Technical Dossier

Business Continuity Plan

I.S. Strategy and recovery solutions

(Disaster Recovery Plan)

English version: November 2004

TECHNICAL COMMISSION FOR LOGIC SECURITY

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS

30, rue Pierre Semard, 75009 PARIS

Tel. : +33 153 25 08 80 – Fax : +33 1 53 25 08 88

e-mail : clusif@clusif.asso.fr - Web : http://www.clusif.asso.fr

CONTENTS

ACKNOWLEDGEMENTS

CLUSIF would like to thank those people who helped to make this document possible, particularly:

Robert	**BERGERON**	*CAP GEMINI*
Annie	**BUTEL**	*PRICEWATERHOUSECOOPERS*
Jean-Claude	**GANDOIS**	*LEGRAND*
Guy	**JOVER**	*CNAMTS*
Guy	**KHOUBERMAN**	*ACOSS CNIR SUD*
Siegfried	**NOEL**	*TELINDUS*

We would also like to express our gratitude to the « Espace RSSI » and its leader, **Pierre SINOQUET**, for the fruitful exchanges that were had over the issue of ensuring the continuity of business activities.

CLUSIF also thanks Louis Vuitton Moët Hennessy for its translation support.

1 INTRODUCTION

This document is primarily intended for security directors, IT departments, risk managers and those involved in internal audits. It also concerns the various players (senior management, the legal department, the human resources department, the administrative and financial departments...) who may play a role in defining, implementing, maintaining or guaranteeing security. It is intended to help in the selection and establishment of the procedures that are necessary to ensure the continuous availability of the company's information systems.

The question of ensuring the continuity of the information systems (IS) may be tackled:

- in the framework of a Business Contingency Plan (BCP). A company's strategic projects are realized at the request of senior management. These plans are meant to ensure the company's survival. The recovery of IT resources is just one of the aspects of a BCP;
- during the development of a Disaster Recovery Plan (DRP). The DRP concerns the recovery of IT resources. However, it has to include the full involvement of senior management. The IT. Recovery Plan aims to guarantee the minimum service required for the information systems;
- during the setup of a new application, during important changes on the technical architecture or during the negotiation of service contracts. It is about responding to a specific need within the framework of the overall strategy (BCP, DRP) – if such a strategy has already been defined.

This document is divided into three main sections:

- Taking needs into account and definite a recovery strategy (chapter 2). This chapter provides elements that help:
  - in the preliminary analysis of the risks;
  - in the selection of the measures to be implemented (permanent measures pertaining to quality or recovery plans that are only set in motion in the event of an incident / disaster).
- The development of a Disaster Recovery Plan (chapter 3). This chapter describes the organization and key components of a DRP and how it fits into a more comprehensive business contingency plan.
- A presentation of the principal measures that need to be set in place to ensure the continued availability of the information systems (chapter 4).

A glossary of terms can be found at the end of this document.

2 RECOVERY STRATEGY

The development of a Disaster Recovery Plan is an operation made complex by the number of scenarios that need to be considered (damage to the premises, equipment breakdown, errors, malevolence, etc) and by the volume and difficulty of the tasks that need to be conducted in order to restore a normal activity. It is a process that inevitably takes a considerable amount of time to set in place. It also requires a great deal of work from the teams involved. The need for service continuity is becoming increasingly important and this leads to ever more costly solutions. In addition, it is essential that the recovery strategy reflects the specificities and requirements of the company.

This chapter presents the traditional stages that ultimately help to define a recovery strategy.

In addition, CLUSIF has several documents on hand that explore the various methods – particularly the MEHARI method – which defines outlines and the various stages of a vulnerability study and the essentials of risk analysis.

2.1 Definitions

In this document, we will also refer to certain notions of risk analysis as set out in the MARION and MEHARI methods:

Impact: the impact level measures the consequences on the company of a disaster (a risk becoming a reality). By defining an impact level, we can specify those situations that will be critical or fatal for the company (financial losses, damage to the company's image, disruption...). It also provides us with a common reference to assess risks.

Potentiality: the potentiality level gives us an understanding of the probability of a risk occurring. Generally, there are 4 or 5 levels, which is enough to differentiate between a slim theoretical possibility and a risk that will probably occur in the near future.

Seriousness: A combination of impact and potentiality. The level defining the seriousness of a risk measures its degree of acceptability as defined by senior management.

2.2 Method

2.2.1 The different phases of the methodology

The method to define a recovery strategy can be broken down into 5 phases:

Figure 1: The various stages of a recovery strategy

2.2.2 Launch phase

Before undertaking a Disaster Recovery Plan study, it is essential to specify the field. In particular, it is advisable to have the business activities concerned and the types of risks to be considered validated by the company's management via a steering committee. Such a plan could cover all of a company's business activities or, conversely, it could be limited to a strategic sector. For each business activity concerned, we assign a corresponding DRP for the project team.

The primary difficulty with this type of study is establishing a DRP adapted to its environment. The adoption of a customized methodology can help the plan's appropriation among the managers concerned.

Management needs to define the risks to be covered. Depending on the choices made, the "elements" at risk (computer hardware, telecommunications equipment, external supplies, personnel, premises, ...) as well as the nature of the risks need to be specified (for example, should industrial unrest be taken into account?).

Depending on the specified risks and the area of coverage desired, the recovery plan will either be a Disaster Recovery Plan or it will be similar to a Business Contingency Plan.

The risk analysis guides at the end of this document list the main groups of elements at risk that can be covered in a DRP as well as the principal risks associated with them.

2.2.3 The operational research phase

The operational research phase aims to define the requirements to ensure the continuity of each business activity. In order to do this, we need to examine the stakes, identify the essential business activities and assess the consequences of an interruption or disruption of these activities (temporary or definitive shutdown, loss of data, disruption of service ...). A comparison of the different situations should help to adjust the impact levels (defining the "unbearable" nature of a situation) which will be used later in the risk analysis phase.

The operational research phase also needs to specify the minimum conditions necessary to ensure an acceptable level of business activity in any circumstances. To do this, one needs to:

- identify the elements of the information system which are essential for the continuation of business activity (applications, means of communication, information)
- specify the minimum level of service acceptable for each business activity, namely:
  - the vital applications;
  - the human resources;
  - the premises;
  - the equipment (work stations, telephones, printers, networks...);
  - the return time objective for the resumption of business activity
  - the duration of the period of minimum service;
  - the degree of service disruption that is acceptable (response time, activities that may be carried out manually...);
  - the conditions for a return to normal;
  - the external supplies which are indispensable.

Such an assessment will be more effective if it includes operational groups that are able to represent each of the company's business activities. In that case, it will be necessary to make consolidations and to verify the general consistency of the needs as expressed by the various groups (it is only natural for user managers to consider their own business activities to be strategic). If necessary, senior management should act as arbitrators. Once the requisite solutions have been quantified, the notion of an "acceptable minimum service" may then be revised (iterative process).

From this phase, a list of applications that comprise the strategic core of the DRP should be deduced.

2.2.4 Vulnerability study phase

As in any security study, it is necessary to evaluate the current security measures as well as those that are planned in the future. If such an assessment has not already been carried out in the framework of an overall study, it will, at the very least, be necessary to conduct a review of the following themes:

- Security organization;
- Insurance coverage of IT-based risks;
- Physical & Environmental security (environment, physical access, fire prevention/safety measures and water damage, security guidelines);
- The security measures that are in place or planned for (servers, network, terminals, electrical feeds, air conditioning, supplies, personnel... depending on the field of study). At this stage, it is important to estimate the degree of confidence one can have in the recovery measures (can the deadlines to implement the measures be guaranteed? Are the measures documented and tested?);

- The means to protect stored information:
  - IT backup measures: backup copies of saved data, archives (accompanied by reliable retrieval procedures);
  - Paper backup (dossiers, archives, documentation, ...);
- The measures established to ensure the security of external exchanges (protection of the network...);
- The maintenance contracts for equipment and software (verifying the obligations of service providers);
- The supplier contracts for sensitive equipment (guarantees to reestablish service in the event of disruption/failure);
- The means for administering and operating the systems (system audit and application vulnerabilities, alert follow-up ...).

An examination of these themes can result in preventive measures aimed at reducing the potentiality of risks.

We can also use the audit questionnaires of the MARION or MEHARI methods to help us conduct the study.

2.2.5 Risk analysis phase

The risk analysis phase is intended to quantify the risks of a total or partial lack of availability of the information systems and to highlight the priorities in terms of processing the risks. The realization of a recovery plan or a Business Contingency Plan is a major operation. If priorities are defined, the plan may be conducted in stages.

The risk analysis phase can be broken down into two parts:

- a technical phase to study incident / disaster scenarios;
- an operational phase to study the potential impact.

By building on the assessment made in the previous phase, the technical study consists of listing one or several significant risks for each asset at risk, then, for each of the risks, to study and describe the direct consequences that such a risk would have on the information system. At this step, we still don't explore the consequences of the impact of the incident / disaster. The objective is to make an assessment of the direct consequences in terms of:

- length of time the resources are available (applications, services...);
- amount of information lost (last updates, flow, archives...);
- potentiality of the risk. Depending on the method used in the previous phase, the potentiality will either be directly attributed or calculated.

The operational phase consists in measuring the impact of the potential risks with the aid of criteria that were predetermined during the launch phase. This evaluation needs to be conducted with the support of the operational managers to take account of any bypass resources that may currently exist.

A scale of seriousness is thus determined by combining impact and potentiality (cf. MARION and MEHARI methods – risk avoidance table). A hierarchical list of the risks is made in descending order of gravity. This helps to determine the risks that need to be taken into account in the recovery plan as well as their priority in that list.

Note: The risk analysis guides at the end of this document list the risk type for each group of elements at risk, and for each, examples of the consequences to analyze and the potential antidotes to them (at this stage of the study, we use these guides to verify the potential existence of an antidote).

2.2.6 Orientation phase: operational targets and the choice of technical recovery solutions:

The operational target is determined by an analysis of the operational organization chart of the information system and a classification of the functions and sub-functions according to the needs in availability as assessed by the operational managers. This classification helps to determine the strategic operational core that represents the minimum required to ensure the company's survival.

Based on the incident / disaster scenarios, it is necessary to estimate the length of time that service is interrupted for each vital function, by attempting to regroup them according to previously determined levels of seriousness (4 to 5 maximum) ranging from a mere service shutdown to a "disaster" situation.

All the "elements" of the information system (applications, hardware, network equipment, supplies…) that are crucial to the operation of the core will be identified and regrouped into indivisible sub-groups.

In regard to these elements, it will henceforth be possible to consider and evaluate return time scenarios and the appropriate means of recovery to bring the estimated impact down to an acceptable level. One also must be sure to retain the coherence of all the constituent elements needed to recover the strategic core. The development of specific interfaces or the definition of manual procedures are often necessary to obtain the desired level of service or the reduced level of service depending on the constraints and the means that have been chosen.

It will also be necessary to establish a plan to circulate information and assess the needs in terms of office space and work stations to enable "strategic" users to ensure the minimum level of service in a crisis situation.

Finally, in order to reboot after an incident / disaster, we will need to study the means to restore and synchronize the data associated with the operational core.

The approach outlined above will result in the specifications for the Disaster Recovery Plan.

3 THE DISASTER RECOVERY PLAN

3.1 Introduction

After working out the specifications of the recovery plan, a phase of research needs to be conducted to determine the various technical and organizational solutions. Once this research has been completed, a compendium of solution options will be submitted to the decision-making committee. Then, it will have the task of defining the definitive content of the Disaster Recovery Plan (the different types of solutions that can be envisaged will be presented in chapter 4). At this stage of the study, an assessment of the solutions may lead to adjustments in the type of resources that are requested.

A *preparatory plan* will be launched to specify the chosen solutions. The plan will include a phase of detailed research and implementation as well as a test phase to formalize the operational procedures. The whole solutions and procedures will make up the *implementation plan* that will ultimately be activated in the event of an incident.

The preparatory plan may be strengthened by the addition of performance indicators. They will point out and evaluate the progression of those who are responsible for the actions to be taken.

The objective of this chapter is to set out the principal themes that will need to be dealt with during the preparatory plan. The documentation produced during this phase will compose the Disaster Recovery Plan.

3.2 Organization

The different tasks associated with steering and implementing the recovery plan must be assigned to the various “protagonists”. These protagonists are predefined operational entities comprised of enough people to ensure that the completion of the task can be guaranteed in event of an incident.

The first people to intervene are those charged with sounding the alarm and issuing the instructions according to pre-determined response procedures.

In the event of an incident, the following will be brought into play:

- The crisis management committee;
- The coordinating committee;
- The operational response teams ;
- The user services.

Through a system of “crisis organization” one also designates a joint crisis management/coordinating committee.

3.2.1 The crisis management committee

At the very least, the crisis management committee needs to include representatives from the following areas: senior management, the principal user departments, the general services department, the human resources department, the IT department, the communications department and of course, the recovery plan director. The crisis management committee will take the principal decisions concerning the recovery procedures. In particular, it will be responsible for deciding when to implement any given aspect of the Disaster Recovery Plan. The crisis management committee may also call upon specific, internal or external expertise, especially in terms of communications and legal guidance.

The means of communication with the crisis management committee need to be predetermined and guaranteed in the event of an incident (the designated meeting place, telephone numbers, fax numbers...).

3.2.2 The Coordinating Committee

The actual task of steering the recovery operations may be delegated to a coordinating committee. This will relieve the crisis management committee of the task of coordinating the various actions.

Ideally, the coordinating committee will be made up of a small number of people: the director of the Disaster Recovery Plan (the person who is familiar with and who has control over the entire plan) and the people in charge of coordinating the computer-based and logistical operations.

Some decision making powers may be delegated to the coordinating committee by the crisis management committee, particularly those pertaining to the implementation of certain advance measures (example: reserving a backup site with a service provider).

3.2.3 The operational response teams

The operational response teams are given the various task of the recovery according to the skills required, availability and the place were the teams are intervening. One needs to make sure that existing work contracts allow for these teams to be sent to a different location.

Examples:

- Logistical team charged with transporting equipment;
- IT response team, composed of a network specialist and a maintenance agent in charge of operations on the backup site;
- A team in charge of emergency communication;
- A network response team in charge of configuring the network at the user backup site;
- etc.

Finally, certain protagonists outside the company also need to be identified: emergency contractors, energy suppliers, telephone service providers, Internet access provider…

All internal and external responders must be listed with the relevant contact information in a regularly updated “recovery plan directory”.

3.2.4 The user services

The user services are in charge of their own business contingency plan depending on the resources that are made available to them. Among the tasks which are the responsibility of the managers of these services, we can include:

- the tasks needing to be achieved while recovery is pending;
- the organization associated with reinitiating (normal or reduced) startup;
- the establishment of possible bypass procedures;
- the organization of special tasks (example: adjustments).

It is important to ensure that the necessary human expertise is fully available in all circumstances and that those involved are aware of the technical procedures to follow in the framework of the backup systems. If needed, it is possible to lean on the expertise of those external responders who have already participated in previous continuity tests.

3.3 Activation

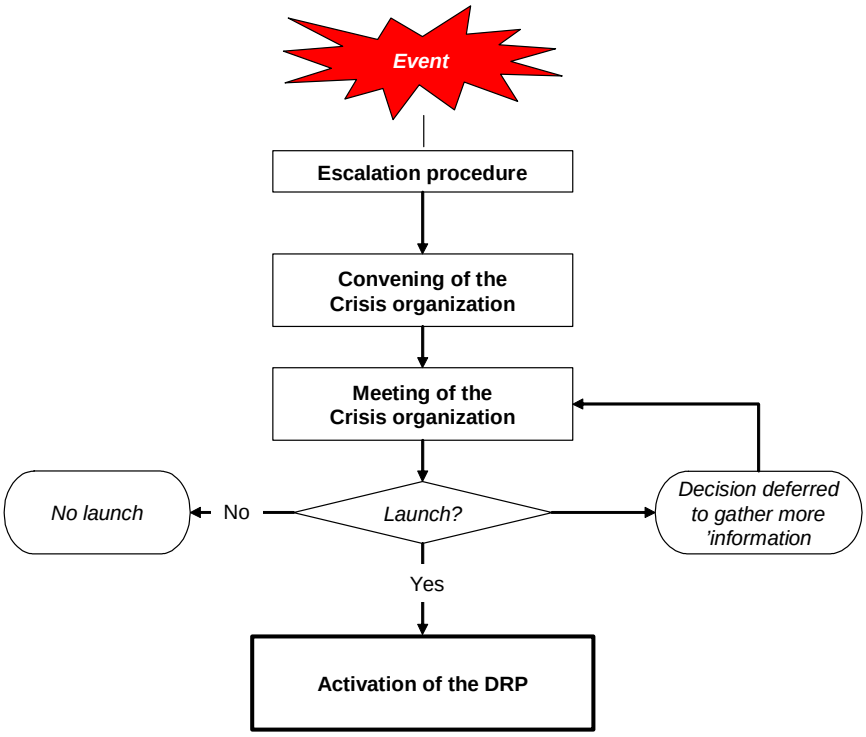

Figure 2: Activation procedures

The crisis organization includes the crisis management committee and the coordinating committee.

The escalation procedures are essential. When an incident occurs, the person informed –often someone in a company security post– needs to know who to contact and how to contact them (particularly if the usual means of communication are not available). In turn, depending on the seriousness of the incident, that person must know which people to contact to get further details or if necessary to set the crisis organization in motion. It is crucial to set out in advance exactly who is authorized to activate the crisis response effort and to call only the people who have been specifically designated to prevent unnecessary congestion on the lines.

3.4 Recovery measures

A recovery plan is comprised of elementary measures (technical or organizational procedures). Their activation will depend on the type of event and the general context in which that event occurs. The activation of certain measures or the way they are activated may depend on multiple factors (example: emergency communication).

The various measures of a recovery plan may be classified by business type:

- Mobilizing the necessary resources:
  - Human resources: mobilizing the operational response teams;
  - reserving additional means as a backup (requisitioning, alerting an external service contractor...) ;

    - recovery of saved data;
    - recuperation of documents;
- Computer equipment backup:
    - restoring the system environments;
    - technical adaptations (often, the backup material is not the same as the original equipment);
    - restoring the applications;
    - validating the restored processes and systems;
- Backup networks:
    - setting up of backup equipment;
    - switching over to backup links;
    - configuring the different equipment;
- Telephone system backup:
    - rerouting of calls;
    - setting up of backup equipment;
    - configuration;
- Resumption of processes:
    - software adaptations;
    - adaptation of operational procedures;
    - restoring the flow and synchronization of data;
    - special processes;
    - operational validations;
- Logistics:
    - transportation;
    - supplies;
    - crisis management of the personnel (choice of staff to mobilize, team rotation, taking account of individual situations...);
- Relocation:
    - organizing the emergency relocation;
    - preparing reception sites;
- Resumption of user service business:
    - user tasks prior to the implementation of backup measures;
    - organizing a minimum level of service;
    - special tasks (bypass procedures, recovery procedures...);
- Emergency communication:
    - internal (personnel, other entities...);
    - external (clients, partners, the public...);
- Post-recovery measures:
    - preliminary measures and support (insurance, returning the premises to normal, salvaging equipment...);
    - Measures to assist the return to normal (making a specific plan).

To be operational, these emergency measures need to be accompanied by permanent measures aimed at keeping the former up to standard (examples: the backup plan, the updating procedures and the training of key players involved in the DRP...).

3.5 Documentation

Documentation is a key element in any recovery plan. Generally, such documentation is voluminous and it is constantly being updated (new personnel postings, changing configurations, new applications...). For all these reasons, it is highly recommended to oversee such documentation with the support of a specialized tool used in the administration of recovery plans or business contingency plans. It is also important to ensure the confidentiality of these documents, since they may very well contain personal and strategic information held by the company.

Depending on the stated objective, the documentation for a recovery plan may be structured into 4 levels: communication, implementation, management, and audit.

3.5.1 Documents used to communicate the recovery plan

Internal communication about the recovery plan must not be neglected. It needs to provide the different managers with a clear understanding of all the anticipated solutions and the general conditions governing their implementation. More particularly, this documentation should include:

- A summary of the objectives of service continuity;
- A general description of the different measures of the recovery plan (recovery of computer equipment, backup telecommunications, relocation solutions, emergency communications...);
- A general description of the crisis organization;
- The principles of alerting the crisis organization and the steering of operations;
- A reminder of the residual risks.

3.5.2 Documents used to implement the recovery plan

These documents effectively make up the core of the recovery plan. They are intended for the people who are responsible for the various measures of the plan. They describe all the elements which are essential to their implementation: procedures, technical documentation, elements of synchronization, contracts etc… The technical documentation should, by its level of detail, help to minimize stress-related human error.

More specifically, the documentation should include:

- A recovery plan directory that lists all the potential responders and contributors inside the company and out, together with the relevant information to contact them;
- A description of the recovery strategy for each of the risks identified. This document is intended to help the crisis organization make the right decisions. The recovery strategy defines all the recovery measures that need to be activated depending on the context of the incident (type of event, extent of the damage...);
- The schedule for the various resumption phases;
- A list of tasks to be completed, structured by player and / or recovery measure;
- An “intervention order” for each of the plan’s actors, for each case indexed;
- All useful appendices (procedure documents, technical files, copies of contracts, diagrams, etc...).

When associated with a control tool, the documentation also enables the crisis organization to follow the various operations as they unfurl.

A copy of the documentation (paper and / or the management tools of the plan) should be kept at a secure location outside the company's premises. This location should nonetheless be accessible to be consistent with the objectives of the planned start up.

3.5.3 Documents used to manage the recovery plan

In order to manage the recovery plan, it will be necessary to provide additional documentation for the plan managers and the various teams associated with them. The aim of this documentation is to ease subsequent developments. It may include resource analysis tables as well as a list of where the documents were circulated. It should also include a history of previous test results and an outline of the consequent adjustments.

3.5.4 Documents used to audit the recovery plan

- Performance indicators:
  - Test schedules;
  - Detailed test reports;
  - Quality indicators of the plan's measures;
  - An assessment of the residual risks.

3.6 Maintaining the plan

3.6.1 Organization

A director of the recovery plan will need to be appointed. His/her primary duties will be:

- to carry out, follow and manage the tests and the resulting modifications
- to commit to and follow up the process of updating the recovery plan according to the ever-changing landscape of risks (new threats, new projects, new technologies…);
- to maintain, secure and distribute the documentation for the recovery plan.

Systems of information gathering should be established to improve awareness of:

- new risks;
- new technical and structural developments;
- new projects.

A recovery plan committee made up of the directors of the various teams as well as the technical managers (IT, general services) should meet regularly (at least twice a year). The committee, chaired by the plan director, will be responsible for assessing new risks and for setting up a plan of action which will focus on:

- the implementation of security measures;
- the updating of all documentation;
- the possible changes in the contract with the service contractor;
- the testing of new recovery measures.

The plan director will coordinate all these actions.

3.6.2 Tools

Recovery is not only complex (it is made up of numerous measures intended to respond to all kinds of situations), it is forever in a state of flux (changes in organization, business practices, priorities, personnel, architecture techniques, and applications...). Believing that one can manage such a plan with just a word processing tool is simply illusory.

The task of maintaining a recovery plan is greatly facilitated by the use of a specialized tool. Such a tool should be able to:

- handle all the documentation needed to implement each measure in the plan;
- manage the resources needed to implement all the measures;
- produce the schedules for the re-launch operation, according to the situation at hand;
- manage all tests (planning, results follow-up, gauging the plan's performance…);
- manage the recovery strategy, according to incident types and degree of seriousness;
- provide performance indicators for the individual measures and the overall plan;
- offer ways of distributing the documents (automatic distribution lists, intranet...);
- audit and verify the regular documentary updates.

It is preferable to have a tool that draws on a database and which can facilitate research into the impact of new developments (identifying the tasks that were the responsibility of a person who has been transferred, identifying the measures which are affected by a change in applications, identifying the incident scenarios that need to be reviewed following the transfer or relocation of a department etc ...).

3.7 The test plan

The Disaster Recovery Plan needs to be validated by a test plan that can help to check off each of the recovery measures and their synchronization, then, audit the operational character of the recovery plan through regular tests that closely reproduce real-life situations.

Basically, there are three categories of tests:

- Unitary technical tests: these technical tests are intended to validate a single backup element (for example a backup server): validating the backup configuration, validating the procedures and the return time, validating the choice of responders, validating the relevant documentation;
- Integration tests: the integration tests help to validate the compatibility of the different backup elements, the synchronization of technical operations and the workload on the different teams;
- Full-scale real-life tests: real-life tests have similar characteristics to the integration tests yet they have an additional objective: to test the reactivity of the teams and to verify that the palliative measures run smoothly by monitoring a group of users in conditions similar to a crisis situation (restricted resources, unavailable or limited documentation...). Full-scale real life tests can only be run if all the other tests outlined above have been successful. As they can pose a risk for business it would be wise to evaluate beforehand. The tests can be conducted in isolation (users working in parallel on expendable copies of the production applications), or they can be real, in which case they will be scheduled at the end of the integration tests on work carried out in the production sites. The full-scale tests also help to test the steering of operations (crisis organization and steering tools). Full-scale, real-life tests can also be conducted without advance notice (at least for the operational response teams).

In the framework of the test plan, it is advisable to ensure that the most critical elements of the Disaster Recovery Plan are tested several times a year. As for the number of integration tests or full-scale tests, we recommend 1 to 2 per year. The unitary technical tests should be performed periodically (once every quarter) though they should be carried out systematically after any changes in backup or recovery-related equipment or after any modification that may have an impact on the existing recovery measures.

For each test, the following operations are to be conducted:

- The intended objectives are formalized;
- The test scenario is analyzed and mapped out: preparation, simulation, tested cases, user test methods, tests conducted in isolation or in a real-life situation, validation methods…
- The preparations for the test are finalized: earmarking of the technical and human resources, presentation and validation of the tasks and the scheduling (except if the test is meant to be impromptu), finalization of the relevant documentation…
- One or several observers are designated to follow operations and to note any problems that may be encountered;
- A test review is drawn up and a report is drafted that can validate all or part of the recovery plan and suggest the necessary corrective actions.

4 RECOVERY SOLUTIONS

4.1 Disaster recovery solutions

The overall solution is the result of several solutions that have been adapted according to the specified requirements governing the resumption of activities and the loss of data accepted by the users. All share a certain number of attributes and those attributes can generally be classified into 3 main groups:

a. The way backup resources are managed contractually (How are the conditions governing activation and availability formalized? How are priorities managed in the event that resources are shared?);
b. The type of resources used (fixed or mobile resources, local or distant…);
c. The level of preparation and availability of the resources (are the resources "ready to use" or do they require additional preparation?) as well as the length of time the backup resources can be used (can the resources only be used for a set period in time due to contractual, technical, performance-related or cost-related reasons?…).

A large number of solutions may result from the association of different possible values for these attributes. For example, in a given situation, the optimal solution could be:

Management = contractual agreement with an external supplier for shared resources

Resources = mobile container

Degree of availability = equipment operational without data

In another situation, the following solution may be more suitable:

Administration = internal, with specific resources

Resources = fixed installation on a internal though distant site

Degree of availability = "mirror" configuration

Even so, it is important to note that all solutions worthy of any confidence will need (material and intangible) investment as well as permanent expenditure in normal times. It is dangerous to believe that one can wait until the day of the incident to define the specifics of a backup solution and implement it. In the same way that you cannot and never will be able to obtain retroactive insurance, it is wholly illusory to think that at the last minute we will always be able to use a business relationship or find a supplier who for a price will be able to "fix things" for a while.

The scenarios for the solutions developed during the "Orientation" phase of a Disaster Recovery Plan (cf. §2.2.6.) are comprised of all the measures intended to ensure the continuity of the information systems necessary for the company's strategic business activities, in the face of all the pre-defined risks.

In a distributed IS context, the chosen scenario will generally be comprised of a collection of technical and/or organizational solutions which will be combined according to the situation. These elementary solutions will offer recovery solutions for specific areas, namely:

- the local network;
- the external access points to the network;
- the specifics of the Internet access;
- the backup strategic servers able to ensure 24-hour service;

- the backup servers able to withstand a loss of availability for 24 hours;
- the backup measures for the telephone systems ;
- the backup measures for a call-center ;
- the backup measures for a user platform;
- etc.

Numerous backup solutions are possible, ranging from the establishment and permanent operation of entire duplicate installations, to the formalized mutual assistance agreements between companies.

The overall coherence of the choices made for each of these sub-systems needs to be assured. Before the chosen solution for the scenario is validated, it is particularly necessary to run an analysis of the residual risks in order to verify that the risks that need to be dealt with are done so effectively and that the envisaged solutions do not create new unacceptable risks.

The criteria used to assess a backup/recovery solution can be classified into two groups.

A - Those criteria that help to verify that the solution for a scenario responds to the needs as stated in the specifications of the recovery plan or contingency plan:

- The return time objective: the total return time objective is the sum of the time needed to activate the plan, the time needed to implement the measures (supplying, restoration, tests...), and the time needed to resynchronize the data. These parameters, together with the maximum length of time that the backup installations are available, are crucial in calculating the potential residual operational losses and, by extension, the solution's effectiveness. Particular attention should be given to the length of time needed to detect an event and the amount of time spent in decision-making in order to minimize them both;
- The acceptable amount of data that may be lost between the shutdown and the resumption of activities;
- The level of coverage: does the planned solution cover the risks that have been selected? Which residual risks have not been dealt with? Can the solution be used outside the context of an incident (relocation, conversion...)?

B - Those criteria that help to assess the pros and cons of the planned scenarios:

- The solution's plausibility: a solution may seem viable and reliable at a particular moment, but its guaranteed availability and its ability to evolve over time like the needs of the company are not assured. Furthermore, certain solutions need to take account of the possibility that risks will accumulate – geographical or sector-based… - and finally, the act of conducting realistic tests on a regular basis is a determining factor and proof of plausibility (or implausibility!);
- The flexibility in establishing the Disaster Recovery Plan: it is often difficult to imagine dealing with all unacceptable risks quickly. A flexible solution will work to build an adjustable recovery plan in stages, and in turn enable it to adapt to different constraints (budget, availability of internal resources, synchronization with other company projects, acquisition of know-how, the degree of maturity in the market...);
- The solution's potential to adapt: evaluating its capacity to take account of developments inside the company (technical architecture, organization, the stakes, new risks...);
- The cost: each type of solution comes with a series of fixed, variable, and recurrent costs:
    - The costs to implement the solution ;

- Subscriptions and various contracts;
- The subsequent costs of maintaining and updating the solution (tests, changes in configuration, additional operational costs, consumption...);
- The cost of using the solution (some of these may be covered by insurance).

The summary below reviews the different types of recovery solutions for each of the attributes mentioned at the outset together with their compatibility with the newly-defined criteria.

4.1.1 Types of recovery solutions and the methods used to manage them

A – Types of recovery solutions

Generally, three main types of solutions can be identified and each makes use of resources from inside or outside the company:

Mutual assistance agreements (between different sites of the same company or between different companies):

If this particular type of solution is highly attractive financially (often it involves agreements that cost nothing), it tends to be illusory in terms of plausibility and effectiveness, in particular since the establishment of interactive processes has become widespread: difficulties following up the synchronization and development of "partner" data processing parks, unlikelihood of maintaining over-capacity permanently in each of the sites, underestimating conflicts of priorities and interests that run the risk of surfacing at the time of the incident, the potential for serious legal problems over the validity of the signatories' powers and the transfer and limits of their responsibility in the event that commitments are not respected, the near impossibility to conduct a test, the underestimation or oversight of logistical problems in both time and space (user helpdesk, connectivity...).

For the same reasons and given the lack of professionalism, the notions of the length of availability and the time needed for implementation are immaterial because under pressure from reality, these can tend towards zero and infinity respectively.

The capacity to cover situations other than incidents is generally nil given the potential for cascading impacts.

Given the complexity and evolving nature of information system architecture, this type of solution can only be considered in specific situations and even then only partially.

The use of shared (potentially specialized) backup resources:

In this case, several entities make provisions to use the same backup resources. The different methods of managing these resources will be examined in the following paragraph. In normal times, these resources can be assigned to other low priority tasks to increase their return value (non-repetitive office services, the development and fine-tuning of applications, trials or simulations, demonstrations…).

The solution will likely be acceptable if one is careful to control the number of entities sharing the structures, the homogeneity of the levels of prevention in place among the partners, the non-accumulation of sectoral risks and the quality of the tests.

The cost of this type of solution varies depending on the extent to which the installations are shared, and their potential to be profitable: since the latter may be unpredictable (as

the installations can only host non-priority business activities) the cost may already be significant (several percent of the cost of acquiring the chosen resources).

Protection from damage resulting from error or malicious intent may be planned for if the backup structure has anti-virus reference or if it is fed with data that has been saved according to stringent security procedures.

Still, this kind of solution is not acceptable when, in the event of an incident, it is imperative that the backup resources are not shared (since by definition, in the case of shared resources, the danger of conflicting needs is never zero). As such, it should not be chosen if the entities are subject to service constraints or when the residual risks cannot be passed on to insurers.

Contractual limitations: in the case of shared resources, the contractor (especially if it is an outside contractor) may set time limits on availability in order to reduce the risk that the same resources will be called upon simultaneously.

The use of dedicated (potentially specialized) resources:

Generally, in this category, each entity has an environment at its disposal which it alone has the power to requisition in the event of an incident. This does not exclude the possibility that these installations may be allocated to other low-priority tasks outside crisis situations.

This solution represents the most plausible of all, since we can predetermine with certainty the availability of the resources, the time needed to implement them and the extent of any functional damage. Furthermore, it is easier to conduct frequent tests, and the infrastructure can be used to resolve loss of availability situations when such a loss is not the result of material damage.

The only drawback with this type solution is the cost of creating and maintaining such infrastructures. Generally, such a solution is reserved for situations where availability is essential, or made necessary by the specificity of the equipment.

Logistical limitations: concerning the backup infrastructure, the resources used need to be acceptable, even in the event of prolonged usage of the backup site.

B – Methods of managing backup resources

Generally, we can identify four different ways of managing recovery solutions, according to the level of formalization and externalization:

Formalized external management:

In this case, the backup resources are obtained from an entity outside the company, either from a specialized firm or from another company guaranteeing to free up and/or make the necessary processing capacity available at the time when an incident occurs. The relationship between requester(s) and provider(s) is controlled by specific contractual agreements (in terms of the services required and any contractual violations) and tested regularly (see the “Contract” sheet).

In this case, it is possible to reasonably guarantee a high degree of plausibility and establish the parameters pertaining to time and duration.

Plausibility can be greatly enhanced by conducting contractual tests regularly. It should be noted that pitfalls may be found in:

- the clauses specifying the limits of the supplier’s responsibility, should the latter be unable to fulfill the mission due to conflicts in priorities or technical problems;
- the ability of the supplier to adapt quickly to technological developments;

- the guarantee of I.S. security, notably in the case of shared resources.

In addition, for most of the solutions in this category, it is possible to cover the risks linked to strikes and industrial unrest.

Formalized internal management:

Here, the backup solutions are found within the company (vs. from an outside contractor), and they are controlled, as above, by specific and regularly tested service contracts.

The advantages of this type of solution are to be found in its flexibility and compatibility in terms of needs, usage and development.

In terms of costs, it is difficult to prejudge the appeal of this solution in relation to the preceding one, in so far that it includes some cost-reducing elements (investments stay in-house, effects of scale on existing infrastructure), however these may be offset by other expenses (the cost of the training phase, difficulty in maintaining the solution's level of operability, the need to split investment in the event of diverging material developments at different sites…).

The coverage of risks related to industrial unrest is generally more difficult with this type of solution and one has to be aware of the fact that such problems can easily spread.

Formalized mixed management:

Here, the backup solutions are split between several entities sharing a common interest. The conditions determining how the costs and resources are divided are subject to legal and contractual obligations .

The functional advantages of this type of solution are numerous (overall cost, suitability of the solution, usage for low-priority tasks…), however, working out the contractual fine print is generally a delicate process (attitudes in the event of a conflict of priorities, managing specific needs, managing the situation when member entities follow different development paths, the dangers of accumulating sectoral risks, the admission and withdrawal of members, the attribution and ownership of investments, managing the transitional phase of the creative process, dividing up the various responsibilities of group organization and the administrating resources…).

To maintain the plausibility of the situation (notably in terms of conducting tests, administrating resources, and managing obsolescence), these structures generally entrust the management of backup resources to companies which specialize in that particular area.

Informal management (internal or external):

In this case, the recovery solutions (be they home-grown within the company or outsourced to a third party) are meant to be available outside the framework of a contract: the hypotheses relative to the time needed to implement the solution, to the length of time it is available, to the accounting of equipment and software, to the limits of responsibility... are not documented and/or countersigned by the different parties concerned.

This type of management style can open the door to significant legal risks and major disruptions at the site where it is being applied. It can also provoke major difficulties in the setup and test phases.

In the age of shared computer networks and the increasingly strategic character of IT communication resources, informal management should be prohibited.

4.1.2 Type of resources brought into play

A Disaster Recovery Plan must enable the processing of both a technical incident and a major disaster. The following table offers a series of solutions for consideration. These may be local or external depending on the company's requirements for the availability of its information systems.

These solutions will be developed at the end of the chapter.

	High Availability	Medium Availability	Low Availability
Sub-systems	Immediate or quasi-immediate resumption (a few minutes). Minimal loss of data.	Recovery in a few hours (less than 12 hours). Limited loss of data (a few minutes to a few hours).	Recovery in 48 hours or more. Loss of data generally less than 24 hours.
Strategic servers	Dedicated backup servers, geographically distant, internal or external, in operation (applications and data). High availability architecture: load balancing, server cluster, mirroring solutions (applications and data).	Internal or external geographically remote dedicated backup servers, interconnected with the principal servers. Ready-to-operate systems: remote mirroring or remote copying of updates and periodical updating of the backup databases.	Internal or external geographically remote backup resources that may be shared.
Local network	Redundancy. Backup hardware and emergency bypassing with automatic switchover.	Backup hardware and emergency bypassing.	Flying cable kit Existence of external pre-cabled backup user sites that can be equipped rapidly (work station, equipment ...).
External network access (voice, images and data)	At least two separate external inlets, if possible on two distinct sites and via different operators. Switching over of communications to the backup site in the event of an incident, with a maximum of automatic functions. Creation of redundant links in the company network.	External backup node with automatic or manual switchover (parameterization) . Contract obligating the operator to intervene and get the connections operational again in a set timeframe. Spare equipment.	Commitment from the supplier to intervene with an obligation to guarantee results. Calls forwarded to a backup site by the provider.
Telephony (equipment)	Backup PAX, preferably at a different site to the main premises with automatic switchover of communications.	Contract obliging the provider to forward calls to a backup site that is equipped to accept those calls (the necessary telephone equipment and human resources in place).	Backup PAX. Calls forwarded to a backup site by the provider. Creation of a pre-recorded message.
Internet access (web site)	Double connection to the Internet at each site (main site and backup site) with different access providers. The switchover can be automatic due to a DNS update and/or a policy of “peering” between access providers.	Internet connection at the backup site with the manual switchover of connections from the main site to the backup site by DNS update.	Internet connection at the backup site with the manual switchover of connections from the main site to the backup site by DNS update.

Before deciding on the IT resources to set in place, it is necessary to examine the type of infrastructure in or from which they will have to operate. In effect, there are four principal types of infrastructure:

Fixed installations:

Two types of usage can be considered:

- either one (or several) remote IS sites integrated with production and capable of providing the immediate backup of I.S. resources;
- or one (or several) remote site(s) that can be used in the event of an incident.

Remote I.S. Site integrated with production and capable of providing the immediate backup of I.S. resources:

This solution corresponds to the requirements of high availability and to the constraints of real time without loss of data. It leads to a doubling of computer equipment, but in the event of an incident, it lightens the business return time procedures considerably. The cost of the solution needs to be assessed in its entirety.

The choice of architecture depends on what is required in terms of the RPO and the return time objectives.

Whatever the architecture, these solutions assume that a backup copy of data is available on the backup equipment and the up-and-running ready-to-use servers.

What differentiates the various possible architectures is:

- how often the remote backup copy of data is updated (cf. replication, § 4.4.2). This may be instantaneous or deferred for several minutes or several hours;
- whether or not the equipment at the second site is involved in the production process. Such involvement could be achieved by spreading the load of the same application between both sites. This would assume the complete mirroring of data between the two sites, or by spreading the production applications over the two sites with each application having a backup copy at the other site. The latter case is technically less complex than the former and it can support deferred replication.

The completeness of the solution is closely linked to the capacity of the operating systems, and the systems managing the databases and the applications.

Remote site that can be used in the event of an incident:

This solution is the more traditional; in the event of activation, a team of employees from the entity affected (IT technicians and probably users) travel to the backup site to continue carrying out transactions and running processes. Generally, this type of solution has limited telecommunications resources and above all excludes the remote connection of the regular terminals (the solutions based on sophisticated telecommunications are examined in the following paragraph).

These solutions have significant negative consequences in terms of organizing the work of the operational teams (traveling, possible breakup of the teams, changes in inflow / outflow, remoteness of archives and documentation), and can only function effectively if the backup centre is not too far from the site needing to be protected (which leads to vulnerability vis-à-vis sectoral risks).

Backup user sites:

The user backup plan is defined in the framework of the Business Contingency Plan and as such does not fall within the realms of this document which is centered on the Disaster

Recovery Plan (DRP). Nevertheless, when choosing a backup site for the company information systems, it would be wise to take account of the possibilities of access to those sites that are liable to host users.

In the case where the Disaster Recovery Plan study is part of a wider project, the choices made to host the users can have an impact on the sharing of certain backup material between the site providing the backup for the information systems and the site set aside for the users (notably for performance-based reasons).

Mobile resources:

With this type of organization, after an incident has been declared, one needs to transport and install the infrastructure for the information systems, either near the affected site, or near another backup site (whether the latter has been planned for or not).

Generally these solutions are made up of either modular container-type structures or inflatable tent-like units. In both cases, they come equipped (as standard or as an option) with air conditioning equipment, generators, security systems, and pre-wired material... They may or may not be delivered with the necessary human and processing resources.

The advantages of this type of solution reside in their flexibility and their ability to adapt to the real life conditions of the incident and to limit the disruptive effects for the users, the teams of computer technicians (who remain close to their regular environment as well as the users), and the information input/output circuits. In addition, reconnecting the network is relatively easy, if precautionary care has been taken to separate the head-ends.

Clearly, these solutions are only viable when the geographical and topological situations are suitable (which generally rules out densely populated urban areas).

Evidently, the initial return time is hampered by the time needed to transport and assemble the installations –and an awareness of the imponderables linked to that transportation.

Service integration:

All of the solutions outlined above might – or might not be – added to the provision of services (provided by teams inside the company, or by outside contractors).

It includes among other things, help in fine-tuning the Return Time Plan for the site being protected, help setting up and laying out the infrastructure (hardware or software), help with tests, help at the re-launch phase, help storing duplicate equipment or supplies specific to the protected site, help storing saved data, help providing operating staff, managing constraints, providing additional insurance, supplementary expenses and recreating media...

4.1.3 Level of preparation and availability of resources

For reasons related to the cost / performance of backup resources, a situation may well arise in which solutions are defined requiring varying degrees of operational preparation. As such, different levels can be envisaged:

Hard ware environment for back up

With these solutions (also called “hot sites” even when it involves mobile resources), all the backup computer equipment is present in the backup infrastructure. Naturally, this equipment is maintained in constant working order, but the programs and data of the entity that will potentially be using it are not loaded (this may extend to the operating system).

The level of plausibility is high, on condition, of course, that exhaustive tests are conducted regularly.

Evidently the costs are significant, and they often will account for a percentage of the IT budget, even for shared installations with reasonable conditions of probability for the simultaneous use of the resources.

The return time may be measured in dozens of hours, since it will be necessary to reload all or part of the operating system by adapting the parameters, reloading the user applications and data, rebuilding lost information due to the backup cycle, and re-synchronizing the applications...

Partial or total “mirror” environments:

Here, not only is all the equipment operational around the clock, but all or part of the operating system, programs, and data of the user entity are permanently on site.

Given the architecture of the systems and the technology used, this type of environment is not compatible with shared solutions.

Even when one manages to share the resources, these solutions are expensive, because they require significant alterations to the infrastructure to enable the permanent feeding of fresh data and to ensure the duplication of local networks and remote networks. However, doing so can help to reduce (though certainly not eliminate!) backup procedures, in so far that the same information is available simultaneously at two different sites (naturally, this assumes that the mirror configuration is at a reasonable distance geographically from the site being protected!).

Naturally, the level of plausibility that can be expected is the maximum, because the logistical constraints and the switchover time are practically zero. The risk that the installations will become desynchronized is high, and the constant maintenance of logical consistency is a major problem.

It should be noted that this type of solution has a peculiarity that makes it more sensitive to intangible incidents (errors, sabotage, virus): any operation carried out on the main installation will be immediately activated on the mirror installation, unless complex filters are installed.

A certain gradation can be considered in these solutions :

- So-called “first response backup” or “stand-by backup”;

  It refers to those limited yet highly specific backup resources that allow for the quasi-instantaneous resumption of the most strategic applications, enabling a type of system “afterglow” that lasts for a few hours during which the main backup solution (or so-called “heavy backup”) is reloaded.

  Typically, they are dedicated to highly transactional rapid cycle systems (Computer Aided Management and Manufacturing with tight flow, running cash registers or ATMs, EDI with timed mailbox pickup, Web servers…).

Generally, they are built on a specialized branch of the network. As such, they are constantly "listening" to the transactions to keep their files up to date. In addition, some are able to start up automatically when no signals are received from the installation they are protecting. Clearly, due to their limited size, their performance value and the relevance of the data they contain deteriorate very quickly once they go into stand-alone mode, but this should be enough to guarantee a relay.

Given the limited architecture of this solution, the operational costs can be reined in, especially if the resources can be shared. Conversely, the research and setup costs may be high because the characteristics of the minimal functional core need to be analyzed.

- So-called "split production" resources;

  In this case, the two centers (the one being protected and the one acting as backup) are both constantly sharing the workload; all the files and access to the strategic network are duplicated, and updates are made as they arrive. Ideally, the processes are carried out equally (and alternatively) on each of the sites from either one of them.

  Naturally, in the event of an incident, with these solutions it is necessary to accept a high degree of deterioration though starting up again can be fast and reliable. However, intangible damage (such as a strike) remains a difficult factor to tackle.

  The costs are significant though not nearly as expensive as the solution below.

- "Complete mirror" environments.

  In the most extreme case, all the strategic activities of the production environment are constantly replicated in the backup environment thus, it is the only task. Unlike the preceding solution, the backup environment does not participate in day-to-day production.

  Clearly, it takes less time to start up again and there is less functional deterioration.

  The costs of possession are very high and can effectively lead to a doubling of the operating budget.

4.2 Telephone systems backup

4.2.1 Network connections

The first area of vulnerability concerns the physical access to the public network. Generally, there is one access point or it is backed up by a second cable passing through the same duct.

Different levels of backup can be considered for the secondary connection:

- A dual connection to the local loop. The two connections are physically distinct and separated. This type of solution can be envisaged when the site allows for it (a campus, a building having access on several streets...);
- A dual connection to the locale loop with access to two different exchanges. This solution helps to protect against a variety of risks, including breaks in the connection, failure of the local loop and unavailability of the telephone exchange;
- A physically distinct backup connection to a second operator;
- Other on-site back up solutions may be envisaged depending on local conditions.

4.2.2 Telephone backup resources

Particularly sensitive in terms of security, the private automatic exchange (PAX) remains the indispensable link of every company with respect to telephone communications and in some cases even IT communications.

Depending on the nature of the risks that need to be covered and the length of time an interruption can be tolerated, numerous backup solutions can be envisaged:

- A duplication of the PAX equipment and wiring: central PAX and satellite PAX(s) with directory duplication, in different buildings if possible;
- Automatic call-forwarding to a secondary operational site in the required timeframe;
- A contract that anticipates the delivery of mobile telephone backup equipment in a set and verifiable timeframe;
- Direct lines that do not pass through the PAX.

Note: in the case of IP-based telephone services, one can also refer to the section on backup solutions for computer networks.

The use of GSM equipment may be envisaged, but in the case of major disasters affecting a large number of people, this solution can prove to be totally ineffective due to network saturation or disruption of the relay transmitters. It is therefore important to anticipate other backup solutions (Positioning the PAX at another site, backup lines to an operator centre, Internet, or other means of communication).

It is clear that bundles of lines have to be negotiated with the operators, yet these will never be able to cover all needs, primarily for budgetary reasons.

4.2.3 The routing of telephone links (on a single number)

In cases where backup telephone equipment is available on a remote site, the problem of forwarding the incoming calls to the new site comes into play.

It is possible to draw up a specific call-forwarding contract with the telephone operator to ensure that calls are transferred from the affected site to the backup site.

Two solutions can be envisaged:

- Either the rerouting of all the Direct Inward Dialing numbers to a single number;
- or the identical rerouting of the Direct Inward Dialing numbers from the affected site to the backup site.

In the former, it is necessary to anticipate incoming call-filtering by an operator yet this can create problems when there is a mix of voice calls, faxes and data transmissions. If this is the case, a pre-PAX filtering of the ISDN frames can be envisaged on condition that the number initially being called is relayed by the operator.

In any event, a technical feasibility study needs to be conducted by the operator depending on where the site being protected and the backup site are located.

Note: an alternative solution could be to ask the operator to prepare a pre-recorded personalized message setting out the new calling options.

4.3 Salvaging the premises and the equipment in it

In the case of material damage (fire, water damage...), it would be wise to preserve as best as we can everything that can be saved in order to facilitate a future return to the site or the retrieval of data from the damaged machines.

More particularly, the following measures should be studied:

- Security protection of the affected site to prevent theft and acts of vandalism or to preserve possible material proof of malevolence;
- The commissioning of companies specialized in salvaging sites and equipment: in the event of a fire for example, numerous pieces of equipment may be damaged by smoke or corrosive fumes. By intervening quickly, such equipment can be quarantined in a controlled atmosphere to stem the progression of the corrosion. A cleanup operation can then be undertaken;
- The commissioning of companies specialized in reconstituting information (flooded archives damaged disks).

At the very least, in the Disaster Recovery Plan, one should maintain an up-to-date list of companies able to intervene.

4.4 Backup / recovery

A backup/retrieval plan is a key component of the Disaster Recovery Plan. In any circumstances, it has to guarantee that the relevant information and the strategic tools are recovered through specifically adapted resources and the use of strict run and control procedures. The nature of the supports and the rules governing their use and preservation are vital to the quality of the backup copies and their retrieval.

4.4.1 Types of backup

The types of backup can be differentiated according to usage and by the way they are made.

Depending on what they are intended for, we can distinguish between production-based backups and loss recovery backups. The first are meant to respond to a common operational incident such as the overwriting of a file. They need to be quickly accessible and can therefore be stored on the operating site. The second are intended to respond to a major incident requiring the use of outside resources. Specifically, they need to respond to the destruction of the operating site and it is therefore imperative that they are transported to a remote site without delay. The loss recovery backup (or backup of “last resort”) has to be totally reliable and can only be used on the specific authorization of the crisis organization. In order to guarantee their reliability and their integrity, they need to be produced according to strict security procedures (secure backup procedures that are different from the operational backup procedures, reinforced controls, reinforced security for transfers and the storage site).

A third category of backups can be considered for archiving purposes. In the case of archives, the return time objective is generally less than for the other two categories but the nature of the proof often needs to be preserved in it.

Finally, it is always wise to make a backup copy prior to any high-risk operation on the disk (maintenance for example or change of release) or on the configuration.

Several ways of making backups can be envisaged:

- physical backup;
- logic backup.

4.4.1.1 Physical backup

It involves the volume-by-volume backup of all or part of the data.

It is used to restore a disk after an operating incident (a head crash, the problem of sudden, untimely shutdowns...). It is preferable that the length of time these backups may be conserved be researched. They can also be used in the framework of a recovery plan if the backup configuration is identical and if the equipment allows it.

The use of RAID disk technology can also respond to these types of operational incidents by replicating data on different disks via a system that continuously replaces the production components.

4.4.1.2 Logic backup

Backup by logical entities.

4.4.1.2.1 Complete logic backup

It is essentially used to reconstitute the information system on a backup configuration that is more limited than the original configuration. The principal advantage is that it facilitates the synchronization of data. On the downside, though, its run time is long. It would be appropriate to ensure the consistency of the recovered system levels, applications and data.

4.4.1.2.2 Incremental backup

It consists of making a backup copy of the files which have been modified between two specific points in time.

This type of backup is often indispensable if it takes too long or is impossible to make a complete backup each day.

It requires an organization (computerized or manual) that can help to identify and locate the formats and the backup files.

Incremental backup is fast but it should not be used over an extended period, because there is a danger of inconsistency. As such, a complete backup is needed and that copy must still be of use for the users. This type of backup often goes hand in hand with a complete backup.

4.4.1.2.3 Application backup

It involves the saving of all the files necessary for the effective running or recovery of an application.

This type of backup helps to ensure the consistency of the information, particularly in the context of recovery plan when the choice of either the partial or total recovery of an application is being decided. If necessary, specific security procedures (transportation, security seals, audit...) will need to be planned depending on the strategic importance of the application.

These backups are linked to the production cycle. The frequency that the backups are made will depend on the number of processes being run.

4.4.1.2.4 Logging

Logging consists of creating a log of all the updates made on a given file.

In the event that there is a problem with the file, the most recent backup will be recovered and all the updates recorded in the log will be applied.

Generally, the database management system has logging procedures. Even so, in certain cases, it may be necessary to plan this logging at the development stage of the application.

Depending on how often the base is updated and the acceptable time needed to recover the data, the logging may be effectuated over different periods (daily, weekly...).

The difficulty with logging procedures rests in the synchronization between the general backup and the start up of a new log. This difficulty is particularly acute in the case of around-the-clock services.

The logs can be the object of a specific backup to enable recovery of the most recent data.

4.4.2 Duplication, backup and recovery techniques

The choice of backup/recovery techniques depends on the operational demands (the freshness of the data needing to be recovered, the time it takes to become available, consistency between all the data recovered) as well as the technical constraints (the time needed to move data to the backup site, the volume of data to recover, effectiveness of the backup and recovery tools). The combination of these objectives and constraints leads us to envisage the following techniques:

4.4.2.1 Replication;

Replication consists of duplicating the information on remote disks in order to lighten or even dispense with the recovery phase. The updates are sent to the remote site at regular intervals and then integrated into the backup copies of the production disks. The various replication solutions differ depending on how often the updates are sent and the time it takes before the backup supports are upgraded.

It is important to note that should the production data be impaired, the data on the backup site is also impaired. As this solution does not have a recurring loss recovery backup, the content needs to be guaranteed.

4.4.2.1.1 Case 1: Immediate replication

Immediate replication is assured directly by the system, the application or the database management system. It works to pass on data modifications on the production environment and on the backup environment instantaneously.

In this case, the loss of data is zero or practically zero and the return time will depend solely on the level of preparedness of the servers and the network.

4.4.2.1.2 Case 2: Updates are passed on at regular intervals

Updates are passed on at regular intervals (a few minutes to several hours) to the backup site, or as in the previous case by the application or the Database Management System, or by a specific operation (developed backup software, update log transmission). The application of the updates on the backup supports may also be deferred and with a different schedule (example: daily upgrade after validation of the stable state of the production data). In the event of an incident and depending on the nature of that incident, the most recent updates received may be applied to limit the loss of information (on condition that data synchronization has been maintained).

4.4.2.2 Traditional backup.

The traditional loss recovery backup consists of duplicating the relevant information (systems, applications and application data) on the detachable supports and transporting them without delay to a secure and distant storage site. The length of conservation is the optimum time between the need for an update (processing, reuse) and the capacity to realize the operation (processing time, software and hardware consistency).

The logical, technical, volumetric and financial constraints often require that recovery plan be organized to allow the mixing of different solutions. For example, physical backup for the system disks, incremental backup for the batches, logic and logging for the bases.

It is advisable to give special attention to the synchronization of data and the application systems during backup and recovery operations. It is necessary, for example, to specify the patches from the editor that need to be applied during recovery.

The management of the backup supports and recovery procedures can be automated by using a special backup / recovery software coupled to a robot.

RELATIONSHIP BETWEEN RISK & BACKUP

USE	CATEGORY			PLACE OF STORAGE		LENGTH OF CONSERVATION	
	BACKUP		ARCHIVING				
	PRODU-CTION	LOSS RECOVERY		ON SITE	OFF SITE	TEMP-ORARY	LONG TERM
Operational Incident	X			X		X	
Making the application available again	X			X			X
Audit	X or X		X	X or X		X	X
Legal availability			X	X or X			X
Damage		X			X	X or X	

Table 1: Relationship between risk and backup

4.4.3 Data synchronization

Data synchronization is a significant problem to deal with in a backup/recovery plan. A simple way to resolve this is to halt the updates on all the data needing to be synchronized while the backup copies are being made. Unfortunately, this solution is becoming less and less practicable because the window needed to make the backup copies is often insufficient, and in some cases non-existent.

As such, other solutions need to be found:

- Replication (see above);
- The "snapshot" technique offered by some tools (Database Management Systems, backup software...) consists of taking a freeze-frame snapshot of the state of the files at a given moment "t" and then using that freeze-frame view to make the backup copy while at the same time allowing the continued updating of the files.

4.4.4 Backup / recovery solutions.

At the present time, there are two major types of backup resources:

- Centralized or "proprietor" resources which are single operating systems;
- Backup systems by distributed architecture on the client-server model which are capable of operating in multi-system environments.

Given the development of computer architecture over the last few decades, open systems currently dominate the market.

4.4.4.1 So-called centralized architecture

The particularity of these backup systems is that they are just as capable of generating physical copies (a disk, a collection of disks or an entire server) as logic backup. They are run by one of the servers, thus they ensure the backup and help to form the bootable supports, which are extremely useful when a server needs to be completely reconstructed. Depending on the configuration and the volume of data needing to be processed, these backup systems are linked to the server peripherals which host them or to more complex robotics.

4.4.4.2 Distributed or client / server architecture

In theory, the backup system is installed on a dedicated server to which one or several robotics on channel or network function are linked. All the backups are managed by a catalog (a highly sensitive entity) which itself needs to be backed up regularly.

The servers needing to be backed up are connected to the backup servers either by the company network or via a dedicated network if need be, and the client software is installed on both of them. In the case of the former, it is advisable to size the network so as not to disrupt regular operations.

Backups may be activated by:

- the backup server itself via the task planner (time activation);
- or by the client agent who may be conditioned by an internal or external event (event-driven backups). Example: a backup operation is activated before or after a specific process.

The backups are called logic (file by file, or directory by directory) and more often than not they are described explicitly, which involves a rigorous backup plan with the appropriate control mechanisms. The backups may be total or incremental. These backup systems are unable to generate so-called “bootable” supports, therefore, the data, the resources to rebuild each operating system, as well as the server and backup software themselves will need to be stored independently.

4.4.5 Procedures, tests, and follow-up

The backup copies need to be the object of procedures written by the technicians. The restoration should also be the object of written procedures specifying among other things the individuals who are authorized to activate it.

These procedures are necessary but they also need to have on a daily basis:

- a control panel of performance indicators to monitor the backups;
- centralized reporting of warnings indicating problems while making backup copies with a review and appraisal of the warnings as per written instructions.

This will give added reliability to the backups as well as to the restorations that will need to be undertaken in the event of an incident.

Complete and / or partial restoration tests need to be conducted at regular intervals in order to verify that the procedures are followed and up-to-date and that the backup copies are functioning well. These tests will need to be monitored and reported to ensure that any malfunctioning is corrected.

4.5 The recovery of printing and mailing resources

The recovery of printing and mailing resources poses specific problems. Generally, backups of these are not supplied directly by IS backup providers. One can either research the possibility of an internal backup solution by physically separating the different lines if several writing lines / fold-and-insert systems exist, or the task can be outsourced to certain professionals such as printers or companies specializing in mailing. These solutions can also help to absorb the printing workload during busy periods.

As with IS system backups, these solutions need to be the object of a contract and they should also be tested regularly.

Other elements also need to be taken into account:

- The stock of printed data;

  Make provisions internally or through a supplier to store printed data off site. In the case of off-site storage, it is necessary to monitor the storage conditions of the paper and to ensure rotation to limit deterioration through age (print quality, keeping the printed data up to date).

  In the case of graduated prints or plain paper, the following should also be assessed;

- The contractual aspects (stock conservation, equipment availability...);
- Relations with the mail delivery companies.

  The circulation of documents in a recovery situation needs to be planned in advance. The backup solutions for regular mail will be covered in the framework of the Business Continuity Plan. However, the mass dispatching of computer-generated data needs to be covered in the Disaster Recovery Plan. It is advisable to coordinate with the companies concerned, especially when the volume to be processed by the backup site is large. A shuttle system may be organized to deliver the printed data to the backup site be it in-house or run by a partner company;

- Postage / franking;
- Special equipment: anticipate the backup of signing machines;
- The confidentiality of the documents produced;
- ...

4.6 Backup Internet access

4.6.1 The Internet connection

In terms of Internet connections, the first point of vulnerability for a company is its access to an Internet Service Provider. Different solutions may be envisaged:

- Two distinct connections to the same ISP (one master, the other slave) but on two different network cards;
- Connection to two different ISPs with traffic shared between the two IP addresses;
- Connection to two different ISPs (on master, the other slave) with a traffic exchange agreement between them (so-called “peering”). As such the company retains the same IP address during and after the switchover;
- Redirecting Internet flow via the company’s internal network to another access point when the principal link becomes unavailable.

4.6.2 Rerouting Internet flow

When the backup site becomes operational, several solutions can be envisaged:

- A backup connection to the same ISP in order to retain the same ISP address;
- A new Internet access connection completely separated from the one at the affected site. In this situation, a range of IP addresses that meet the requirements of the backup site need to be reserved in advance and the company's DNS details need to be updated with the new ISP address at the time of start up.

4.7 The contract for the backup resources

Irrespective of the backup solution chosen (internal, external, re-manning the cold site...), it is crucial to formalize relations between the user of the backup resources and the entities which make available all the resources needed to guarantee continuity of service (servers, network, work stations...).

In the following examples, we generally use terms like "subscriber", "service provider", and "contract", bearing in mind of course that this relationship can apply to any scenario (clients / service companies, divisions or entities within the same company, user companies linked by reciprocal agreements...).

As such, the following text will need to be adapted as some clauses may not be applicable nor may need to be extrapolated according to the resources and relationships concerned.

4.7.1 Object of the contract

The “contract” linking the “service provider” and the “subscriber” must first of all indicate the general purpose of what both parties are committing themselves to:

- The nature of the resources being made available and the conditions setting out their shared use (fixed or mobile environment, with or without telecommunications...);
- The situations that will make the backup resources available (material damage, intangible damage, peak limiting, voluntary loss of availability, such as migrations, relocation, strikes...). It is preferable that all exclusions be mentioned explicitly (via the formula "everything except...") ;
- The time allowed to making backup resources available and the maximum length of time they can remain at the subscriber’s disposal;
- etc.

4.7.2 Detailed description of the “services”

This clause specifies the resources that are to be made available, the place where they will be made available (in the event of a limited incident, a specific clause can be added that allows for the backup equipment to be delivered to the client by the service provider) and any additional services that may subsequently be provided. For example, does the “service” include the assembly and startup of the equipment, the configuration of the system (standard or custom), the connection to the local and remote networks, the reloading of the “subscriber’s” data, technical assistance / operating staff?

Depending on the choice of solution, the legal issue of whether the company has the right to use the software at the backup site needs to be researched.

At this point, the exact length of time the backup resources are available should be specified (how long the contract is valid, extension clauses, the time needed for the backup resources to become fully operational or conversely their progressive reduction...). Evidently, the clauses must be consistent with the general restocking and reconstruction times for the technology used.

4.7.3 Activation procedures

The “service provider” needs to specify in detail the terms and conditions governing the activation of operations (procedure, resources used - telephone, fax, written confirmation – the times of day that the service provider’s call center is open, public holiday restrictions...).

More particularly, the “contract” must include a complete list of the “subscriber’s” representatives who are authorized to activate an emergency response, as well as the call authentication and logging procedures.

Certain “contracts” may include a two-stage activation procedure (an initial alert, triggering a warm up phase at the backup site, followed by the definitive confirmation from the subscriber, after the latter has made a detailed appraisal of the damage and followed the escalation procedures).

4.7.4 Conditions of use

In the event that the backup solution involves a fixed site, the “Contract” should clearly specify the opening hours of that site, the security procedures, the procedures controlling access, plans of all the entry points, availability of parking… It may be preferable to integrate all or part of the site’s in-house regulations into the contract as well as to specify the situations which may engage the responsibility of the “subscriber”.

In cases where the service provider makes a private room permanently available to the client for the strategic backup servers, the contract should specify the level of security needed to guarantee the protection of the client's equipment (controlled entry, fire-prevention measures, electrical feeds...) and to guarantee and secure all external exchanges. The contract should also specify the entity which will manage operations and, where applicable, the sharing of responsibilities in terms of operating the equipment.

4.7.5 Logistics

The "contract" needs to take into account the logistic implications identified in the continuity plan (telephone, fax, network access, printing, Internet access, telex, secretariat, accommodation for the "subscriber" teams, installation and/or storage of additional materials...). In addition, given the pressures that the teams will be under, it will be necessary to ensure a minimum level of comfort for them.

4.7.6 Tests and dry runs

The backup solutions will only have meaning if they are tested regularly. It is therefore essential that the parties involved agree on a timetable and a protocol for regular tests. These tests should be an integral part of the "contract" and be the object of co-signed reports. The contract should specify the consequences for the "service provider" or the "subscriber" should either one fail to respect this clause.

Certain backup solutions are difficult to test (reciprocal agreements in the absence of overcapacity, re-manning of the cold site, transfer of users, service disruptions), however, it is crucial to test as far as is humanly possible. A backup solution that is impossible to test bodes ill for its implementation in a real situation.

Each service provider must undertake to ensure and test its interoperability with the resources of other service providers. The contract should include an appendix with the relevant contact information for each of the different service providers.

It is advisable to give the contract between the service provider and the subscriber a clause that would only make it valid after the completion of thorough tests that are the subject of a contradictory protocol (suitability of the configuration provided, tests of the interfaces and networks, printers...).

4.7.7 Managing priorities

With the exception of mirror configurations where all the critical equipment is replicated at the backup site, the majority of backup resources are shared between two or more entities and the whole is limited in terms of hardware and installations.

As a result, it is possible that these entities may call on the same resources simultaneously. It is essential then, to define the guidelines and priorities clearly so that conflicts of access can be resolved immediately. At the very least, the following factors should be taken account:

- The cause of the request for intervention (major damage, partial damage, a spike in traffic, tests, anticipation of a quasi-certain event...);
- the type of use requested / possible (exclusive, shared);
- The length of time the resources need to be available (as much the length of time requested as the maximum time remaining as stipulated in the contract, since a system of decreasing priority over time can be developed);

- In the case of a client-external supplier relationship (though the same could just as well happen with an internal relationship), the different customer categories could end up competing to acquire the resources. Similarly, reciprocity within the contractual relationships might also come into play (a one-off client, an office service subscriber, or a manpower subscriber versus a full service subscriber...).

Such priority clauses may take into account the potential availability of the backup resources from the secondary service provider. If these resources are inferior to the primary resources, there may be reason to define the compensation that will be guaranteed to the subscriber to make up for the net loss in service quality.

Such causes could, by extension, lead the subscriber company to beef up its Recovery Plan (by developing hypotheses such as: "if the primary Backup Center is not available, then...").

4.7.8 Commitments and responsibilities

The service provider must indicate the maximum number of "subscribers to whom it may commit to providing assistance within a given environment.

In the case of a client/external supplier relationship, this notion takes on particular importance, since it evokes the probability that the supplier will be overwhelmed. This in turn opens the door to a possible conflict of priorities that is liable to leave one or several customers dissatisfied.

This is all the more serious since most external suppliers of backup resources only take responsibility for the means they are committing to provide (they make "all they can" available for their customers), and not the end result for the customer / subscriber (in the event of an incident, the supplier can only guarantee that he will be able to satisfy a given client because his resources are limited).

It is not possible to make a recommendation as to the optimal number of sites that can be supported: in effect it is a question of balancing between the cost of the service (inversely proportional to the number of sites protected) and the probability that requests for intervention will "collide". Now, the latter parameter varies considerably depending on the technology involved (shareable or not), the quality of the customers' preventive measures, and the overall size of the service provider (law of large numbers), customer psychology ("better a small contract than nothing at all", or conversely, a quest for "custom-made"), ...

The extent to which resources are shared has to be systematically examined case by case, according to the technology used (shareable or virtual operating systems, the average delivery times for new and used hardware), the professionalism of the partners, the nature of the risks covered, and the potential increase in risks for the company (its exposure to acts of malicious intent, the increased stakes, the potential accumulation of risks at the service-provider level... see the last paragraph of this chapter).

In any event, the "contract" must specify the responsibilities of the "service provider" when the latter is unable to respect its commitments or whether the rules setting out the order of priority have been rigorously applied or not. The contract should also set out the limits of that responsibility.

Finally, it is only natural that the "service provider" be freed of responsibility when it comes to the quality of the "subscriber's" programs, data, procedures and backup copies (this again underscores the fact that it is almost impossible for a "service provider" to guarantee results).

4.7.9 Financial aspects

The organization of backup resources often translates into a significant investment in terms of time and material.

As such, it is necessary that the associated costs are clearly defined. Beyond the cost of developing a recovery plan, one needs to consider:

- the potential costs of subscribing to a backup service. This should be taken into account even in the case of reciprocal or in-house agreements, since the "subscription" helps to complete the equipment and thus honor the commitments. In the case of outside suppliers, the subscription will help to finance shared equipment and to keep the entire "first-response" structure permanently operational. As a result, the cost is proportional to the chosen configuration;
- The cost of activating an intervention (cost of preparing and conducting tests and real interventions);
- The effective cost of use, during and after the base length of usage as set out in the contract. This may be linked to the amount of power that was really consumed (and of course the length of use). It is commonplace to set rates that increase over time as this encourages the "subscriber" to free up the backup installations as quickly possible. These may also vary depending on the extent of the usage.

Analysis shows that costs vary considerably from one type of service to an another: certain subscriber contracts may have a high price tag, but the actual costs of activating and using the resources are covered by that cost. Conversely, some solutions may have lower subscription fees but the costs of usage - be it for a test or for a real incident - are high.

All of these costs may be itemized as a "basic service" and additional services (help re-starting the systems...).

For example, some "contracts" (notably those with outside suppliers) may be supplemented with insurance contracts covering the costs engendered by the real usage of the backup resources (clauses entitled "additional charges" or "Reconstitution of Media"). As such, it is necessary to specify the amount of capital guaranteed, to determine who pays for the insurance and to make sure that the clause specifically covers all expenses linked to the implementation and operation of the backup resources during an incident.

4.7.10 Evolving configurations

Computer configurations change rapidly. It is preferable that the "contract" adapts to those changes by taking account of the evolving situation of the "subscriber" and possibly that of the "service provider" (this point, obvious though it may seem, is often overlooked in formal and informal reciprocal agreements. which are often based on a vague similarity of the configurations at the time of the agreement, but deliberately ignore that they will probably diverge very quickly).

It is important that the "contract" specify the duration of its "technological" validity, the measures that are to be taken to keep both parties informed of developments, and the implications resulting from the need to change one and/or the other configuration.

4.7.11 Confidentiality

It is common for the "service provider" and the "subscriber" to sign a reciprocal confidentiality agreement (particularly if the subscriber wants to be covered against fraud, malicious intent, strikes...).

For certain sectors, this notion of confidentiality may have a significant impact on the way the tests are conducted –and by extension, the costs (for example, a ban on using outside staff to oversee the reconfiguration and reloading of data and the destruction of magnetic supports after use, impossibility to use the configurations and/or shared networks...).

4.7.12 A few recommendations

The most sensitive points with such contracts are as follows:

- Secondary backup: the "service provider" must, do everything possible to provide a backup solution should the service provider's own installations become unavailable (following an incident, an overload, a strike, or loss of access...). Similarly, it is preferable that the service provider undertakes to inform its subscriber(s) of any situation that would prevent it from honoring its primary engagements;
- Accumulation of risks: it is important to verify that the service provider is not in a situation where competing requests for the backup resources are likely to occur. For example, corporate-style backup solutions (economic interest groups and others) are attractive yet a strike in the sector may prove disastrous. The same may be true for an accumulation of geographical risks. It is advisable to include a predefined safety zone in the contract inside of which the service provider undertakes to supply the requested resources even in the event of competing requests for those resources;
- The limits of responsibility: as indicated above, cost and degree of certainty regarding availability are two opposing parameters. In short, a solution that is totally reliable risks having a prohibitively high price tag, which undermines the whole point of having that security. Conversely, a "low price" solution may prove to be wholly ineffective;
- Transfers of resources to the service provider: in the case where the contract also anticipates the use of resources made available by the client (software, data, human resources...) the responsibilities need to be specified, particularly vis-à-vis the respecting of regulations.
- Respecting guidelines governing the number of subscribers and the implementation of priorities: in the case of customer relations / external suppliers, it is commonplace (and normal) for the service provider to refuse to divulge the identity of its other clients, as this would undermine the accepted rules of confidentiality. However, this may be in contradiction with the need for transparency and the effective implementation of contractual agreements in terms of the maximum number of subscribers, and the rigorous application of the rules governing priority in the event of competing requests for access. It might therefore be preferable for the contract to identify a third party, who, bound by the rules of confidentiality, would have the authority at any time to audit the physical nature of the services, the professionalism with regard to the management of the backup installations and whether or not the rules set out in the contract have been respected.

In conclusion, the "service providers" can only take responsibility for the resources. It is up to the "subscriber" company to ensure that the service provided truly represents the optimum between the plausibility of the solution, the budget earmarked for it, and the reduced risk in the event of an incident.

5 APPENDIX: RISK ANALYSIS GUIDES

5.1 Premises and infrastructure

The risk of them becoming definitively unavailable

Types of threat	Consequences	Possible countermeasures[1]

Total destruction (site or building)	▪ Site and / or services affected
	▪ Length of the interruption
	▪ Deteriorated service
	▪ Loss of data
	▪ Transfer of personnel
		▪ External backup copies
		▪ Sites and backup resources
		  ▪ Information systems
		  ▪ Users
		▪ Formalized recovery plans
		  ▪ Premises
		  ▪ Equipment
		  ▪ Business activities

Destruction of the room containing the information systems	▪ Site and / or services affected
	▪ Length of the interruption
	▪ Deterioration in service
	▪ Loss of data
	▪ Transfer of personnel
		▪ Keep all backup copies outside the room
		▪ Backup site
		▪ Backup equipment
		  ▪ Internal
		  ▪ External
		  ▪ Delivery
		  ▪ Maintenance
		▪ Backup cabling

Destruction of a nodal site	▪ Reduced operation of the local network
	▪ External links severed
		▪ Secured architecture
		▪ Possibility of reconfiguring via another technical site
		▪ Emergency kit
		  ▪ Cables
		  ▪ Network hardware

Destruction of a technical site	▪ temporary interruption of the network in the zones affected
	▪ Deterioration in service
	▪ Transfer of personnel
		▪ Secured architecture
		▪ Possibility of reconfiguring via another technical site
		▪ Emergency kit
		  ▪ Cables
		  ▪ Network hardware

[1] All the possible countermeasures can only be effective if they are formalized and tested regularly

Types of threat	Consequences	Countermeasures
Destruction of the media library	▪ Loss of archives ▪ Loss of backup copies ▪ Loss of application data	▪ Keeping a copy of sensitive data (legal backup copies, archives) off site ▪ Researching the possibilities of rebuilding the data (external recovery, paper trail) ▪ Copies on disk

Destruction of a user zone or an archiving zone (function of a fire separator)	▪ Loss of documents
	▪ Total loss of data (if backup copies are stored locally)
	▪ Transfer of personnel
	▪ Deterioration in service
		▪ Keeping a backup copy outside the zone
		▪ Backup of local equipment
		  ▪ Servers
		  ▪ PC park / printers
		  ▪ Specific equipment
		▪ Backup physical flow supports and files (paper, disk…)
		  ▪ External copy
		  ▪ Scanning
		  ▪ Possibility of rebuilding
		▪ Backup user sites

Destruction of the air conditioning system	▪ Disk failure and deterioration of data ▪ Servers stop operating ▪ Deterioration of the supports ▪ In certain cases, the building may become unusable	▪ Redundancy of air-conditioning equipment (iced water plant, cabinets…) ▪ Protection of technical sites (access, fire) ▪ Recovery plan and backup resources for the unavailable servers and applications

Destruction of electrical feed equipment (transformer, cabinet, ...)	▪ Disk failure and deterioration of data
	▪ Servers stop operating
	▪ Deterioration of the supports
	▪ In certain cases, the building may become unusable
		▪ Regularly tested electrical generator
		▪ Separation of incoming cables and electrical transformer stations
		▪ External backup resources
		  ▪ Information systems
		  ▪ Users
		▪ Rapid reaction contract
		▪ Respecting the user loads recommended by the manufacturers
		▪ UPS + secured shutdown of the machines

Types of threat	Consequences	Countermeasures
Destruction of the main UPS (or one dedicated to a particular room)	▪ Disk failure and deterioration of data ▪ Servers stop operating	▪ Network switchover (automatic if possible) ▪ Backup UPS with automatic switchover ▪ Securitization of the area where the UPS is located (access, fire...) ▪ External backup resources for the information systems ▪ Maintenance contract which makes provisions for replacement in an appropriate period of time

Table 2 : Premises and infrastructure (risk of the premises becoming definitively unavailable)

Risk of the premises becoming temporarily unavailable

Types of threat	Consequences	Countermeasures
Temporary inaccessibility with no destruction ▪ following a threat (bomb scare, pressure on the personnel…)	▪ Halt of activities at the site ▪ Inaccessibility of the driver consoles ▪ Risk of hardware deteriorating	▪ External backup resources for IT systems and users for temporary minimum service ▪ External backup copies ▪ Alert procedures and implementation of emergency measures
Temporary inaccessibility with no destruction ▪ following an environmental accident	▪ Halt of activities at the site ▪ Risk of equipment shutdown ▪ Risk of hardware deteriorating ▪ Risk of losing data	▪ External backup resources for IT systems and users for temporary minimum service ▪ Remote access and control ▪ External backup copies
Temporary inaccessibility with no destruction ▪ due to the premises failing to conform to regulations	▪ Halt of activities at the site	▪ External backup resources for users to guarantee temporary minimum service ▪ Remote access and control
Temporary inaccessibility with no destruction ▪ Following a security system breakdown	▪ Halt of activities at the site	▪ External backup resources for users to guarantee temporary minimum service ▪ Remote access and control
Blocked access due to a strike , without equipment shutdown	▪ Halt of activities at the site ▪ Inaccessibility of the driver consoles ▪ Risk of occupation	▪ External backup resources for users to guarantee temporary minimum service ▪ Offsite printing ▪ Remote access and control ▪ Physical protection of the building ▪ Strategy of anticipating a worsening situation
Occupation of the premises due to a strike without equipment shutdown (worsening of the previous risk)	▪ Halt of activities at the site ▪ Inaccessibility of the driver consoles ▪ Risk of equipment shutdown or acts of sabotage	▪ External backup resources for users to guarantee temporary minimum service ▪ Offsite printing ▪ Remote access and control ▪ Physical protection of critical equipment ▪ Alert procedures and implementation of emergency measures
Occupation of the premises due to a strike with equipment shutdown (worsening of the previous risk)	▪ Halt of activities at the site ▪ Shutdown of site equipment ▪ Risk of hardware deteriorating	▪ External backup resources for IT systems and users for temporary minimum service ▪ External backup copies

Table 3: Premises and infrastructure (risk of the premises becoming temporarily unavailable)

5.2 Computer and telecommunications equipment

Risks of equipment becoming definitively unavailable

Types of threat	Consequences	Countermeasures
Destruction (accident or sabotage)	▪ Loss of data ▪ Temporary or definitive interruption of service ▪ Deterioration of service ▪ Interruption of the flow	▪ Redundancy ▪ Degraded mode ▪ Regularly tested backup equipment ▪ Extension of the maintenance contract ▪ Custom and complete backup ▪ Physical protection
Breakage of irreplaceable material	▪ Loss of data ▪ Temporary or definitive interruption of service ▪ Deterioration of service ▪ Interruption of the flow	▪ Same as destruction + ▪ Surveillance ▪ Stock of spare parts ▪ Obtaining system sources and specific applications ▪ Ensuring the quality of the maintenance ▪ Mobility of the applications
Theft	▪ Loss of data ▪ Temporary or definitive interruption of service ▪ Deterioration of service ▪ Interruption of the flow ▪ Loss of confidentiality (data and know-how)	▪ Same as destruction + ▪ Encryption of sensitive data

Table 4: Computer and telecommunications equipment (risks of becoming definitively unavailable)

Risks of becoming temporarily unavailable

Types of threat	Consequences	Countermeasures
Breakdown or breakage of replaceable material…	▪ Loss of data ▪ Interruption of flow ▪ Temporary interruption of service ▪ Loss of confidentiality	▪ Secure repair procedures ▪ Results-based maintenance contract ▪ Maintenance stock ▪ Improved use of the equipment
Obsolescence	▪ Temporary or definitive interruption of service ▪ Deterioration of service ▪ Difficult or impossible to update	▪ Surveillance ▪ Mobility of the applications ▪ Stock of spare parts
Saturation	▪ Interruption of flow ▪ Temporary interruption of service	▪ Improved use of the equipment

Table 5: Computer and telecommunications equipment (risks of becoming temporarily unavailable)

5.3 Operating systems, applications, data and flow

Risk of becoming definitively unavailable

Types of threat	Consequences	Countermeasures
Loss of software	▪ Interruption of service ▪ Interruption of flow ▪ Loss of data	▪ High security software backup (integrity locking, periodic restore tests) ▪ Conservation of the original supports and the various updates ▪ Externalizing the backup of software
Loss of non-retrievable data (Accidental deletion, system error, virus, malicious intent, voluntary destruction, configuration error...)	▪ Interruption of service ▪ Interruption of flow ▪ Loss of data	▪ High security software backup ▪ Externalizing backup copies

Table 6: Operating systems, applications, data and flow (risks of becoming definitively unavailable)

Risks becoming temporarily unavailable

Types of threat	Consequences	Countermeasures
Temporary interruption of flow by logic attack (network saturation)	▪ Temporary interruption of business activities	▪ Use another means of transmission ▪ Network surveillance

Loss of retrievable data (Accidental deletion, system error, virus, malicious intent, voluntary destruction, configuration error...)	▪ Interruption of service
	▪ Interruption of flow
	▪ Loss of data
		▪ Preventive measures
		  ▪ quality of the operating environment
		  ▪ quality of the operating organization
		  ▪ anti-virus software
		  ▪ overall security organization
		▪ Data retrieval procedures (from original documents or other files in the possession of clients or partners)

Table 7: Operating systems, applications, data and flow (risks of becoming temporarily unavailable)

5.4 Services, supplies and outside contractors

Risks of becoming definitively unavailable

Types of threat	Consequences	Countermeasures
Sudden loss of a supplier or contractor	▪ Service / supply shutdown ▪ Interruption of supplies ▪ Interruption of flow ▪ Loss of data	▪ Policy of diversification vis-à-vis suppliers ▪ Mobility of outside services and external contractors ▪ Conforming to market standards ▪ Product or service substitution ▪ Operating in degraded mode ▪ Supplier monitoring and audit
Loss of a product or service	▪ Service shutdown ▪ Interruption of supplies (supplies, energy, raw materials…) ▪ Interruption of data flow ▪ Loss of data	▪ Requiring all suppliers to have a recovery plan ▪ Substitute products or services operating in fail soft mode ▪ A contractual clause requiring advance warning and / or a substitute product or service ▪ Strategic monitoring ▪ Availability of key service-related documents ▪ Backup stock
Forced shutdown of a product or service (regulation, embargo, conflict)	▪ Service shutdown ▪ Interruption of supplies (supplies, energy, raw materials…) ▪ Interruption of data flow	▪ Monitoring ▪ Anticipating a shutdown ▪ Stock ▪ Emergency communication

Table 8: Services, supplies and outside contractors (risks of becoming definitively unavailable)

Risks of becoming temporarily unavailable

Types of threat	Consequences	Countermeasures
A telecom service provided by an operator becomes unavailable	▪ Total or partial isolation of a site (voice, data…)	• Make sure that service quality obligations are included in the contract and that they comply with service requirements: ▪ Specific time frame to reestablish service with penalties for non-observance, ▪ guarantee of availability ▪ securing access resources (physical seperation of access infrastructure) ▪ Implementation of backup solutions (switchover to backup line, and activation of the backup site) ▪ Diversification of suppliers (automatic routing on another operator)
An operational service contracted out to an external provider (EDI, ISP, ASP…) becomes unavailable Delivery delay	▪ Total or partial interruption of business activities ▪ Deterioration of service	▪ Make sure that service quality obligations are included in the contract and that they comply with service requirements. ▪ ISO 9000 certification of the provider's services ▪ If necessary, verify the existence of a recovery plan and test reports. ▪ Diversification of resources
Prolonged electrical power outage	▪ Total or partial interruption of business activities ▪ Loss of data ▪ Malfunctions during rebooting	▪ Test the backup power generator regularly (operation and endurance) ▪ Separate the incoming cables and the electric transforming station ▪ External backup resources ▪ UPS with a system to shutdown the servers securely ▪ Contractual guarantees vis-à-vis the time frame for reestablishing service
Deficiencies in the electrical power supply (micro-outages and surges)	▪ Loss of data ▪ Deterioration of equipment ▪ Repeated interruptions in business activities	▪ Establishment of control interfaces between the incoming cables and the equipment: ▪ Dynamic interfaces (dynamic groups with flywheel) ▪ Static interfaces (dry insulation transformers, voltage regulators, network conditioners, UPS)

Table 9 : Services, supplies and outside contractors (risks of becoming temporarily unavailable)

5.5 Human resources

Risks of becoming definitively unavailable

Types of threat	Consequences	Countermeasures
Death / disappearance of strategic personnel	▪ Loss of know-how ▪ Temporary or definitive shutdown of activities ▪ System or application lockout (passwords, maintenance, operation…) ▪ Deadlocked decision-making	▪ Duplication of skills vis-à-vis strategic business activities ▪ Delegation of authority ▪ VIP insurance ▪ Documentation of strategic tasks ▪ Security guidelines for group business trips ▪ Emergency replacement Plan (recruitment, outsourcing…)
Resignation / departure of strategic personnel	▪ Loss of know-how ▪ Temporary or definitive shutdown of activities ▪ System or application lockout (passwords, maintenance, operation…) ▪ Deadlocked decision-making ▪ Deterioration in service or sabotage linked to the conditions of the departure	▪ Replacement plan with recovery period for the transfer of skills. ▪ Duplication of skills vis-à-vis strategic business activities ▪ Documentation of strategic tasks ▪ Increased monitoring of personnel who resign and restrictions on their rights ▪ Should there be a risk of malicious intent, immediate suspension of the individual's rights and security clearance (physical and logic)

Table 10 : Human resources (risks of becoming definitively unavailable)

Risks of becoming temporarily unavailable

Types of threat	Consequences	Countermeasures
Industrial unrest	▪ Temporary, partial/total shutdown of activities ▪ Risk of intentional blockage of the site and/or equipment (cf. fiche premises & infrastructure table)	▪ Adapted social policies for the IT department ▪ Externalizing critical functions ▪ Mobile backup personnel outside the company ▪ External and confidential backup sites and resources
Transportation problems	▪ Temporary shutdown of business activities at the site ▪ Risk of equipment shutdowns	▪ Organization of emergency transportation resources (shuttles, carpooling...) ▪ remote access and operation ▪ Off-site printing ▪ External backup user resources to ensure minimum service
Large-scale, accidental unavailability of personnel (epidemic, contamination, …)	▪ Temporary shutdown of the site's activities ▪ Risk of equipment shutdowns	▪ Preventive medicine ▪ Preventive maintenance of AC system (regular filter changes, monitoring of air quality) ▪ Mobile backup personnel outside the company

Table 11 : Human resources (risks of temporarily unavailable)

6 DIAGRAMS AND TABLES

7 GLOSSARY

BCP

The Business Contingency Plan is intended to guarantee the survival of the company by planning in advance to ensure the continuity of those business activities that are deemed to be strategic. It is not restricted to a Disaster Recovery Plan.

DRP

The Disaster Recovery Plan is a subcomponent of the BCP and it covers the IT resources. It guarantees the revival of critical systems in a minimum set period. It also guarantees the retrieval of data with a minimum of fixed losses.

Recovery plan

In this document, the recovery plan is a generic term for the DRP or the BCP.

Return time objective

The RTO is the time needed to get the information systems back on line from the point when business activities were first shut down.

Recovery plan objective

Depending on the defined needs, the recovery plan objective corresponds to the acceptable amount of data that may be lost between the shutdown and resumption of activities. For example, when starting up after an incident, the data may date from the evening, morning or minute before that incident.

Crisis management committee

The crisis management committee is comprised of the directors of each of the user departments affected by the recovery plan. It includes people from senior management, the general services department, the human resources department, the communication department, the IT department and the directors of the recovery plan. In the event of a major incident, the committee will meet and decide whether to activate the recovery plan or not.

Crisis management committee meeting room

The designated place where the crisis management committee meets if the need arises. It is located in an area close to the environment covered by the recovery plan though not adjacent to it. At the very least, it is equipped with a telephone, a fax and a strong box containing the procedures of the recovery plan.

Technical procedures

The technical procedures outline the actions to be taken by the IT department on a daily basis to keep the technical resources up to date. It also outlines the actions to be taken should the DRP be activated or in the event of tests. The procedures are written by the IT department.

Test plans

Firstly, test plans help to validate what has been set in place vis-à-vis the defined needs. Then, when conducted at regular intervals they help to guarantee the operational character of the DRP.

Load Balancing

Load balancing is a technical solution based on an applicative duplication that uses between 2 and ***n*** servers to balance resources. This technique helps to maintain the availability of the applications should one or several servers shut down. The integrity of data is preserved by the propagation of updates on all the servers. Even so, in the event of a sudden shutdown of an operational server, the session underway is lost.

In the framework of a DRP, the possibility of spreading the machines over two geographically different sites should be studied.

Server clusters

Server clusters are a technical backup solution that relies on a cluster of 2 to ***n*** machines all sharing the resources necessary to maintain the availability of services. In the event of a sudden shutdown of a given resource, only the transaction underway will risk being lost.

Mirroring

A backup solution relying on a technique of duplicating saved data in real time, either in synchronous or asynchronous mode. The duplication of data from a server may be partial or total, and remote where possible, depending on the level of security needed and the technical constraints of the IT environment.