# IPE audits and inspections

Seek more evidence now

Merely testing for SOX compliance doesn't cut it with regulators. Recent audit inspections of Information Produced by the Entity (IPE) call for greater evidence that companies perform and document their own procedures.

Management, as well as auditors, have an obligation to test that IPE is complete and accurate to meet Auditing Standards (AS) reviews. The findings delivered by the Public Company Accounting Oversight Board inspections raise several questions about how organizations provide evidence to auditors, including:

- What are the major challenges companies face to comply?
- Who is responsible for testing ownership?
- Do companies benchmark key IPE and, if so, what does that look like?

KPMG surveyed clients in a cross-section of industries with market capitalization from $200 million to more than $300 billion to determine what comprises their respective IPE programs. We collected data related to unique IPE challenges, the range and average number of IPE that is required to be tested, testing responsibility, and other factors that ultimately hinder successful execution of the program.

Based on clients' responses, we identified differences and similarities in how they manage their IPE. The trends presented may assist others in developing a path forward to collect appropriate evidence needed to perform and document their own procedures.

## The challenges uncovered

Among the companies we polled, the most common challenge was an overall lack of IPE ownership. When there is a lack of ownership oversight, any turnover of control operators or leadership can compound the issue, so it is important for ownership to carefully monitor IPE. Difficulties also occur due to a failure to consider the risks occurring within the IPE (or controls) process. Additionally, we've repeatedly seen control gaps among our clients that may not have a strong leadership view on the importance of standardized audit procedures. The continued challenges of IPE programs faced by companies is a potential cause of the increased regulatory scrutiny.

# Challenges facing owners, controllers, and auditors

| | |
|---|---|
| Lack of ownership/ownership changes | 42% |
| Difficulty testing due to report complexity, dynamic system data, and/or lack of access to parameters/logic | 33% |
| Identification and scoping of key reports within management controls | 17% |
| Understanding of IPE validation requirements and external audit expectations | 8% |

# Risk assessment and testing needed?

It's important to perform a risk assessment to identify potential risks associated with an interprofessional education program. This can involve analyzing factors such as the type of IPE, the level of complexity involved, potential adverse events, and the consequences of those events. IPE testers must also consider the risks affecting relevance and reliability of the individual data elements contained within the IPE including data input, integrity, and extraction risks. Data input risks result from data that is incompletely or inaccurately entered into the IT system. Manually input data raises data input risks. Data integrity risks are the risks that data is inappropriately altered during processing, while in storage, or during transfer from one system to another. Insufficiently restricted access or lack of monitoring over databases can increase data manipulation risks. Data extraction risks result from the incomplete or inaccurate extraction of data from IT systems. This could also result from including irrelevant data during the extraction process. Additionally data manipulation after extraction could also result in inaccurate or incomplete IPE. Gaining a thorough understanding of the data extraction process and maintaining a chain of custody for the IPE helps to reduce data extraction risks for IPE. Without proper risk assessment, it's impossible to develop an effective testing approach.

Once risks have been identified, it's important to determine which IPEs are critical to the success of the program (key) and which are less important (non-key). For example, if a certain IPE directly impacts the business operations or key financial statements, then it would be considered key. If it involves a routine task like filling out paperwork, then it would be considered non-key.

# Spreadsheets—risk ranking

**The risks associated with key spreadsheets will determine the appropriate level of controls required to help ensure the information produced is reliable. Risks are assessed based on qualitative measures to determine an overall three-tier risk rating, as follows:**

**Low risk**

Spreadsheets serve as an electronic log, information tracking system, or are used to perform simple calculations. There is low dependency on the spreadsheet and the design is not complex.

**Medium risk**

Spreadsheets that perform simple calculations or collate or format data that can be duplicated manually within required timelines are considered medium risk.

**High risk**

Spreadsheets that support complex calculations, valuations, or modelling tools are considered high risk. This also includes spreadsheets facilitating simple calculations of a very large volume of data that cannot be easily or quickly duplicated manually. These spreadsheets can be considered information technology (IT) applications.

When evaluating the risk of key spreadsheets, the following qualitative factors should be considered:

- Purpose of the spreadsheet
- Number of spreadsheet users
- Complexity of calculations or volume of data
- Quality and type of inputs
- Frequency and extent of modifications
- Availability of external sources to validate the output of the spreadsheet.

After identifying key and non-key IPEs, it's important to further simplify different categories of IPEs that may exist. These can include standard IPEs that are done consistently, custom IPEs that are tailored to specific situations, ad-hoc IPEs that are done on an as-needed basis, etc. This will help to determine the appropriate testing approaches for each type of IPE. Based on the combined factors of risk assessment, type of IPE, and frequency of that IPE being used, the testing approach should be adjusted accordingly. For example, if a key IPE involving complex equipment is identified as high-risk, then it may be necessary to conduct frequent testing and simulations to ensure that all stakeholders are prepared in case of an adverse event. Overall, by implementing a thorough risk assessment and developing appropriate testing approaches, institutions can ensure that IPE programs are effective and safe for all stakeholders involved.

## Whose job is it anyway?

| | |
|---|---|
| Business process/ control owners<br>**70%** | IT<br>**20%** |
| Compliance/ Internal Audit<br>**70%** | No clear ownership<br>**30%** |

The majority (70%) of respondents share IPE ownership between the Business Process/Control Owners and Compliance/Internal Audit. A smaller percentage also have IT in the mix while 30% have not defined IPE ownership in their organization. Business process and control owners are typically considered leading practice as the ultimate owners of IPE. These users are usually the generators of the information and, therefore, are the most intimately involved with the development, storage, and reporting of the data. The reviewers of the control should not be completing this step, but rather reviewing how the information is gathered. IT may be an appropriate owner dependent on the nature of the control or owner of the data. Ideally, this responsibility is shared between owners and IT, given the digitization of reporting and data storage. Disturbingly, approximately 30 percent of companies reported no clear ownership.

## Where does responsibility for testing fall?

| | |
|---|---|
| Internal Audit/ Cosourcing<br>**80%** | IT<br>**20%** |

An overwhelming majority of our clients' Internal Audit/Cosourcing teams have accepted the responsibility of testing IPE, with IT being the next in line. As noted above, Internal Audit is the appropriate group to review and test the IPE procedures produced by the business and control owners. Appropriate independence needs to be maintained, based on the line of defense in use.

## To benchmark or not to benchmark?

| | |
|---|---|
| Yes<br>**80%** | No<br>**20%** |

Eighty percent of the responses indicated benchmarking processes are being implemented or are already in use. This is a common trend among companies to streamline the audit and can be effective (if implemented appropriately) year-over-year and across organizational and personnel changes. However, this process will only be effective in stable environments where change is not occurring at a high frequency.

# Which presentation is most appropriate?

In our survey, respondents indicated that they utilize a wide array of methods to document IPE, including:

- Standard Word documents/templates outside of the audit system
- As a stand-alone control within the audit system
- As a test step within a management review control.

Any of these methods are sufficient, but whichever path is chosen, the documentation should be reperformed by internal and external audit teams to ensure the data is complete and accurate. Additionally, the method for documentation and presentation should indicate why management and/or the control owners are confident the correct and appropriate data is being utilized in the performance of the control.

The survey questions considered the parameters presented in the following table.

# New IPE standards and categories

**Your responses to our survey provided valuable information for this table.**

| Auditing standards | IPE categories |
|---|---|
| **AS 1105.10—Using Information Provided by the Company**<br><br>When using information produced by the company as audit evidence, the auditor should evaluate whether the information is sufficient and appropriate for purposes of the audit by performing procedures to test the accuracy and completeness of the information or test the controls over the accuracy and completeness of that information and evaluate whether the information is sufficiently precise and detailed for purposes of the audit.<br><br>**AS 2201.B31—Benchmarking of Automated Controls**<br><br>To determine whether to use a benchmarking strategy, the auditor should assess the following risk factors. As these factors indicate lower risk, the control being evaluated might be well-suited for benchmarking. As these factors indicate increased risk, the control being evaluated is less suited for benchmarking. These factors are:<br><br>• The extent to which the application control can be matched to a defined program within an application<br>• The extent to which the application is stable (i.e., there are few changes from period to period)<br>• The availability and reliability of a report of the compilation dates of the programs placed in production. (This information may be used as evidence that controls within the program have not changed.) | **Configured Reports (covered by GITC)** – System-generated reports that the end user does not have the ability to modify report logic or parameters.<br><br>**Configurable Reports (covered by GITC)** – System-generated reports that the end user has the ability to modify "parameters" only. End users are unable to make changes to report logic.<br><br>**Configurable Reports (not covered by GITC)** – System-generated reports that the end user has the ability to modify parameters of the report. End users may also have the ability to edit/modify the "report logic." Each time the report is run, no reliance is placed on General IT Controls (GITC).<br><br>**Spreadsheets** – Non-system-generated reports: manual spreadsheets or schedules. End users have the ability to enter and modify all information. If a report is extracted into Excel and the data is not manipulated, then it is still considered a report. The trigger is manipulation (e.g., adding data, deleting data) of the report data that changes the IPE to a spreadsheet. |

## Can we automate?

Automating IPE testing can be a complex task but there are steps that can be taken to streamline the process:

1. Identify testing requirements: First, identify the specific testing requirements for each IPE scenario. This can involve analyzing factors such as competencies, learning objectives, and assessment criteria.
2. Develop test scenarios: Once the testing requirements have been identified, develop test scenarios that match those requirements. This can involve creating a series of predefined scenarios and cases that can be used to simulate IPE scenarios.
3. Use technology to automate tests: There are many different types of technology that can be used to automate IPE testing, such as simulation software, virtual reality, artificial intelligence-based simulations, etc. You can leverage these technologies to automate testing, such as to check the accuracy and completeness of documentation, to monitor for patient safety concerns, and more.
4. Continuous monitoring: With automation, continuous monitoring of IPE events and performance can become possible. Automated alerts can be set up to flag cases that do not meet certain criteria, such as the wrong medication, missed doses, or incomplete orders. This can help to identify problems early and take corrective action.

By automating IPE testing, institutions can streamline the testing process, ensure that compliance requirements are followed, and reduce the risk of errors or adverse events. Additionally, it can help to free up valuable time and resources for other activities related to IPE program management, such as curriculum development or stakeholder.

## What does it all mean?

The basic IPE principle to keep in mind when reviewing these trends is the need for management to have a process to confirm that IPEs such as key reports, spreadsheets, and schedules used in executing control activities are complete and accurate. KPMG can assist with identifying opportunities to support our clients, to build out these procedures where reasonable, or help strengthen subpar processes that require constant rework each year. Providing our clients training at both the leadership and owner level with education on the importance of consistent and standardized IPE processes is a key part to their audit success.

Discover more KPMG technology risk insights by visiting read.kpmg.us/TRM.

# Contact us


**Subash Samuels**
**Principal,**
**Technology Risk**
**KPMG LLP**
**T**: 213-593-6656
**E**: ssamuels@kpmg.com

**Nadine Sborz**
**Director,**
**Technology Risk**
**KPMG LLP**
**T**: 480-459-3495
**E**: nyassine@kpmg.com