

**Internal Audit Report
Corporate
2008**

Internal Audit Department
Co-Source: Securance Consulting



SAMPLE TABLE OF CONTENTS

SECTION I: EXECUTIVE SUMMARY

INTRODUCTION

OBJECTIVES & SCOPE.....

METHODOLOGY & ASSESSMENT.....

CONCLUSION

SECTION II: SAMPLE ANNUAL REVIEW REPORT

BACKGROUND (omitted in this sample report)

SPECIFIC OBJECTIVES AND SCOPE (omitted in this sample report)

APPROACH AND ASSESSMENT (omitted in this sample report)

ANALYSIS OF FINDING.....

SECTION III: WRAP-UP

SECURANCE VALUE



SECTION I: EXECUTIVE SUMMARY

INTRODUCTION AND SCOPE

During the fourth quarter of 2007, the Internal Audit Group, through a co-source agreement with Securance Consulting, conducted an integrated technology controls review of the ERP application.

OBJECTIVES AND SCOPE

The objective of the review was to assist the Internal Audit organization in testing the effectiveness the IT controls specific to the ERP application. Technical application controls include the following types of controls...

The scope of this review was limited to the...

METHODOLOGY AND ASSESSMENT

To achieve the objectives of the review, we designed an approach for understanding, documenting and testing the controls surrounding the ERP application. Including....

CONCLUSION

Based on our review and our experience assessing the financial reconciliation process and ERP systems, the ERP environment is adequately controlled.

We rate our findings as follows:



Priority: Recommend immediate attention.



Priority: Requires attention within the coming year.



Priority: Long-term issue or an issue with minimal financial/operational impact.

ANALYSIS OF FINDINGS – SAMPLE ANNUAL REVIEW

No. 1: Income Statement Misstated

The minority interest percentage is manually calculated and reviewed by the Consolidations/SEC reporting group for all subsidiaries with a minority interest. The manual calculations are not being completely reviewed for accuracy. Per review of the September 2007 calculations, and of the seventeen subsidiaries with a minority interest, only three were properly calculated and substantiated with appropriate sign offs as being reviewed by the Consolidations/SEC reporting group. As a result, the financial statements are incorrectly stated.

Recommendation:

We recommend that the manual process of calculating the minority interest percentage for all applicable subsidiaries with be fully reviewed by a supervisor or manager in the Consolidations/SEC reporting group before inclusion in the financial statements. We also recommend that the Company consider automating this process to ensure the calculations are accurate and complete.

To re-design the process of minority interest calculations, we strongly recommend that management designate a project team that, at a minimum, consists of the following personnel:

- Chief Financial Officer;
- Chief Information Officer;
- Corporate Controller;
- Treasurer; and,
- Lead Finance Director.

A sample automation work flow process can be provided upon request.



Priority: Recommend immediate attention.

Management's Response:

No. 2: Root Access

An excessive number of users (company employees and ERP vendor support personnel) have been granted unrestricted 'ROOT' access to the application. 'ROOT' access allows unrestricted access within the application, creating improper segregation of duties and unauthorized access to data files and application processes.



Priority: Recommend immediate attention.

ANALYSIS OF FINDINGS – SAMPLE ANNUAL REVIEW

No. 2: Root Access continued

Management's Response:

No. 3: AIX Operating System Security

The AIX system is the server that hosts the ERP Application. We performed a comprehensive review of all of the security setting to determine how susceptible the server was to being breached internally. With the exception of password management/administration the server is relatively secure. We did identify several 'house-cleaning' type activities that should be addressed to improve the security of the AIX server. Below is a summary of the issues, including password management that we identified.

- Password Management – current password change interval, history length, and history period is set to 0. These should be set to 4, 6 or greater, and 26 or greater respectively. Additionally, login retries is currently set to 5, our recommendation, which is consistent with 'Best Practices' is 3 retries before the system locks-out a user.
- Password Discrepancies – there are 29 users whose passwords are either in the Shadow Password file or in the normal Password file. All passwords should be in both files. We recommend that these passwords be reviewed and synchronized between the two system files.

Recommendation:

We can make the details related to the finding above available to the AIX Administrator so that he can address these 'housekeeping' issues. We recommend a review of the supporting details related to each item above and the implementation of the related housekeeping recommendation.



Priority: Requires attention within the coming year.

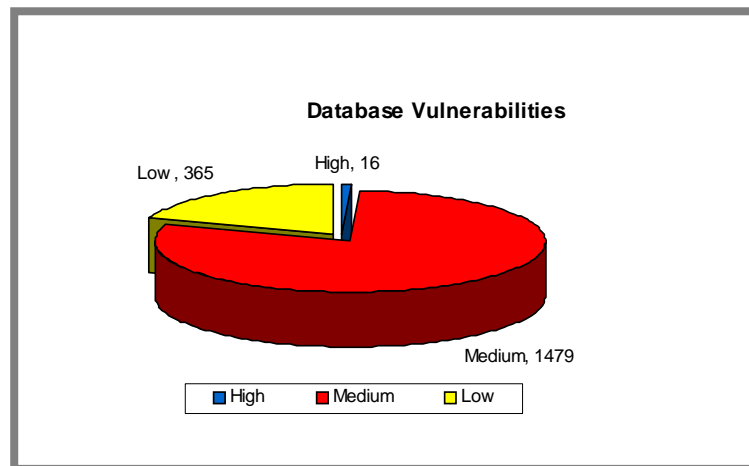
Management's Response:

No. 4: Database Vulnerabilities

To determine the general state of database security we performed procedures against the application's database. Our objective was to determine the security posture of the database and to assess the level of effort it would take an unauthorized user to gain direct access to the database. We discovered an unusually high number of 'High' risk vulnerabilities specific to the database. Some of these vulnerabilities if exploited could corrupt the entire database. The graph below is a summary of the types of vulnerabilities that present a 'High' risk to the technology environment.

ANALYSIS OF FINDINGS – SAMPLE ANNUAL REVIEW

No. 4: Database Vulnerabilities continued



Recommendation:

We recommend that all critical database technologies be review for 'High' risk vulnerabilities and that at a minimum all 'High' risk vulnerabilities be addressed by implementing the vendor recommended fix. Most of the vendor recommended fixes simply require the application of a vendor supplied patch or configuration change.

While perimeter security may be considered adequate most breaches occur by internal users. By its nature, having high risk weaknesses at any layer in a technology environment exposes the entire environment to being breached.



Priority: Recommend immediate attention.

Management's Response:

SECURANCE VALUE...

Securance Consulting would like to **THANK YOU** for your business. Aside from benefiting from the highest level of service possible, you also received unique advantages that only Securance Consulting delivers.

Our hands-on approach is tailored to fit the needs of your organization. Our technical expertise, outstanding reputation, and personalized attention ensure you a level of service surpassed by no other internal audit services firm in the market.

As a Securance customer, you can be confident in your sound decision to manage your technology risk with a co-sourced relationship with Securance!