Computer Task Group, Inc.
Sarbanes-Oxley Act
Automated Continuous Monitoring

Although many organizations are confident they will meet the Sarbanes-Oxley ("SOX") Section 404 compliance deadline, that confidence diminishes exponentially when they're asked whether they consider themselves 'COSO-compliant' in relation to all aspects of the organization's "compliance iceberg." Most would acknowledge an even lesser degree of confidence that—given the ever-changing nature of the corporate (and regulatory) environment—the work carried out for the first 404 event will equally satisfy future 404 requirements or 302 certifications. That fact poses a second fundamental question: one that all corporate executives should be asking themselves today. "Since 404 compliance is merely the tip of the compliance iceberg, how can I improve my confidence level as regards fully satisfying the need for overall compliance with the spirit (or complete COSO compliance) of the Sarbanes-Oxley Act?"

The Sarbanes-Oxley (SOX) service line, along with the Information Security Solutions Practice of CTG, is working with several software vendors to develop an automated software tool to incorporate into its ISO-methodology to address continuous monitoring. At this time, CTG and the vendors are working on a proof-in-concept by integrating this software solution at CTG's world headquarters in Buffalo, NY, where the methodology was already successfully used in CTG's first-ever 404 assertion. The objective of the software tool is to provide companies with a means to effectively and efficiently report on key process and control activities associated with SOX compliance. For key processes associated with financials, the software will:

- Create a complete body of evidence for all phases of assessment, documentation, remediation and attestation with:
    - context searches
    - pre-built reports
    - ad hoc analyses
    - audit walk-through paths
- "Automate" (through work-flow and e-mail protocols) financial controls to strengthen the effectiveness of financial operations
- Overcome organizational and geographical barriers to enforce compliance policies
- Provide scalability as business conditions change and the financial control environment broadens and matures
- Positively impact related monitoring costs, easily producing an "ROI" for the initial investment
- Reduce time-to-compliance with quick implementations and minimal training requirements
- Incorporate changes in the regulatory environment, such as new PCAOB interpretations, and standards pronouncements

For key automated controls associated with the IT infrastructure that supports these key processes, the software will:

- Provide the ability to proactively assess, audit, and secure multi-platform IT environments from internal and external attacks
- Provide scalable patch assessment, packaging and deployment of software patches
- Provide closed-loop identification and resolution to find and eliminate security exposures
- Reduce host- and network-based security breaches using simplified configuration management to manage risks against downtime and revenue loss
- Automate tasks enterprise-wide, enabling organization to be proactive in even the most resource-constrained environments
- Provide auditing capabilities with ready-to-run reports using customization options and audit creation in each environment to improve internal and external results

The software tool will also provide for the deployment of customizable dashboards for continuous tracking and monitoring of key processes and controls, as defined by the users. Dashboards can be created for executive management, internal audit, IT and even external auditors.

The effort logged by many organizations to prepare solely for Section 404 compliance has been estimated to exceed 5,000 hours of internal work, with expense estimates ranging from $500,000 to several million. These figures underline the vital importance of ensuring that a methodical approach is taken to determine the depth of compliance necessary for the organization and to realistically assess both the organization's current control maturity and the desired target level once the process is complete, and to monitor this control maturity on an ongoing basis, with archival abilities to provide artifacts as needed for independent verification. This "continuous monitoring program" under development by CTG and its alliance partners will readily achieve those goals in a cost-effective manner.