Disaster Recovery Planning

NOW *or* NEVER

Disaster Recovery Team

Aura Advanced Technologies

Aura Advanced Technologies Inc
1301-1121 Sixth Avenue SW Calgary, Alberta T2P 5J4
Phone: 403-269-6123 Fax: 403-269-6169
Website: **www.auraadvanced.com**

This paper outlines Aura's approach to disaster recovery planning and discusses steps our customers need to take to implement a ***successful disaster recovery plan****.*

From a disaster recovery (DR) standpoint, September 11 brought to light some hard lessons. Recent hurricanes –Rita and Katrina- have added to the woes of many businesses that were caught off-guard.

While you can't stop the physical forces of nature, you can plan ahead to mitigate their devastation. Thinking about disasters before they hit can help save a company's resources, protect the safety of its employees, and minimize business interruption.

Historical analysis suggests that:

- Of companies without a Business Continuity Plan (BCP) that experience a disaster, 30% never reopen and an additional 50% will fail within 2 years.
- Service disruptions have a direct impact on revenues, shareholder value, market share and overall customer relationships.

The objective of a disaster recovery (DR) plan is to get your company operational in a logical, efficient order after being affected by a disaster. A disaster could be external (such as a hurricane) or internal (fire). If your success is critical to the intellectual property of a few key people, a disaster may be the loss of those individuals.

For those organizations that need to dust off their current disaster recovery plan and those that have yet to craft one, the following are key issues and questions disaster preparedness plans must take into account.

- Data replication is at the heart of any disaster recovery plan. But will your current data replication strategy meet your enterprise's needs in the event of an actual disaster?
- Has the enterprise determined which servers are mission-critical, which are important but not do-or-die, and which are expendable? Has technology been implemented that can prioritize and redirect assets according to that hierarchy?
- If the data center is located in an area where the most likely problem is weather-related flooding, is vital gear on an upper floor of the building? If earthquakes are a threat, is the data center configured in such a way that heavy objects won't hit sensitive equipment if they fall?
- Is there a list of the names of *existing* and *alternate* vendors and parts suppliers? Are key contacts at these companies, complete with their work and home numbers, identified? Is that list updated as employees change jobs and leave?
- Are employees asked or required to say what they know as they leave the company? Is there a fool-proof knowledge management system that captures this knowledge before it is lost?
- Is there any employee backup plan?
- Does everyone understand what to do in an emergency?

If these questions bewilder you, your business needs a disaster recovery plan. You cannot afford to be caught off-guard by a natural or human-made disaster. Therefore, it is imperative that you act now before it is too late.

Disaster Recovery Planning should be triggered by management awareness. Prior to appointing a *Disaster Recovery Team*, you should ensure that senior management is on-board. We suggest that you pursue the following nine-step approach towards emergency preparedness. These steps should be seen as guidelines necessary for planning your disaster recovery efforts; however, your business may have specific needs for which you should always consult third-party auditors.

1. Garner Management Support

Management buy-in is the first and most important step in creating a successful disaster recovery plan. To obtain the necessary resources and time required from each area of your organization, senior management has to understand and support the business impacts and risks.

Emergency preparedness takes a corporate commitment,
and it isn't cheap.

Begin with identifying the top five disasters and analyze their impact on your business. The possibility of each scenario depends on factors such as geographical location and political stability. Examples of natural and human-made disasters are: hurricane, earthquake, fire, theft, power outage etc. Your analysis should cover effects on:

- Communications with suppliers and customers
- Impact on operations
- Disruption on key business processes

Assess the impact of a disaster on your business from both a financial and physical (infrastructure) perspective.

Once management understands the financial, physical, and business costs associated with a disaster, it is then able to build a strategy and ensure that this strategy is implemented across the organization.

2. Establish *Disaster Response Management* Team

After getting senior management on-board, establish a *Disaster Response Management team* responsible for management of all aspects of the disaster response which include evacuation, recovery, and relocation. All other teams are coordinated by this team. It also has the responsibility of budget issues. Some of the roles and responsibilities of the Team-Champion (who is also the team-captain) are listed as follows:

PRE-DISASTER

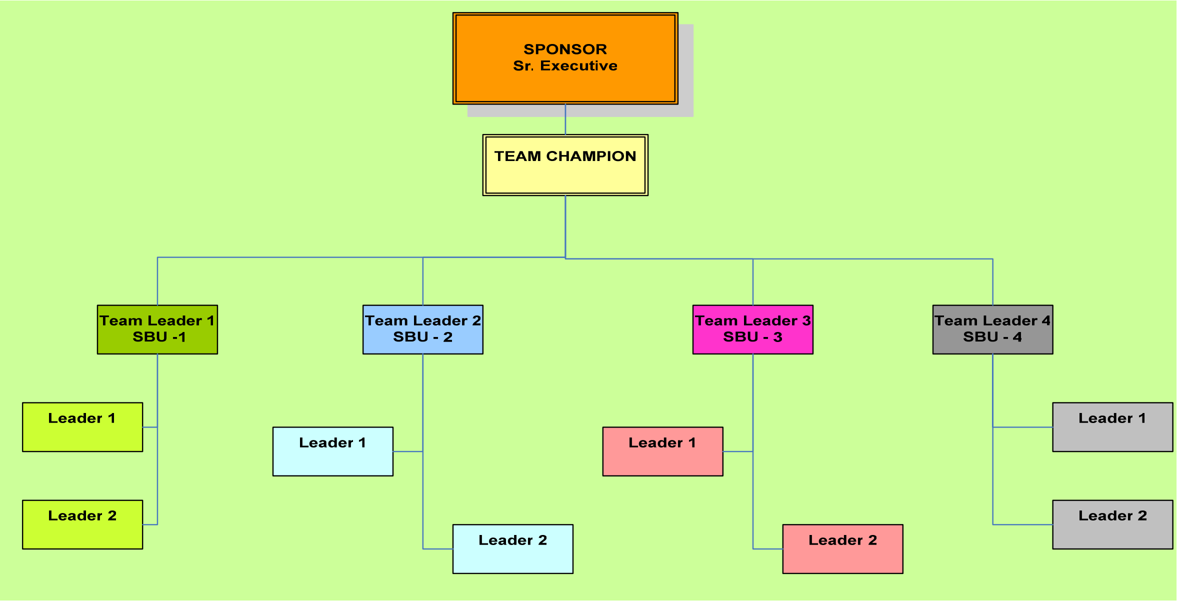
Manages the response planning process;
Supervises the maintenance of the plan;
Supervises testing of the plan;
Supervises the training of the teams

POST-DISASTER

Makes the disaster declaration;
Invokes the Disaster Recovery Plan;
Manages the response process;
Assures coordination of all response teams

The following structure for Disaster Response Team outlines the execution strengths of team members. It should be noted that senior executives are “sponsors” of the initiative and should only look after strategic and financial needs. Ideally, senior executives play a “support” role for Team Champion and his/her team. Executive powers should reside with the Team Champion (or team captain, who is also the executive-head of the initiative) and his group of Team Leaders.

Team Leaders should be key people from each business unit (SBU- Strategic Business Unit) or operational/functional area (HR, Marketing, Finance, etc). They are responsible for all disaster recovery activities, planning, and providing regular monthly reports to senior management including Team Champion and Sponsors – Senior Executives.



Copyright© 2005 Aura Advanced Technologies Inc

While appointing Leaders, consider a broad cross-section of people from throughout your organization. These will likely include people with technical skills as well as mid-level managers. It is definitely prudent to have at least one Leader from the IT/Network Design team on-board.

In several cases, we have found that organizations are better-off if they have created a back-up for Team Champion. Role of a Vice Team Champion (or Vice-Captain) is to assist the Team Champion. Vice Team Champion undertakes responsibilities of Team Champion (Captain) during his/her absence; and assumes the role of any Team Leader as required.

3. Perform Risk Assessment and Audits

It is important to thoroughly understand the business and its processes, technology, networks, systems, and services. You should carefully assess how your company functions, both internally and externally, so as to determine which staff, materials, procedures and equipment are absolutely necessary to keep the business operating.

Review your *Business Process Flow chart*[1], if one exists, and identify operations critical to survival and recovery. You should also assess your service-level agreements, customer and supplier-list.

Not having an external independent third-party review your security posture is like not having an independent auditing firm review your financials **PricewaterhouseCoopers (*PwC)***

Research indicates that external independent third-party auditors help you identify gaps in your process more effectively and accurately. Aura continues to advise its customers to hire external auditors who can offer outsider's perspective during the assessment phase of the disaster recovery plan.

4. Analyze and Prioritize

After the initial assessment of business processes and systems, you should analyze both quantitative and qualitative risks.

- **Quantitative Risk Analysis**: This approach employs two basic fundamentals of forecasting potential loss in the event of a disaster. These fundamentals are: the *probability* of an event occurring and the *likely loss* should it occur. You can calculate *Estimated Annual Cost* by multiplying the potential loss by the probability of an event occurring.
- **Qualitative Risk Analysis**: Most of the times, this risk approach involves analysis of two interrelated risk factors - *threats* and *vulnerabilities*[2].

When you have analyzed both quantitative and qualitative risks posed to your business processes from each disaster scenario, assign a priority level to each business process. Consequently, you should be able to rank your business applications as per the following suggested format:

- **Mission Critical**: Network, application or business process that requires significant effort to restore, or the restoration process is disruptive to the business or other systems.
- **Important**: Network or application that requires a moderate effort to restore.
- **Minor**: Network or application that can be easily restored.

5. Develop Recovery Strategy

Just as the analysis of the business processes determine the priorities of the network, applications, and systems, the same analysis should be applied to your network design.

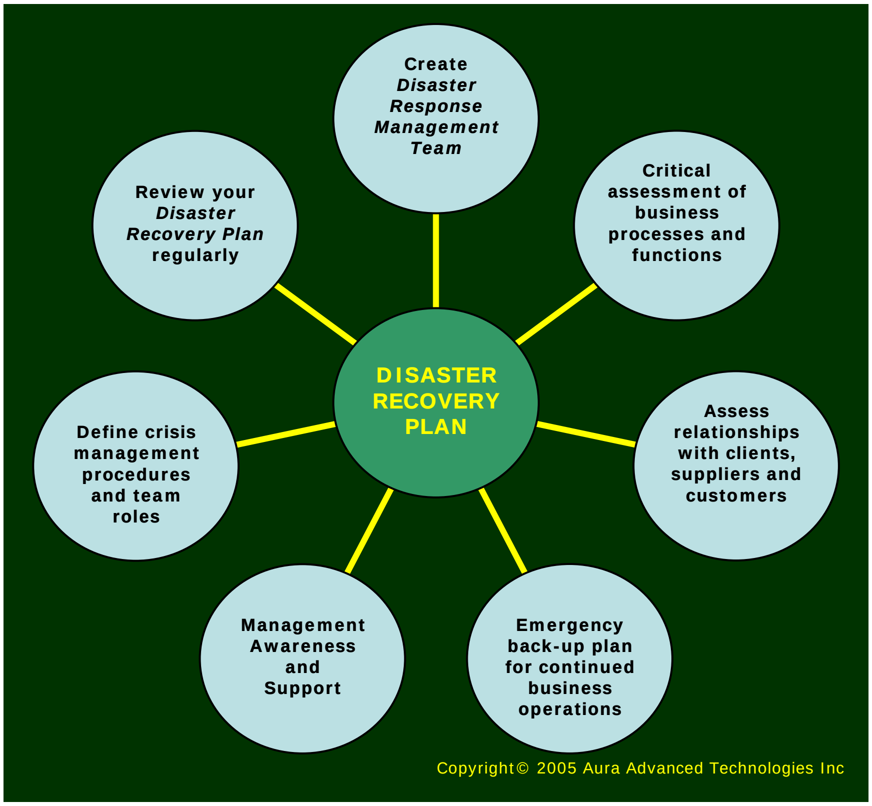
Develop a recovery strategy to cover the practicalities of dealing with a disaster. Your recovery strategy should include the expected down time of services, action plans, and escalation procedures. Your plan should also determine thresholds, such as the minimum level at which can the business operate, the systems that must have full functionality (all staff must have access), and the systems that can be minimized.

[1] For information on Business Process Flow, visit our **Business Process Improvement** practice. Learn more about our practice at www.auraadvanced.com or Contact Us at TollFree#: 1-877-264-2872

[2] For explanation; Refer: **Definitions and Explanations**

Recovery Time Objectives (RTO- the time to recover the system after a disaster) and Recovery Point Objectives (RPO – time passed since last backup prior to a disaster)[3] need to be defined whether you are recovering at your own alternate Data Center or your are recovering at a cold or hot site operated by a third party. RPOs and RTOs are usually tiered depending upon your company's unique requirements. While determining RPO and RTO for your business process, you should consider:

- Objective of the business process
- Resources needed for this business process to continue to operate in a disaster scenario
- Vital information flow through this business process[4]; degree of dependence of other business processes on the activities of this process
- Direct and indirect financial implications caused by damage to this business process in the event of a disaster


DISASTER RECOVERY PLAN
Create *Disaster Response Management Team*
Critical assessment of business processes and functions
Assess relationships with clients, suppliers and customers
Emergency back-up plan for continued business operations
Management Awareness and Support
Define crisis management procedures and team roles
Review your *Disaster Recovery Plan* regularly
Copyright© 2005 Aura Advanced Technologies Inc

6. Documentation of Recovery Plan

Remember, a disaster elsewhere can be a disaster for you if your critical vendors become unavailable. Develop a list of suppliers in other parts of the country for backup. It is important to keep your inventory up-to-date and have a complete list of all locations, devices, vendors, used services, and contact names. Your disaster recovery documentation should include complete inventory, including a prioritization of resources.

[3] Refer: Glossary of Terms
[4] For more information on information-flows: refer our Business Process Improvement practice

It is a good practice to always document knowledge-resources within your organization. It may include preparing contact-list of employees, capturing experience/knowledge[5] of employees or even keeping list of emergency-help numbers handy. Document your training and budgeting needs for the recovery plan. Moreover, list all important findings from the assessment and auditing phase; document procedures the organization will take to implement the plan.

Once you've created a draft of the plan, you should create a verification process to prove the disaster recover strategy and, disaster recovery and implementation plans. We recommend documenting the verification process and procedures, and designing a proof-of-concept-process.

7. Review of Network Resiliency and Backup Services

Review network resiliency and backup services to meet the criteria for your disaster recovery plan. You should test your network for its ability to recover from any network failure or issue whether it is related to a disaster, hardware, design, or network services.

Replication Strategies: Your Data-replication strategy should reflect your business needs. You may either go for **synchronous replication** or **asynchronous replication** depending upon level of data-risks you perceive. Synchronous replication ensures both primary and remote site are 100% synchronized. Asynchronous replication, on the other hand, enables customer to choose an acceptable lag time for replicating and restoring data. This solution provides a greater amount of protection by extending the distance between the primary and secondary locations of the data.

Third-party providers now have advanced recovery services that can meet high availability requirements for RTO and RPO.

8. Protect your value-chain

Collaboration is the key to success of your Disaster Recovery Plan. Your plan should involve your suppliers, partners and even customers (in few cases). Share your DR strategies and encourage them to set in motion their own continuity planning. To ensure that your organization's value-chain remains safe and robust, it is critical to get all stakeholders on-board with your disaster recovery efforts. Your plan should be integrated with recovery plans of your suppliers and customers organizations.

9. Review your Disaster Recovery Plan

Just as your business changes over time, so do your preparedness needs. When you hire new employees, change suppliers or when there are changes in your business operations, you should update your plans and inform your people.

At the same time, it is important that periodic reports are issued by the Disaster Recovery Management team to Senior Executives in the organization. Recovery processes and strategies, training a budget needs should be reviewed periodically.

[5] Knowledge Objects are used to capture the knowledge of employees in most company. Available *Knowledge Management tools* are often used to enable this.

Are You Really Prepared For Disasters?

Even though you may think that you have a disaster recovery plan in place that provides for recovery of critical business application, you could still be wrong. It is important for you to know how comprehensive your emergency plan is.

- What processes and criteria were used to determine the recovery time objectives (RTO) and recovery point objectives (RPO)[6] for those systems?
- Is your plan focused on the recovery of the critical business processes or only focused on the recovery of the systems?
- Are there any Zero Data Loss (ZDL) objectives addressed in your plan?
- Do you have an organized team structure for your Disaster Response Management Team? Do you even know if you have a *Disaster Recovery Manager*?
- Do you have a comprehensive list of backup options in the event of disaster?

Project Management for Disaster Recovery Planning

Aura is best positioned to help you in this scenario. Through years of experience in this industry, Aura has developed BCP and DR solutions for your business. Our specialized knowledge in Business Continuity Planning and Disaster Recovery combined with our expertise in delivering end-to-end solutions will help you deal with potential disasters.

Gartner estimates that less than 25% of large enterprises have comprehensive BCP programs, and just 50% have comprehensive disaster recovery programs.

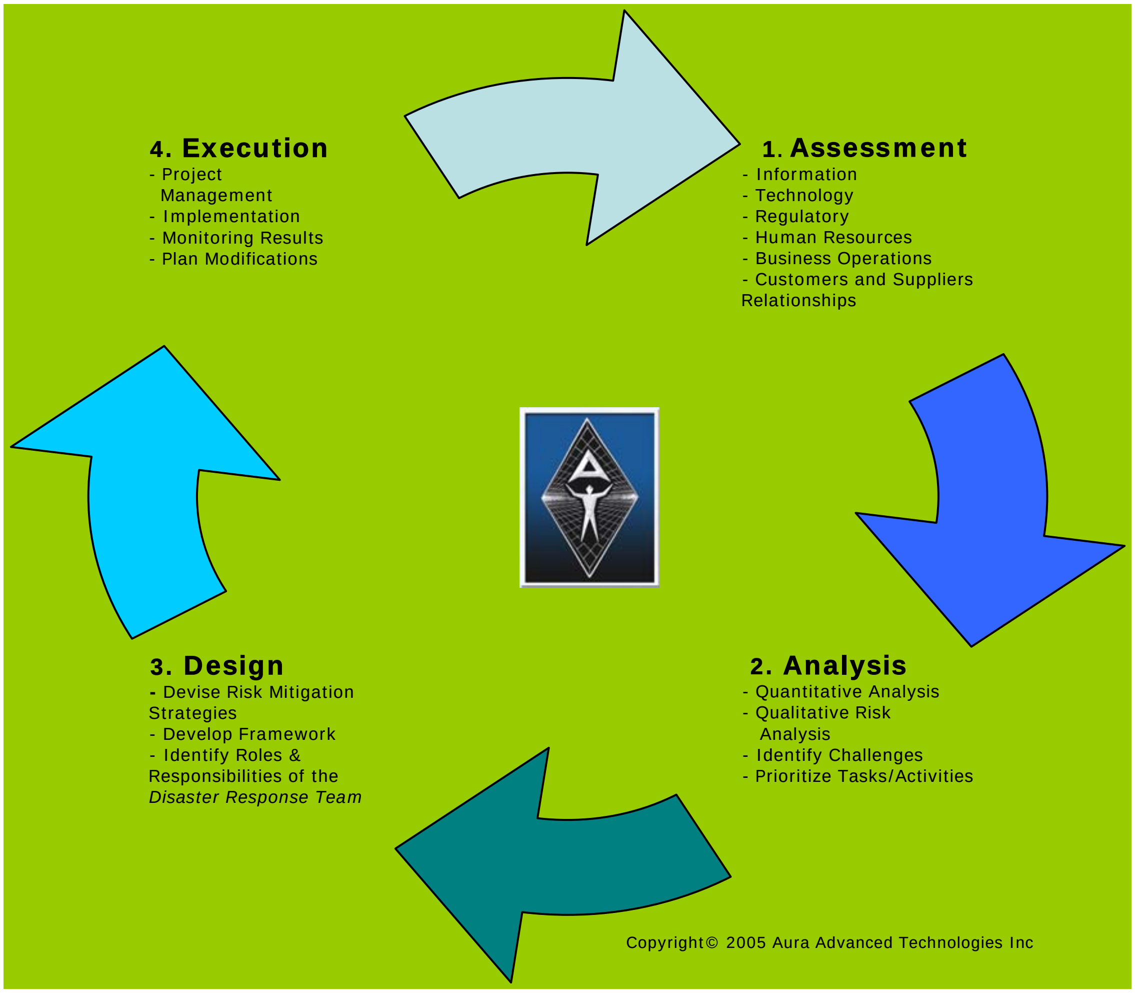
- We have highly specialized knowledge in – PIPEDA, ISO 17799 and BS 7799-2, Succession Planning, Intrusion Detection, Security,Network Design and Implementation.
- Our team of experts will develop a plan specific to your business environment, risk and corporate strategy
- Working with well-accepted methodologies, we will minimize the impact to your organization when an incident occurs.

At Aura, we believe that an effective disaster recovery plan covers both the hardware and software required to run critical business applications and the associated processes to transition smoothly in the event of a disaster. To prepare your business for any emergency, you need to first assess your mission-critical business processes and associated applications before creating the full disaster recovery plan.

Aura's project management approach for disaster recovery planning is outlined in the figure.

- **Assessment**
- **Analysis**
- **Design**
- **Execution**

[6] Refer: **Glossary of Terms**



1. Assessment
- Information
- Technology
- Regulatory
- Human Resources
- Business Operations
- Customers and Suppliers Relationships

2. Analysis
- Quantitative Analysis
- Qualitative Risk Analysis
- Identify Challenges
- Prioritize Tasks/Activities

3. Design
- Devise Risk Mitigation Strategies
- Develop Framework
- Identify Roles & Responsibilities of the *Disaster Response Team*

4. Execution
- Project Management
- Implementation
- Monitoring Results
- Plan Modifications

Our approach is unique: while our competition leaves their customers before the execution phase, we help our clients implement comprehensive disaster recovery solutions. Aura's infrastructure capabilities (intelligent internet –datacenter, phone systems, email and network support) combined with BCP experience allow us to give our customers complete disaster recovery solutions.

Think of Aura as a seamless extension of your IT organization and a strategic and tactical partner in your success.

GLOSSARY OF TERMS

This section is intended to help assist the reader in correlating acronym used within this white paper. Single line definitions are provided not as a means of fully explaining the terms, but as an overall supplement to their fuller explanations found within the text of this document.

BCP - Business Continuity Plan: A comprehensive business plan that details actions to take in the event of a disaster.

BIA – Business Impact Analysis: A follow-up to the RA in a BCP that identifies the impact a risk might have to a business.

DR – Disaster Recovery: Recovery processes designed to recover business objectives.

RA- Risk Analysis: An initial phase of a BCP that identifies risks a business (process) is susceptible to.

RPO – Recovery Point Objective: The amount of data a business can afford to lose in the event of a failure. It is also the total time passed since last backup prior to a disaster.

RTO – Recovery Time Objective: The amount of time required to return to operation following a failure/disaster.

ZDL – Zero Data Loss: An objective of no data loss during a failure.

DEFINITIONS AND EXPLANATIONS

This section is intended to help the reader understand important concepts discussed in this white paper.

Threats: These are things that can go wrong or that can 'attack' the system. Examples might include fire or fraud. Threats are ever present for every system.

Vulnerabilities: These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire, vulnerability would be the presence of inflammable materials (e.g. paper).

Probability: A probability provides a quantitative description of the likely occurrence of a particular event. Probability is conventionally expressed on a scale of zero to one. A rare event has a probability close to zero. A very common event has a probability close to one.