

### Solution

A complete IT Security audit involving Hardware, Operating Systems, Network, Disaster Recovery Management, Computer controls and Human Relations was done. It includes:

- Business impact assessment.
- Completed internal control questionnaires to identify stated procedures.
- Evaluated stated procedures.
- Performed vulnerability assessment of the operating systems, network hardware and database by scanning the system with the use of tools
- Performed Benchmarking analysis with the use of tools.
- Performed compliance testing of the controls determined to be effective.
- Evaluated controls and results of tests.

The outcome of the audit is as follows:

- Baseline security policy has been recommended.
- General Security Controls have been evaluated and recommendations provided.
- Disaster Recovery Plan and Business Continuity Plan formulated.

## Information Systems Audit

A leading manufacturing company based in south India implemented an in-house data center for hosting their servers. There are about 25 servers comprising ERP servers, E-Business Servers, Storage Systems, etc., It is a BaaN ERP environment.

### Client

To determine whether adequate security controls in respect of Information Systems are in place and working effectively

### Requirement

### Benefits

- Protected company information from data tampering, fraud, inappropriate access to and disclosure of sensitive information, and disruptions in critical operations.
- Proper accountability and audit trail is established
- Adequacy of information protection was gauged against usual standards and practices and specific measures proposed by the audit team helped to make the company's investment in information security more efficient and effective

