



Contents

CONTENTS	1
INTRODUCTION	2
IDENTIFYING THE MISSION- OR BUSINESS-CRITICAL FUNCTIONS	3
IDENTIFYING THE RESOURCES THAT SUPPORT CRITICAL FUNCTIONS	4
HUMAN RESOURCES.....	4
PROCESSING CAPABILITY.....	4
AUTOMATED APPLICATIONS AND DATA.....	4
COMPUTER-BASED SERVICES.....	5
PHYSICAL INFRASTRUCTURE.....	5
DOCUMENTS AND PAPERS.....	5
ANTICIPATING POTENTIAL CONTINGENCIES OR DISASTERS	6
SELECTING CONTINGENCY PLANNING STRATEGIES	7
HUMAN RESOURCES.....	7
PROCESSING CAPABILITY.....	8
AUTOMATED APPLICATIONS AND DATA.....	8
COMPUTER-BASED SERVICES.....	8
PHYSICAL INFRASTRUCTURE.....	9
DOCUMENTS AND PAPERS.....	9
IMPLEMENTING THE CONTINGENCY STRATEGIES	10
HOW MANY PLANS?	10
WHO PREPARES THE PLAN?.....	10
DOCUMENTING.....	11
TRAINING.....	11
TESTING AND REVISING	12
SUMMARY AND CHECKLIST	13
IDENTIFY CRITICAL FUNCTIONS.....	13
IDENTIFY CRITICAL RESOURCES.....	13
IDENTIFY POTENTIAL CONTINGENCIES OR DISASTERS.....	13
SELECT CONTINGENCY PLANNING STRATEGIES	13
IMPLEMENT THE CONTINGENCY STRATEGIES	14
DOCUMENTATION AND CHECK LISTS	15
CRITICAL RESOURCES LIST	15
KEY PERSONNEL CONTACT LIST	15
CHECK LISTS.....	15
EQUIPMENT DOCUMENTATION.....	15
SOFTWARE DOCUMENTATION	16
KEY DATA DOCUMENTATION	16
PROCEDURES.....	16
CREEPING DISASTER MONITORING.....	16



Introduction

Contingency planning involves more than planning for a move off site after a disaster destroys a data centre. It also addresses how to keep an organisation's critical functions operating in the event of disruptions, both large and small. This broader perspective on contingency planning is based on the distribution of computer support throughout an organisation. The contingency planning process involves the following steps:

- Identifying the mission- or business-critical functions,
- Identifying the resources that support the critical functions,
- Anticipating potential contingencies or disasters,
- Selecting contingency planning strategies,
- Implementing the contingency strategies, and
- Testing and revising the strategy.



Identifying the Mission- or Business-Critical Functions

Protecting the continuity of an organisation's mission or business is very difficult if it is not clearly identified. Managers need to understand the organisation from a point of view that usually extends beyond the area they control. The definition of an organisation's critical mission or business functions is often called a business plan.

Since the development of a business plan will be used to support contingency planning, it is necessary not only to identify critical missions and businesses, but also to set priorities for them. A fully redundant capability for each function is prohibitively expensive for most organisations. In the event of a disaster, certain functions will not be performed. If appropriate priorities have been set (and approved by senior management), it could mean the difference in the organisation's ability to survive a disaster.



Identifying the Resources That Support Critical Functions

After identifying critical missions and business functions, it is necessary to identify the supporting resources, the time frames in which each resource is used (e.g., is the resource needed constantly or only at the end of the month?), and the effect on the mission or business of the unavailability of the resource. In identifying resources, a traditional problem has been that different managers oversee different resources. They may not realise how resources interact to support the organisation's mission or business. Many of these resources are not computer resources. Contingency planning should address all the resources needed to perform a function, regardless whether they directly relate to a computer.

The analysis of needed resources should be conducted by those who understand how the function is performed and the dependencies of various resources on other resources and other critical relationships. This will allow an organisation to assign priorities to resources since not all elements of all resources are crucial to the critical functions.

Human Resources

People are perhaps an organisation's most obvious resource. Some functions require the effort of specific individuals, some require specialised expertise, and some only require individuals who can be trained to perform a specific task. Within the information technology field, human resources include both operators (such as technicians or system programmers) and users (such as data entry clerks or information analysts).

Processing Capability

Traditionally contingency planning has focused on processing power (i.e., if the data centre is down, how can applications dependent on it continue to be processed?). Although the need for data centre backup remains vital, today's other processing alternatives are also important. Local area networks (LANs), minicomputers, workstations, and personal computers in all forms of centralised and distributed processing may be performing critical tasks.

Automated Applications and Data

Computer systems run applications that process data. Without current electronic versions of both applications and data, computerised processing may not be possible. If the processing is being performed on alternate hardware, the applications must be compatible with the alternate hardware, operating systems and other software (including version and configuration), and numerous other technical factors. Because of the complexity, it is normally necessary to periodically verify compatibility. (See Testing and Revising.)



Computer-Based Services

An organisation uses many different kinds of computer-based services to perform its functions. The two most important are normally communications services and information services. Communications can be further categorised as data and voice communications; however, in many organisations these are managed by the same service. Information services include any source of information outside of the organisation. Many of these sources are becoming automated, including on-line government and private databases, news services, and bulletin boards.

Physical Infrastructure

For people to work effectively, they need a safe working environment and appropriate equipment and utilities. This can include office space, heating, cooling, venting, power, water, sewage, other utilities, desks, telephones, fax machines, personal computers, terminals, courier services, file cabinets, and many other items. In addition, computers also need space and utilities, such as electricity. Electronic and paper media used to store applications and data also have physical requirements.

Documents and Papers

Many functions rely on vital records and various documents, papers, or forms. These records could be important because of a legal need (such as being able to produce a signed copy of a loan) or because they are the only record of the information. Records can be maintained on paper, microfiche, microfilm, magnetic media, or optical disk.



Anticipating Potential Contingencies or Disasters

Although it is impossible to think of all the things that can go wrong, the next step is to identify a likely range of problems. The development of scenarios will help an organisation develop a plan to address the wide range of things that can go wrong.

Scenarios should include small and large contingencies. While some general classes of contingency scenarios are obvious, imagination and creativity, as well as research, can point to other possible, but less obvious, contingencies. The contingency scenarios should address each of the resources described above. The following are examples of some of the types of questions that contingency scenarios may address:

Human Resources: Can people get to work? Are key personnel willing to cross a picket line? Are there critical skills and knowledge possessed by one person? Can people easily get to an alternative site?

Processing Capability: Are the computers harmed? What happens if some of the computers are inoperable, but not all?

Automated Applications and Data: Has data integrity been affected? Is an application sabotaged? Can an application run on a different processing platform?

Computer-Based Services: Can the computers communicate? To where? Can people communicate? Are information services down? For how long?

Infrastructure: Do people have a place to sit? Do they have equipment to do their jobs? Can they occupy the building?

Documents/Paper: Can needed records be found? Are they readable?



Selecting Contingency Planning Strategies

The next step is to plan how to recover needed resources. In evaluating alternatives, it is necessary to consider what controls are in place to prevent and minimise contingencies. Since no set of controls can cost-effectively prevent all contingencies, it is necessary to co-ordinate prevention and recovery efforts.

A contingency planning strategy normally consists of three parts: emergency response, recovery, and resumption. Emergency response encompasses the initial actions taken to protect lives and limit damage. Recovery refers to the steps that are taken to continue support for critical functions. Resumption is the return to normal operations. The relationship between recovery and resumption is important. The longer it takes to resume normal operations, the longer the organisation will have to operate in the recovery mode.

The selection of a strategy needs to be based on practical considerations, including feasibility and cost. The different categories of resources should each be considered. Risk assessment can be used to help estimate the cost of options to decide on an optimal strategy. For example, is it more expensive to purchase and maintain a generator or to move processing to an alternate site, considering the likelihood of losing electrical power for various lengths of time? Are the consequences of a loss of computer-related resources sufficiently high to warrant the cost of various recovery strategies? The risk assessment should focus on areas where it is not clear which strategy is the best.

In developing contingency planning strategies, there are many factors to consider in addressing each of the resources that support critical functions.

Human Resources

To ensure an organisation has access to workers with the right skills and knowledge, training and documentation of knowledge are needed. During a major contingency, people will be under significant stress and may panic. If the contingency is a regional disaster, their first concerns will probably be their family and property. In addition, many people will be either unwilling or unable to come to work. Additional hiring or temporary services can be used. The use of additional personnel may introduce security vulnerabilities.

Contingency planning, especially for emergency response, normally places the highest emphasis on the protection of human life.



Processing Capability

Strategies for processing capability are normally grouped into five categories: hot site; cold site; redundancy; reciprocal agreements; and hybrids. These terms originated with recovery strategies for data centres but can be applied to other platforms.

- Hot site - A building already equipped with processing capability and other services.
- Cold site - A building for housing processors that can be easily adapted for use.
- Redundant site - A site equipped and configured exactly like the primary site. (Some organisations plan on having reduced processing capability after a disaster and use partial redundancy. The stocking of spare personal computers or LAN servers also provides some redundancy.)
- Reciprocal agreement - An agreement that allows two organisations to back each other up. (While this approach often sounds desirable, contingency planning experts note that this alternative has the greatest chance of failure due to problems keeping agreements and plans up-to-date as systems and personnel change.)
- Hybrids - Any combinations of the above such as using having a hot site as a backup in case a redundant or reciprocal agreement site is damaged by a separate contingency.

Recovery may include several stages, perhaps marked by increasing availability of processing capability. Resumption planning may include contracts or the ability to place contracts to replace equipment.

Automated Applications and Data

Normally, the primary contingency strategy for applications and data is regular backup and secure off site storage. Important decisions to be addressed include how often the backup is performed, how often it is stored off-site, and how it is transported (to storage, to an alternate processing site, or to support the resumption of normal operations).

Computer-Based Services

Service providers may offer contingency services. Voice communications carriers often can re-route calls (transparently to the user) to a new location. Data communications carriers can also re-route traffic. Hot sites are usually capable of receiving data and voice communications. If one service provider is down, it may be possible to use another. However, the type of communications carrier



lost, either local or long distance, is important. Local voice service may be carried on cellular. Local data communications, especially for large volumes, is normally more difficult. In addition, resuming normal operations may require another re-routing of communications services.

Physical Infrastructure

Hot sites and cold sites may also offer office space in addition to processing capability support. Other types of contractual arrangements can be made for office space, security services, furniture, and more in the event of a contingency. If the contingency plan calls for moving off site, procedures need to be developed to ensure a smooth transition back to the primary operating facility or to a new facility. Protection of the physical infrastructure is normally an important part of the emergency response plan, such as use of fire extinguishers or protecting equipment from water damage.

Documents and Papers

The primary contingency strategy is usually backup onto magnetic, optical, microfiche, paper, or other medium and off site storage. Paper documents are generally harder to backup than electronic ones. A supply of forms and other needed papers can be stored off site.



Implementing the Contingency Strategies

Once the contingency planning strategies have been selected, it is necessary to make appropriate preparations, document the strategies, and train employees. Many of these tasks are ongoing.

Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources. For example, one common preparation is to establish procedures for backing up files and applications. Another is to establish contracts and agreements, if the contingency strategy calls for them. Existing service contracts may need to be re-negotiated to add contingency services. Another preparation may be to purchase equipment, especially to support a redundant capability.

It is important to keep preparations, including documentation, up-to-date. Computer systems change rapidly and so should backup services and redundant equipment. Contracts and agreements may also need to reflect the changes. If additional equipment is needed, it must be maintained and periodically replaced when it is no longer dependable or no longer fits the organisation's architecture.

Preparation should also include formally designating people who are responsible for various tasks in the event of a contingency. These people are often referred to as the contingency response team. This team is often composed of people who were a part of the contingency planning team.

There are many important implementation issues for an organisation. Two of the most important are how many plans should be developed and who prepares each plan. Both of these questions revolve around the organisation's overall strategy for contingency planning. The answers should be documented in organisation policy and procedures.

How Many Plans?

Some organisations have just one plan for the entire organisation, and others have a plan for every distinct computer system, application, or other resource. Other approaches recommend a plan for each business or mission function, with separate plans, as needed, for critical resources.

The answer to the question, therefore, depends upon the unique circumstances for each organisation. But it is critical to co-ordinate between resource managers and functional managers who are responsible for the mission or business.

Who Prepares the Plan?

If an organisation decides on a centralised approach to contingency planning, it may be best to name a contingency planning co-ordinator. The co-ordinator prepares the plans in co-operation with



various functional and resource managers. Some organisations place responsibility directly with the functional and resource managers.

Documenting

The contingency plan needs to be written, kept up-to-date as the system and other factors change, and stored in a safe place. A written plan is critical during a contingency, especially if the person who developed the plan is unavailable. It should clearly state in simple language the sequence of tasks to be performed in the event of a contingency so that someone with minimal knowledge could immediately begin to execute the plan. It is generally helpful to store up-to-date copies of the contingency plan in several locations, including any off-site locations, such as alternate processing sites or backup data storage facilities.

Training

All personnel should be trained in their contingency-related duties. New personnel should be trained as they join the organisation, refresher training may be needed, and personnel will need to practice their skills.

Training is particularly important for effective employee response during emergencies. There is no time to check a manual to determine correct procedures if there is a fire. Depending on the nature of the emergency, there may or may not be time to protect equipment and other assets. Practice is necessary in order to react correctly, especially when human safety is involved.



Testing and Revising

A contingency plan should be tested periodically because there will undoubtedly be flaws in the plan and in its implementation. The plan will become dated as time passes and as the resources used to support critical functions change. Responsibility for keeping the contingency plan current should be specifically assigned. The extent and frequency of testing will vary between organisations and among systems. There are several types of testing, including reviews, analyses, and simulations of disasters.

A review can be a simple test to check the accuracy of contingency plan documentation. For instance, a reviewer could check if individuals listed are still in the organisation and still have the responsibilities that caused them to be included in the plan. This test can check home and work telephone numbers, organisational codes, and building and room numbers. The review can determine if files can be restored from backup tapes or if employees know emergency procedures.

An analysis may be performed on the entire plan or portions of it, such as emergency response procedures. It is beneficial if the analysis is performed by someone who did not help develop the contingency plan but has a good working knowledge of the critical function and supporting resources. The analyst(s) may mentally follow the strategies in the contingency plan, looking for flaws in the logic or process used by the plan's developers. The analyst may also interview functional managers, resource managers, and their staff to uncover missing or unworkable pieces of the plan.

Organisations may also arrange disaster simulations. These tests provide valuable information about flaws in the contingency plan and provide practice for a real emergency. While they can be expensive, these tests can also provide critical information that can be used to ensure the continuity of important functions. In general, the more critical the functions and the resources addressed in the contingency plan, the more cost-beneficial it is to perform a disaster simulation.



Summary and Checklist

Identify critical functions

- Review business plans
- Review project plans
- Examine roles and responsibilities
- Use risk analysis

Identify critical resources

- Classes of resource:
 - Human resources
 - Physical infrastructure
 - Documents and Papers
 - Applications and data
 - Computer hardware and operating systems
 - Printers and print queues
 - E-mail facilities
 - LAN access facilities
 - Host access facilities
 - Remote access facilities
- Determine time frames for each resource
- Liaise with other managers

Identify potential contingencies or disasters

- Access to site, key personnel, picket lines
- Computer damage, partial failure
- Data integrity, application sabotage, other platforms
- Data communications, voice communications, services failures
- Office space, equipment availability, building safety
- Access to records, readability, security

Select contingency planning strategies

- Protect lives, limit damage
- Continued support for critical functions



- Resumption of normal operations
- Test after every full or partial restore

Implement the contingency strategies

- Establish procedures, contracts and agreements
- Maintain up-to-date documentation
- Designate staff
- Create and secure the plan
- Train regular and reserve staff
- Test and revise regularly



Documentation and check lists

Critical resources list

- Human resources
- Physical infrastructure
- Documents and papers
- Applications and data
- Computer hardware and operating systems
- Printers and print queues
- E-mail facilities
- LAN access facilities
- Host access facilities
- Remote access facilities

Key personnel contact list

- System administrators
- Computer operators
- Key users
- Staff with unique skills
- Disaster contingency team members

Check lists

- Disaster assessment
- Disaster recovery
- Salvage
- Restoration

Equipment documentation

- Servers and hosts
- Workstations
- Printers
- Cabling system and active components
- Power supply



Software documentation

- Host operating systems and utilities
- Server operating systems and utilities
- Workstation operating systems
- Applications (packaged and bespoke)
- Access control lists

Key data documentation

- Host-based data
- Server-based data
- Workstation-based data
- Mobile computer data

Procedures

- Backup (and restore!)
- Virus control and recovery
- Workstation failure
- Server failure
- Host failure
- Network infrastructure failure
- Power failure
- Communications failure

Creeping disaster monitoring

- Disk space
- Network traffic
- Number and type of users
- Number and type of applications
- Workstation configuration changes