

Stocking Stuffers™ for SOX

Clever Sarbanes-Oxley compliance ideas for iSeries (or i5 or i)



☑ **Stitch-in-Time® Observation of iSeries Data Integrity**

Stitch-in-Time software provides a tool to observe and analyze details about data changes in critical databases, without any changes to your programs or files. Observation can be defined by file at the field-by-field level.

The recorded details include the pre-change and post-change contents of fields, information that identifies the user executing the change, the precise date and time the change was performed, and the program he/she used.

☑ **Needle in a Haystack™ Rare Event Detector for Crucial iSeries Databases**

The software watches for database changes that appear to be anomalies or rare events. The product teaches itself what is “normal/anticipated” by analyzing data accumulated by Stitch-in-Time during a statistical analysis period.

When a pre-post field change falls outside of Needle-in-a-Haystacks’ self-taught statistical boundaries, the product immediately authors an e-mail alert addressed to the pre-designated “guardian” of whatever database has experienced the abnormal field change.

☑ **TD/OMS (Tight as a Drum®) Software Change & Configuration**

This comprehensive suite of Object Management Software has matured into a robust Software Lifecycle Tool from a strong tradition of software change management practices on the iSeries platform. The brand name of the product was OMS for some years, became Tight as a Drum in North America several years ago, and is now in world-wide distribution as TD/OMS. V6R1 is fully supported.

☑ **up a notch™ Regulatory Compliance Vulnerability Assessment + Mitigation**

This very comprehensive service is designed to prepare an enterprise well for a challenging regulatory compliance audit. We look at weaknesses in the operating system configuration, software change management, changes to crucial files, and operational procedures.

☑ **Bill of Health® security diagnostics and R_x for OS/400**

Bill of Health runs a fine tooth comb through operating system security vulnerabilities and threats. The product then composes very comprehensive documentation about the risks that have been discovered and the potential security implications of each discovery. The diagnostics report is a Ph.D.-level description of distinctions between world-class security practice and a company’s existing operating system configuration.

Click [here](#) to see compliance ideas specifically related to BPCS / ERP LX

Click [here](#) to go to the navigation page for IT security topics and standards