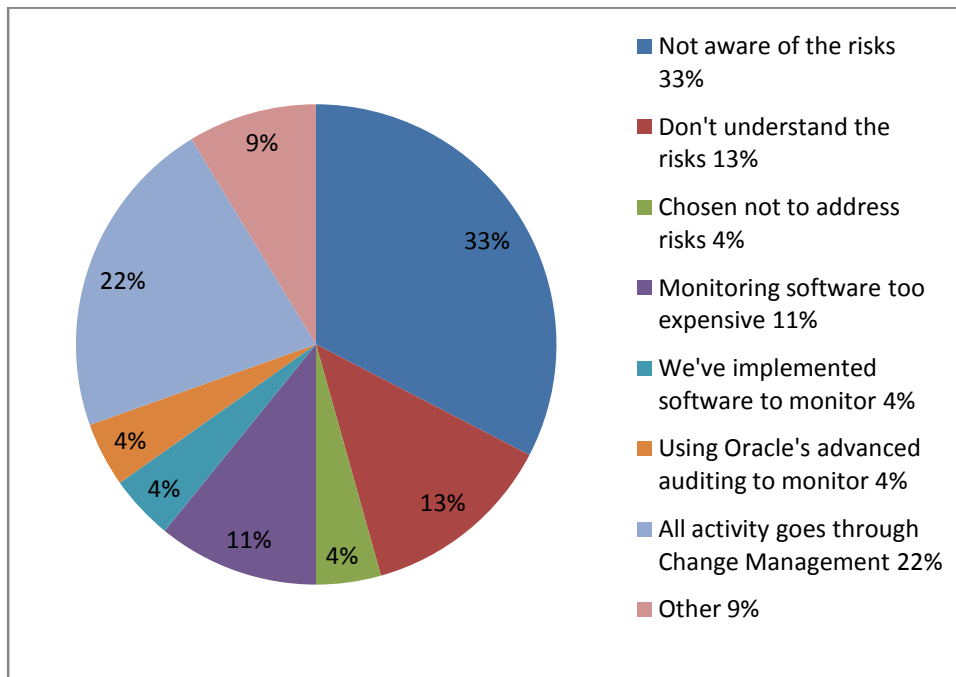




## SQL Forms Survey Results and Analysis

The intention of the survey was to determine awareness of and response to risks related to access to SQL forms in a production Oracle eBusiness Suite environment. The background given related to the risks are Oracle’s Metalink document 189367.1 (Best Practices for Securing Oracle eBusiness Suite) and our white paper “Accessing the Oracle Apps Database without a Database Login.” As you will see from the demographic information in Appendix A, respondents to the survey have varying skills and experience with Oracle eBusiness Suite and work for companies representing various install bases. The survey results are as follows.

Question: The following best describes my awareness of the risks related to access to SQL forms.



### Analysis

This question allowed for multiple responses. Here are the key findings:

- 46% of the respondents were not aware of the risks or didn’t understand them.
- 15% of respondents were aware of the risks, but either have chosen not to address the risks or feel the cost of monitoring software is too expensive.

- Only 8% of the respondents have purchased and installed software or are using Oracle's advanced auditing to monitor the risks
- 22% of respondents require that activity through the SQL forms go through IT change management. However, none of the respondents said they reconcile actual activity from system audit trails to their change management approvals.
- A noteworthy finding was that no respondent indicated that "My company reconciles actual activity to our Change Management approvals" suggesting that none of the companies in the survey are following the best practices in the Institute of Internal Auditors guidance on change management.

## ***Recommendations***

### All companies

Consider downloading and reading the white paper called "Change and Patch Management Controls: Critical for Organizational Success" from the Institute of Internal Auditors at <http://www.theiia.org/guidance/technology/gtag/gtag2/>. This guide contains some practical guidance to help you understand what internal auditors deem to be best practices for change management. One quote from this guide related to unauthorized changes that should put fear in you is "Lower is better, but typically the only acceptable number of unauthorized change is zero; one rogue change can kill an entire operation or create material risk." The only way to identify unauthorized changes is to reconcile actual changes with the population of changes from the system to those that are authorized via your change management process. In order to generate an audit trail of changes from the system, you would need to use either a log or trigger-based solution.

### Companies not aware of the risks

We will be hosting a free webinar in early August to highlight the risks related to access to SQL forms and to discuss best practices related to such. Watch for an email with more information. Those interested in signing up for the webinar, but who are not on our email list can sign up from a link on our home page ([www.erpseminars.com](http://www.erpseminars.com)).

### Companies aware of the risks, but who have taken no action or think that monitoring software is too expensive

First, participate in the upcoming webinar to make sure you are fully aware of the risks with SQL forms. Second, there are various software companies that provide either trigger or log-based auditing software. Based on our channel checks, prices range from \$15K to several hundred thousand installed. We have worked with several software providers to help them identify the critical tables to monitor including the SQL forms. This has added to the quality and reduced the costs of several software solutions.

### Companies that have installed software or Oracle's advanced auditing to monitor SQL forms activity

Consider signing up for the [Internal Controls Repository](#) (ICR) and compare the tables/columns you are monitoring versus those we have identified. The 'Tables to Audit' spreadsheet in the ICR is a public domain effort and your participation would be welcomed and benefit other companies in the future. To the extent, we have identified content you aren't currently monitoring, consider adding more audits.

Companies requiring SQL form activity to go through your change management activity, but not reconciling back to your change management process

You are part of the way there, but 'you don't know what you don't know.' How can you be certain that all changes are going through your change management process? The only way to know whether or not there are unauthorized changes is to have an audit trail of actual changes and compare them to those that were approved via your change management process.

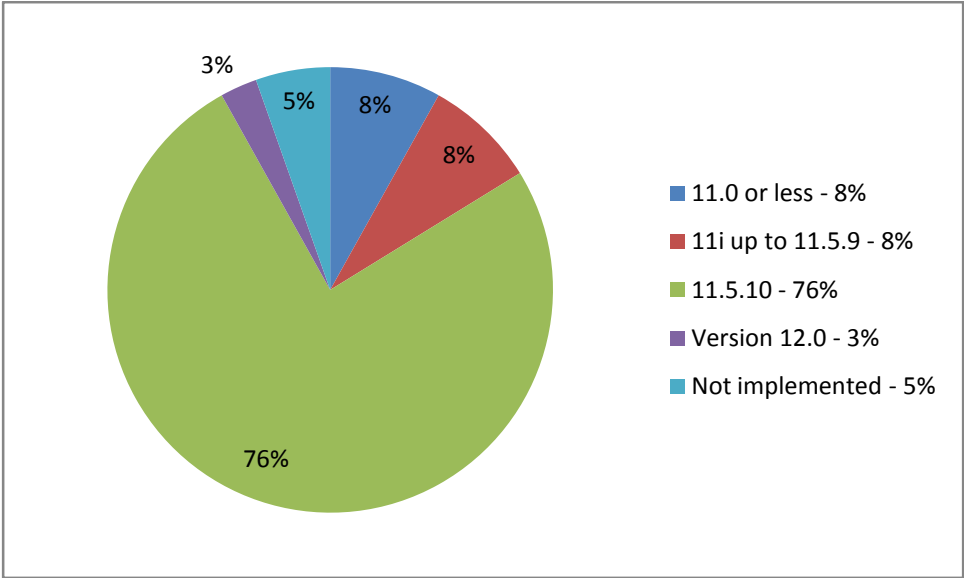
***Conclusion***

The results of the survey are shocking. The companies that responded are mature users of the eBusiness Suite with nearly 85% of the respondents have been live for more than two years and 64% over five years. Sixteen percent of respondents have over 2,500 professional users (excluding those that just use Self-Service applications such as Employee SS or OTL). Access to SQL forms is like giving an end user access to the 'Apps' login and only 8% of companies are actively monitoring for activity via a trigger or log-based solution. The results also indicate that none of the companies that require such changes to go through their change management process are monitoring for unauthorized changes (i.e. reconciling actual changes from system audit trails to approved changes).

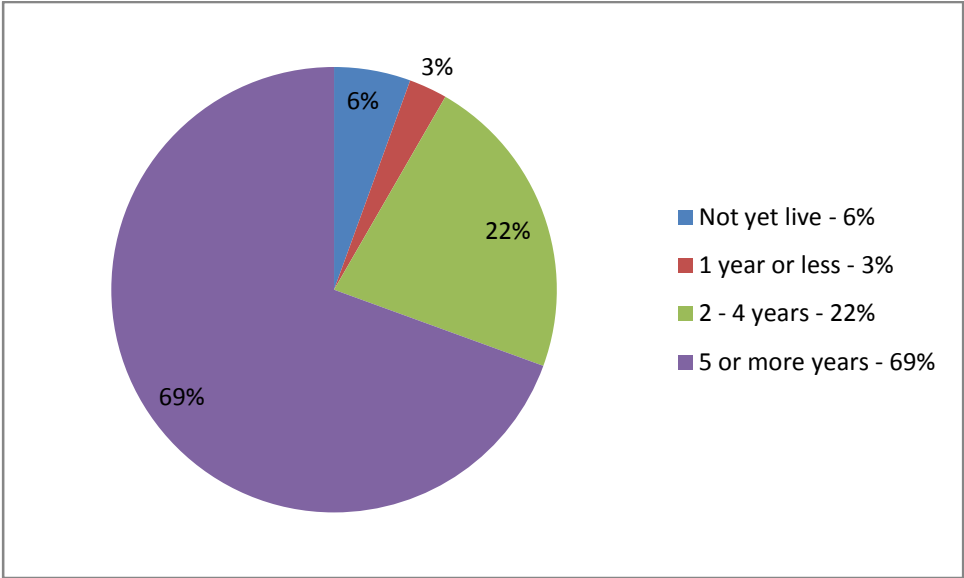
While I have heard horror stories about IT auditors placing a lot of emphasis on controls related to the 'Apps' database login, the survey results seem to show that both auditors and management need to take another look at this issue.

# Appendix A – Demographics of the Respondents:

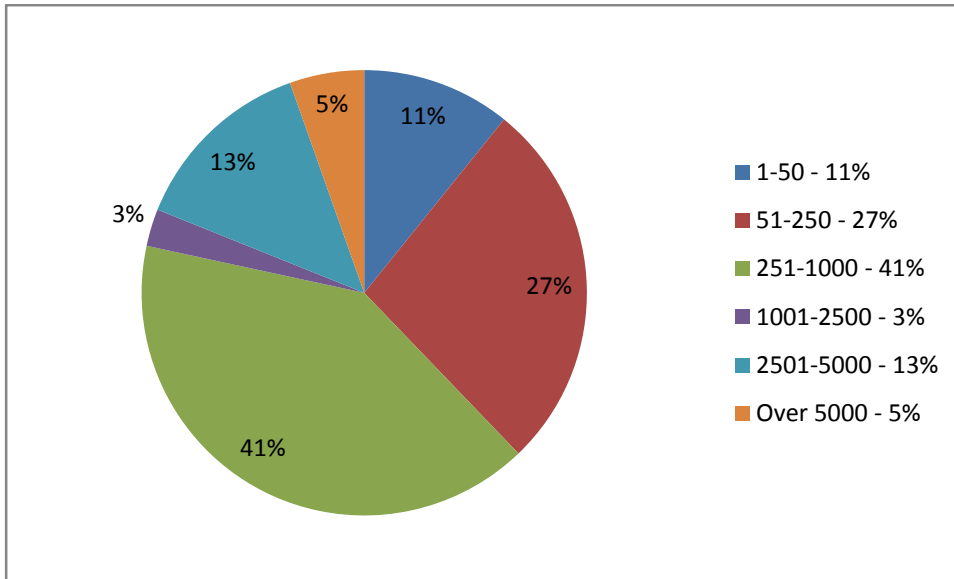
Version of the applications



How long have you been live with your Oracle eBusiness Suite?



How many users (not counting those with just self-service apps):



Describe your role:

