IMMACULATE HEALTHCARE SERVICES LIMITED

BUSINESS CONTINUITY AND DISASTER RECOVERY IMPACT ASSESSMENT

1. Objectives

The objective of having a Business Continuity and Disaster Recovery Plan and associated controls is to ensure that the organization can still accomplish its mission and it would not lose the capability to process, retrieve and protect information maintained in the event of an interruption or disaster leading to temporary or permanent loss of computer facilities.

2. Risks

The absence of a well-defined and tested Business Continuity and Disaster Recovery Plan may pose the following major threats to the very existence of the organization in the event of a disaster:

- The organization's ability to accomplish its mission after re-starting its operations.
- To retrieve and protect the information maintained.
- To keep intact all the organizational activities after the disaster.
- To start its operations on full scale at the earliest to minimize the business loss in terms of money, goodwill, human resources and capital assets.

3. Steps of Disaster Recovery Plan formulation

1. Develop the contingency planning policy statement. A formal policy provides the authority and guidance necessary to develop an effective contingency plan.

2. Conduct the business impact analysis (BIA). The business impact analysis helps to identify and prioritize critical IT systems and components.

3. Identify preventive controls. These are measures that reduce the effects of system disruptions and can increase system availability and reduce contingency life cycle costs.

4. Develop recovery strategies. Thorough recovery strategies ensure that the system can be recovered quickly and effectively following a disruption.

5. Develop an IT contingency plan. The contingency plan should contain detailed guidance and procedures for restoring a damaged system.

6. Plan testing, training and exercising. Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness.

7. Plan maintenance. The plan should be a living document that is updated regularly to remain current with system enhancements.

Following the mentioned steps we can expand those activities into the following structured sequence of activities.

1. The plan development team should meet with the internal technology team, application team, and network administrator(s) and establish the scope of the activity, e.g., internal elements, external assets, third-party resources etc. IT department senior management should be properly informed.

2. Gather all relevant network infrastructure documents, e.g., network diagrams, equipment configurations, databases.

3. Obtain copies of existing IT and network DR plans if they exist.

4. Identify what management perceives as the most serious threats to the IT infrastructure, e.g., fire, human error, loss of power, system failure.

5. Identify what management perceives as the most serious vulnerabilities to the infrastructure, e.g., lack of backup power, out-of-date copies of databases.

6. Review previous history of outages and disruptions, and how the firm handled them.

7. Identify what management perceives as the most critical IT assets, e.g., call center, server farms, Internet access.

8. Determine the maximum outage time management can accept if the identified IT assets are unavailable.

9. Identify the operational procedures currently used to respond to critical outages.

10. Determine when these procedures were last tested to validate their appropriateness.

11. Identify emergency response team(s) for all critical IT infrastructure disruptions; determine their level of training with critical systems, especially in emergencies.

12. Compile results from all assessments into a gap analysis report that identifies what is currently done versus what ought to be done, with recommendations as to how to achieve the required level of preparedness, and estimated investment required.

13. Have management review the report and agree on recommended actions.

14. Prepare IT disaster recovery plan(s) to address critical IT systems and networks.

15. Conduct tests of plans and system recovery assets to validate their operation.

16. Update DR plan documentation to reflect changes.

17. Schedule next review/audit of IT disaster recovery capabilities.

Important IT disaster recovery planning considerations

- Senior management support. ensure to obtain senior management support so that your plan goals can be achieved.
- Take the IT DR planning process seriously. Although the IT DR plan can take a great deal of time for data gathering and analysis, it doesn't have to be dozens of pages long. Plans simply need the right information, and that information should be current and accurate.
- Keep it simple. Gathering and organizing the right information is critical.
- Review results with business units. Once the IT disaster recovery plan is complete, review the findings with business units leaders to make sure your assumptions are correct.

5. Audit Procedure.

Our back-up copies of systems software, financial applications and underlying data files are taken regularly. Back-ups are cycled through a number of generations by, for example, using daily, weekly, monthly and quarterly tapes. Back- ups are stored, together with a copy of the disaster recovery plan and systems documentation, in an off-site fire-safe.

The IT auditor while assessing the adequacy of business continuity and disaster recovery plan should consider:

- Evaluating the business continuity and disaster recovery plans to determine their adequacy by reviewing the plans and comparing them to organizational standards and/or government regulations.

- Verifying that the business continuity and disaster recovery plans are effective to ensure that information processing capabilities can be resumed promptly after an

unanticipated interruption by reviewing the results from previous tests performed, if any, by the IT organization and the end users.

- Evaluating off site storage to ensure its adequacy by inspecting the facility and reviewing its contents and security and environmental controls. It may be ascertained whether backups taken earlier have ever been tested for data recovery by the auditee organization.

- Evaluating the ability of IT and user personnel to respond effectively in emergency situations by reviewing emergency procedures, employee training and results of their drill.