up a notch™


# Sample Deliverable:

## Regulatory compliance vulnerability assessment report

## Getting ready for your SOX audit

The document on the next five pages was prepared by Unbeaten Path for internal use by the CFO of a manufacturing enterprise. That company embraced the action steps encouraged by the content and their Sarbanes-Oxley audit was subsequently passed without any adverse findings in the final written opinion.

[ *The name of the enterprise and employees working in that enterprise have been thoroughly disguised.* ]

Unbeaten Path®

Return to the regulatory compliance **up a notch** services description


# High Performance Enterprises

## Sarbanes-Oxley Compliance Vulnerabilities

**This IT response prepared: October 12, 20xx**

## Background and overview

The Sarbanes-Oxley Act (SOX) holds corporate executives accountable for the information reported on key financial statements. Sections 302 and 404 of the legislation have the most direct impact on HPE as summarized in Schedule A.

### *Financial management subjects*

Financial management concerns about the accuracy of inventory valuation prompted the commission of a third-party study in early September. The report from that work stated that inventory values on the HPE balance sheet have been misstated as evidenced by frequent lump sum financial adjustments to cost of sales measurement. The report also concluded that there is insufficient financial information to simulate future business results and that the structure of the information that is available generates results that require substantial manual intervention.

In response, HPE funded and launched an aggressive project to address the eleven categories of findings/recommendations in that consulting report.

### *Information technology subjects*

Implications for HPE's IT function flow from the Public Company Accounting Oversight Board's interpretation of SOX as summarized in Schedule B. The six vulnerabilities noted in Schedule B are material and HPE management has now moved from our initial "assessment phase" to the remediation phase as detailed later in this document.

Our objective is to avoid variance findings in the January external audit. We are reasonably hopeful that the plan we have developed and the external resources available to execute that plan are sufficient to achieve that objective.

## Remediating financial vulnerabilities

Weaknesses in our application of BPCS accounting functionality have been identified and then addressed with training and support from a consulting firm (Unbeaten Path). A variety of material improvements are implemented or in the process of implementation.

The next fruit of our efforts shall be the announcement of a written standard cost accounting policy for the division. A draft of that policy is almost completed and it shall be reviewed by the plant controllers on October 19th.

Our strategy shall be to first apply the approved corporate **cost accounting policy** to the newly acquired Janesville site. We have retained Unbeaten Path to lead that effort as one facet of our campaign to replace the non-integrated/out-of-control Janesville systems with BPCS software.

The cutover to BPCS software in Janesville is currently anticipated at the end of the 2008 calendar year. As major parts of the Janesville effort are concluded, we will then take steps to adopt net internal control improvements vis-à-vis our current BPCS application at the Akron/Dalton facilities.

Return to the regulatory compliance **up a notch** services description


# Remediating IT vulnerabilities

The six IT vulnerabilities enumerated in Schedule B merit immediate attention and the content below demonstrates that each of those concerns are being actively addressed:

### *Vulnerability Number 1: monitoring changes to iSeries master files*

HPE has purchased and is in the process of implementing **Stitch-in-Time** Data Integrity software. If it is determined that an unauthorized change has been executed in a critical file, Stitch-in-Time provides comprehensive information to enable analysis of that change and subsequent risk mitigation.

Stitch-in-Time software saves the following information about every data change that is executed in an observed file:

- What the data record looked like before the change.
- What the data record looked like after the change.
- What user executed the change at precisely what time.
- The program or utility used to execute the change.

### *Vulnerability Numbers 2 and 3: precise definition of BPCS user access*

HPE has purchased and will soon start active usage of **By Invitation Only** software. This product greatly simplifies the definition, maintenance, removal, and documentation of BPCS user authorization information.

Reporting from this software is designed to support audit inquiries. For example, the product will present the entire list of users who have access to a given BPCS program.

The product has a tiered user template functionality which will help us establish and sustain separation of duties.

### *Vulnerability Number 4: BPCS data clean-up*

HPE recognized that the enormous quantity of obsolete item master records associated with unused divested companies makes it more difficult to focus on the integrity of data pertinent to running our division. Therefore, we have purchased two BPCS "janitorial" software products to help us clean out the database: **Item Undertaker** and **Locksmith**.

Beginning in late October, Item Undertaker has been used to deactivate several tens of thousands of obsolete item master records.

Locksmith is an archiving tool that physically removes deactivated item master records and moves them out of the production library together with all of the transaction history associated with those records.

Locksmith will also be used to archive very large quantities of old HPE data in a way that will permit BPCS to reacquire access to that information as if it had never been removed from our BPCS production files. (We have elected to archive instead of purge old BPCS data.)

Return to the regulatory compliance **up a notch** services description


# Remediating IT vulnerabilities, *continued …*

### *Vulnerability Number 5: iSeries operating system security*

HPE is considering the purchase of this software: **Bill of Health Security Diagnostics.** The product will provide approximately 50 risk assessment reports describing our iSeries security status together with a competent prescription to address each identified vulnerability.

The objective is to identify and remediate vulnerabilities within our internal network and any internal control weaknesses so as to prevent deliberate or accidental exploitation by a hacker, employee, or contractor. If we proceed promptly, it is reasonable to think that we will be well prepared for our January audit.

The information delivered by this product complies with the most stringent requirements for risk assessments, vulnerability analyses, and internal control due diligence described by the Information Systems Audit & Control Association (COBIT). COBIT is a more demanding standard than the **PCAOB interpretation of SOX** requirements.

### *Vulnerability Number 6: software change management*

HPE is currently ready to execute the purchase and implementation of a change management software product called: **Tight-as-a-Drum**. This very comprehensive iSeries object control product will enable us to codify and enforce good software change management practices. One of the utilities arriving with this product will enable an auditor to print off the entire history of changes to any selected iSeries object.

If we proceed promptly with the implementation of this product, it is reasonable to think that it will be in operation by the time our final follow-up audit takes place. Unfortunately, the implementation of any software change management product will only help us prospectively. It will not address historical errors and omissions.

It is our fond hope that the external auditors will not include information about our historical change management problems in their written opinion if we can demonstrate that we have an excellent process enforced by strong software for future time periods.

## Concluding comments

A variety of significant challenges merit simultaneous attention by the Divisional Controller:

- ☑ Remediation of identified SOX vulnerabilities in finance and IT
- ☑ Leadership of the Janesville financial/systems integration on BPCS
- ☑ Development/documentation of world-class policies and procedures
- ☑ Redefinition of IT roles and responsibilities in the form of formal job descriptions and then a recruiting effort to staff authorized positions

We have retained the professional services of Unbeaten Path International so as to realize immediate traction on these challenges. They have assembled a consulting team to help HPE and members of that team are making very constructive headway.

Return to the regulatory compliance **up a notch** services description


# Schedule A

## *Overview of Sarbanes-Oxley Sections 302 & 404*

The two parts of the **Sarbanes-Oxley Act** (*numbered H.R. 3763, passed in the 107th Congress on January 23, 2002*) which have the biggest impact on HPE are sections 302 and 404. These sections were designed to improve the reliability and accuracy of corporate financial reporting.

***Section 302***

Requires management to proactively design and implement steps so as to verify the reliability of internal systems and controls for financial reporting. We must document controls that have a bearing on financial reporting, test them for efficacy, and report on gaps and deficiencies.

***Section 404***

Requires external auditors to provide an annual written opinion about the effectiveness and comprehensiveness of the Section 302 compliance steps that have been implemented by corporate management. This written opinion will be included in the company's annual report.

## Implications for HPE - finance

Management is precluded from concluding that the company's internal control over financial reporting is effective if there are one or more material weaknesses.

HPE management has determined that these important financial vulnerabilities required attention in the short term:

- User understanding of BPCS accounting (CEA) functionality was not sufficient.
- The division did not have a formal cost accounting policy and current practices depart from accepted standard cost accounting practices.
- Work-in-process (WIP) inventory counts are not captured with sufficient detail.
- BPCS bill of material structures are not well designed to value WIP and several different methodologies are used for bill of material structuring.

To be effective, HPE's internal controls must be analyzed and weakness addressed. All the controls necessary to provide reasonable assurance about the fairness of a company's financial statements must be implemented/performed by appropriately qualified employees.

Return to the regulatory compliance **up a notch** services description


# Schedule B

## *SOX Implications for Information Technology at HPE*

The Public Company Accounting Oversight Board (PCAOB) created an official standard for interpreting the Sarbanes-Oxley Act. The official title of that document is: "Auditing Standard No. 2 (AS#2): An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statement.

AS#2 makes only very high level mention of information systems. Nevertheless, these two pertinent quotations make it clear that PCAOB intends heavy information systems involvement in SOX compliance audits:

- *" ... the auditor should determine whether management has addressed the following elements: ... Including information technology general controls, on which other controls are dependent."*
- *" ... Information technology general controls are part of the control activities component of internal control ... "*

Now, since AS#2 enables (and encourages) auditors to dig into great detail across nearly every business process, and given that those details are processed by and stored within our iSeries, then the implication is that HPE's IT management must be fully engaged in SOX audit preparations and also the external audit process.

## Implications for HPE – information technology

HPE management has determined that these important IT vulnerabilities must be addressed in the short term:

1. Changes to critical iSeries master files have not been monitored.
2. The concept of "least privilege" (*giving users access only to data and applications that they have a direct need for*) has not been implemented.
3. Within BPCS, there are at least two concerns about BPCS users:
   - Individuals without sufficient knowledge have the user authority to change financial application configurations.
   - A separation of duties analysis is needed.
4. BPCS data integrity maintenance has been difficult because our database has been cluttered with millions of obsolete records associated with Consolidated Foodways
5. The integrity of our OS/400 security administration has not been audited in a comprehensive way.
6. Software change management principles have been neglected.
   - There is currently no practical way to **enforce** comprehensive procedures.
   - Unbeaten Path has reported evidence of ill-advised object movements which introduce risk and have actually caused system problems.
   - Reporting disciplines have not been sustained.

Return to the regulatory compliance **up a notch** services description