

Thinking outside the SOX

Let's talk about
What to do with all these IT
reports?



© 2019 PricewaterhouseCoopers LLP. All rights reserved.

SOX Centre of Excellence

Gerhard Wiese
SOX Centre of Excellence Manager

Thinking outside the SOX: 3 simple steps to ensure “IPE” SOX Compliance

Are you experiencing challenges in your ‘IPE’ (“Information Produced by the Entity”) approach and are you confident that your data supports all your key controls for Sarbanes-Oxley (SOX) compliance? In the SOX Centre of Excellence we frequently see our clients experience this specific challenge - how do I get my IPE SOX compliant?

As part of the SOX Centre of Excellence, I have had many clients approach me and ask: “How do I ensure the information I use is accurate and complete for SOX purposes?”. This is a very important question, especially in the current regulatory environment where organisations are expected to ensure that validation of its IPE occurs.

Why this emphasis? Simply put, if your organisation uses inaccurate or incomplete data in the execution of key controls, it may potentially face the consequence of having a material weakness disclosed in your SEC filings.

I would therefore suggest the following simple four step approach that will assist you in developing your IPE testing approach:

1. Create an IPE inventory per Category

By creating a listing of all SOX relevant IPEs that support key controls, you will have visibility over the full scope of IPE testing required. It would also be important to determine the attributes to be included in the listing, which may include:

- Report type;
- Key control supported;
- System where data resides;
- Reporting tool used (if applicable);
- Report owner;

- Last change or tested date;

There are three report type classifications, being standard or canned reports; customised reports/ queries subject to IT General Controls (ITGCs) and customised reports/queries not subject to ITGCs, known as “ad-hoc” queries.

2. Categorise your IPE

Your report classification will assist you in developing appropriate testing procedures, based on how the reports have been created.

- A standard or canned report is developed by the software provider and comes with the software and typically cannot be modified by end users;
- A custom report or query is built in-house by your IT team to meet specific needs of the business, using specific software functionality. Where subject to your change management process, changes to these IT reports will be subject to the normal change testing such as testing and approval;
- An “ad-hoc” query not subject to ITGCs is usually more risky, since in this case the end user can use any set of parameters to generate a report. This would require higher scrutiny since it is not subject to the normal control testing.

3. Determine your testing approach

You can now determine the most effective testing approach. A key consideration, regardless of the approach followed, is that appropriate evidence should always be maintained.

Testing approaches include:

- Obtain and evaluate programs/queries generating the reports;
- Obtain and evaluate parameters used;
- Sample data in resulting report; and
- Identify data sources (e.g. database, system).

4. Maintain your IPE process

Accountability and ownership of the process to a specific set of individuals in your risk and compliance team is cardinal to success. These individuals have to be tasked to maintain and update the IPE inventory as well to train report owners to ensure they understand their responsibilities.