impact of successful attack on each functional area
- Attack profiles should include scenarios depicting typical attack including:
 - Methodology
 - Indicators
 - broad consequences
- More details are added including alternate outcomes—best, worst, and most likely



Potential Damage Assessment

- From detailed scenarios, the BIA planning team must estimate the cost of the best, worst, and most likely outcomes by preparing an attack scenario end case
- This will allow identification of what must be done to recover from each possible case



Subordinate Plan Classification

- From existing plans, a related plan must be developed or identified from among existing plans already in place
- Each attack scenario case is categorized as disastrous or not
- Attack cases that are disastrous find members of the organization waiting out the attack and planning to recover after it is over



Combining the DRP and the BCP

- Because DRP and BCP are closely related, most organizations prepare them concurrently and may combine them into a single document
- Such a comprehensive plan must be able to support reestablishment of operations at two different locations
 1. Immediately at alternate site
 2. Eventually back at primary site
- Therefore, although a single planning team can develop combined DRP/BRP, execution requires separate teams



Sample Disaster Recovery Plan

- Name of agency
- Date of completion or update of the plan and test date
- Agency staff to be called in the event of a disaster
- Emergency services to be called (if needed) in event of a disaster
- Locations of in-house emergency equipment and supplies
- Sources of off-site equipment and supplies
- Salvage Priority List
- Agency Disaster Recovery Procedures
- Follow-up Assessment



Testing Contingency Plans

- Once problems are identified during the testing process, improvements can be made, and the resulting plan can be relied on in times of need
- There are five testing strategies that can be used to test contingency plans:
 - Desk Check
 - Structured walkthrough
 - Simulation
 - Parallel testing
 - Full interruption

A Single Contingency Plan Format

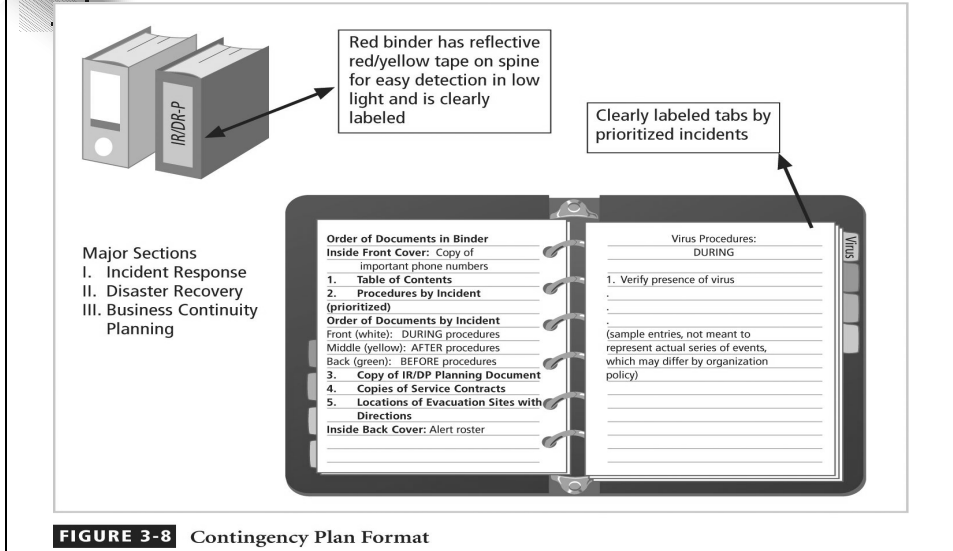


FIGURE 3-8 Contingency Plan Format

Continuous Improvement

- Iteration results in improvement
- A formal implementation of this methodology is a process known as continuous process improvement (CPI)
- Each time plan is rehearsed, it should be improved
- Constant evaluation and improvement leads to an improved outcome