



From the SAS 70 Type II Audit: DISASTER RECOVERY PROCESS

HR MANAGEMENT
PAYROLL SERVICES
BENEFIT ADMINISTRATION

AUTOMATE.	THE INTEGRATION OF BUSINESS AND TECHNOLOGY
ORGANIZE.	
STREAMLINE.	
CUSTOMIZE.	

In today's global economy, service organizations must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers. Mangrove annually receives a Statement on Auditing Standards (SAS) Number 70 Type II, a recognized auditing standard of objectives and activities for information technology and related processes. The audit is a detailed description of controls and an independent assessment of whether the controls were placed in operation, suitably designed, and operating effectively.

Disaster Recovery and Business Continuity Planning

Mangrove maintains a disaster recovery and business continuity program in the event of failure of its primary operating environment. This program deals with rebuilding its operational and technical infrastructure after the occurrence of a disaster and keep critical systems running during a period of displacement or interruptions to normal operations.

Prevention

Preventative measures ensure that the data center facilities and their key systems are properly maintained and monitored. These key systems included facility security systems, network security systems, data backup systems, network infrastructure, and data center infrastructure.

Preparation

To prepare for possible Disaster Recovery, the data centers (in Tampa, Florida and Henderson, Nevada) and their systems (facility, data, network, and phone) have undergone preparations. Redundancy is an important tool used in such preparations. Documentation is kept for such things as phone system circuit IDs and key vendor contacts. Contact lists are kept for all key members of the Response Team, who are cross-trained to better ensure redundancy.

Testing

Test procedures are routinely conducted on facility and network security systems, data backup systems, network and data center infrastructure, and network resiliency, as well as on Response Team members' knowledge of the disaster recovery plan.

Implementation

Following a disaster, the Disaster Recovery plan will be initiated. Steps are implemented according to plan, and team members manage, monitor, and provide regular status reports. Contact is made with Clients for a summary report, and arrangements are made with Vendors for continuity of service and, if necessary, replacement of hardware.

