Success Story

Information Technology

Systems and Security Audit

Storyline…

The client is a leading provider of building materials and décor solutions in Dubai. The organisation desired to review its internal processes, risks, and vulnerabilities.

MaGC performed the Systems and Security Audit for the Client.

Once upon a time…

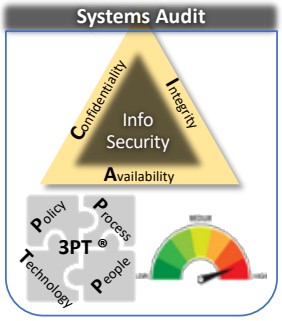
As a part of the Client's approach to review internal processes, risks and vulnerabilities, it decided to commission a Systems and Security Audit. The Management needed an audit of critical information flows & processes that affected operational or strategic decision making in respect of IT Governance & Compliance, IT General Controls, and IT Operations.

Moving on…

MaGC's audit team visited the Client and undertook a preliminary study to understand its business processes, information flows, reporting/review mechanisms and control system. Following this, the team adopted the following methods to examine the client's Information System:

- Study of documentation including – Organisation structure, existing policies, procedure manuals, schedule of authority, and previous Audit reports;
- Walkthroughs and examination of workflows with Users;
- Survey of 266 users across the organisation on aspects relating to IT experience, usage, issues, etc.;
- Key Management Personnel (KMP) Survey - Survey of 9 KMP regarding information availability and policy for key decision making;
- Use of vulnerability assessment and penetration testing (VAPT) tools for a comprehensive review of the information systems to determine the current security posture.

Observations on the IS Governance Framework were scored on the dimensions of Strategy, Policies, Organisation, Risk Management, Program management, Security metrics, Reporting & oversight, Asset management, and Compliance.



Observations made in respect of the systems audit were classified as per the CIA triad of IS: Confidentiality, Integrity, and Availability. Based on criticality of each observation, the risk was rated as High, Medium, or Low. The recommendations arising out of the IS audit were classified according to MaGC's 3PT© framework: policy, process, people, and technology.

The Penetration Tests focused on testing the network security and included External Penetration, Internal Penetration, Log Reviews, Network Sniffing and Port Scan. Test results and corrective actions to fix the high and medium risk gaps were provided in the report.

Finally…

The report was well received and appreciated by the Management. it immediately initiated action to address the lapses identified in the Information System. One of such initiatives was the preparation of various IT/IS policies. The recommendations provided by MaGC were most helpful in strengthening the Client's Information System.