SOX COMPLIANCE

The Sarbanes-Oxley Act (SOX) was created to improve accounting and disclosure and to increase transparency in corporate governance and financial reporting.

SOX COMPLIANCE CHECKLIST

Safeguards to Prevent Data Tampering

- Tracks user login access to all computers containing sensitive data and detects break-in attempts to computers, databases, fixed and removable storage, and websites.

Safeguards to Establish Timelines

- A system that timestamps all data received in real-time to be stored at a remote location as soon as it's received, preventing any data altering or loss.

Verifiable Controls to Track Data Access

- Implement a system that receives data messages from an unlimited number of sources. Collection of the data should be supported from file queues, FTP transfers and databases, separate of the actual framework.

Ensure Safeguards are Working

- A system to issue daily reports to e-mail addresses and via RSS to verify the system is up and running from any location.

Report Safeguard Effectiveness

- A system to generate multiple types of reports, including a report on all messages, critical messages, alerts and uses a ticketing system that archives what security problems and activities have occurred.

Detect Security Breaches

- A system to perform systemic analysis of messages in real-time and use correlation threads, counters, alerts, and triggers to refine and reduce incoming messages into high-level alerts.

Disclosure to Auditors

- A system that provides complete access for compliance auditors to inspect safeguards, security breaches and failures of security safeguard requirements.