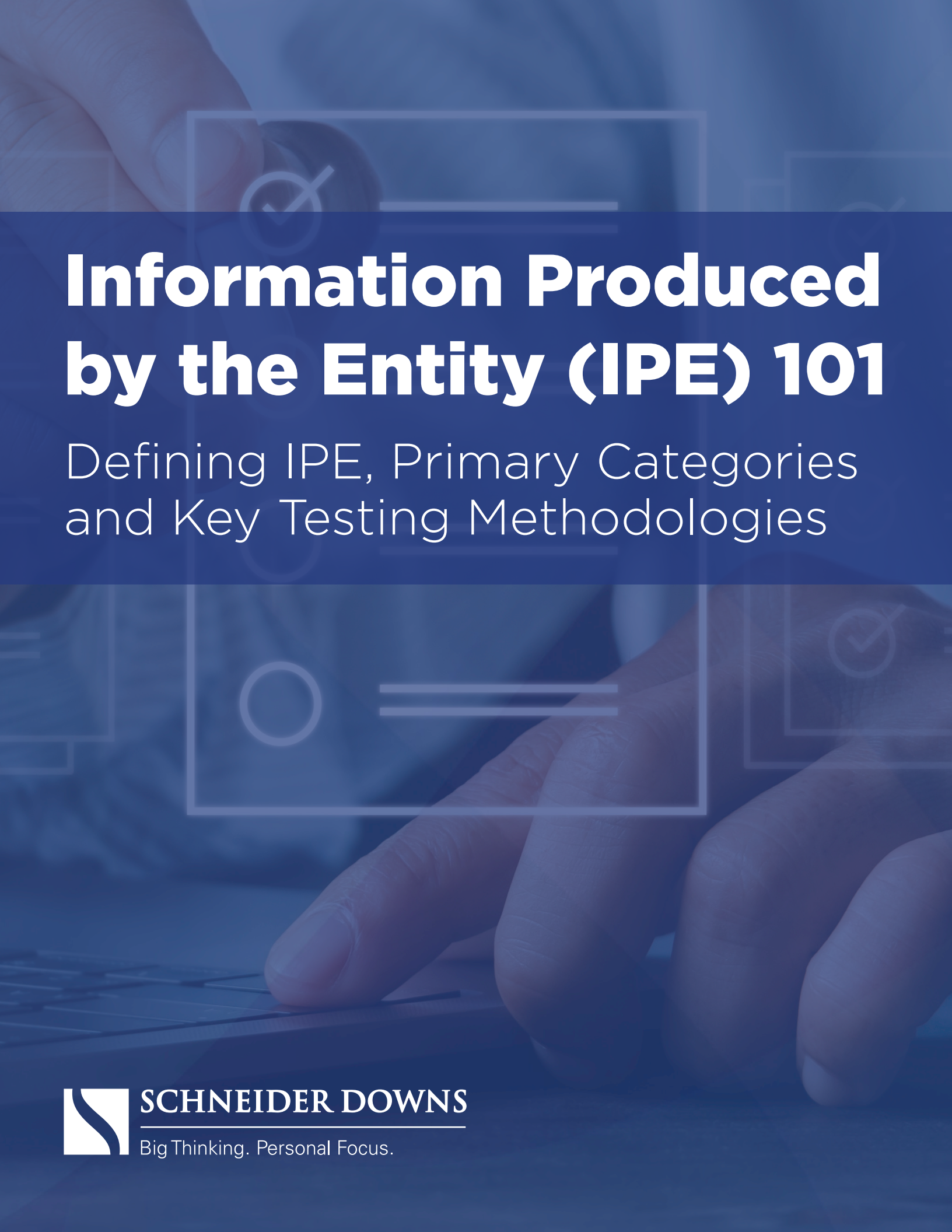

Information Produced by the Entity (IPE) 101

Defining IPE, Primary Categories and Key Testing Methodologies

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

Information Produced by the Entity (IPE) 101

Defining IPE, Primary Categories and Key Testing Methodologies

Sarbanes Oxley (SOX) testing is no stranger to the ebbs and flows of accounting trends. Every year, the Public Company Accounting Oversight Board (PCAOB) reviews a sample of audits for compliance. One of the constant themes is that firms are struggling with identifying and documenting the completeness and accuracy of IPE or Information Produced by the Entity. To help you avoid this challenge, let's define IPE, including its main categories and essential testing methodologies.

What is IPE?

The **PCAOB defines IPE** as all the information, whether obtained from audit procedures or other sources, that is used by the auditor in arriving at the conclusions on which the auditor's opinion is based. Audit evidence consists of both information that supports and corroborates management's assertions regarding the financial statements or internal control over financial reporting and information that contradicts such assertions.

When conducting an audit in accordance with Internal Controls over Financial Reporting (ICFR), auditors typically break IPE into two groups: Key Reports and Populations. Key reports are classified as any data used by management in the performance of a control whereas populations are data obtained by auditors to select a sample of transactions to verify management's process.

Regardless of which type of IPE is present, the auditor has an obligation to document the procedures performed to gain comfort over the completeness and accuracy of the data which will be discussed in the *Key Reports* section below.

What Does Completeness and Accuracy Mean?

When evaluating the completeness and accuracy of IPE, the **PCAOB states** that 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.

Simply put, when evaluating the IPE used in a control, the auditor must document the methods and rational for how they obtained comfort over the accuracy (individual line items) and completeness (report totals). When determining the audit procedures required to validate the completeness and accuracy of the data, each audit firm will have their own guidance depicting the required procedures, but it will also vary based upon the IPE report type. It is important to align testing plans with your external audit partner as you develop your IPE approach.

Populations

Populations are system-generated reports provided to auditors to select a sample of transactions to verify management's control procedures. Only the auditor must attest to the completeness and accuracy of the population.

For example, when testing a control over the approval of purchase orders, auditors will test to verify that orders were appropriately approved in accordance with company policies. They must first obtain the listing of all purchase orders (i.e., the population) and confirm that this population accurately reflects all purchase orders during the defined period.

This is typically done by verifying the source system is in scope for IT General Controls testing, obtaining the relevant input parameters/query used to create the population and tying row counts from the system screenshot to the report output. Another method to gain comfort over the data is to inspect the SQL/query used to create the population to understand how the data was generated.

Key Reports

If system-generated data is utilized by management to perform a control, then it is considered a key report. There are four types of key reports:

- **Standard Report** – The report comes from an in-scope system but has not changed since implementation by the vendor (i.e., out of the box).
- **Third-party Report** – The report comes from a third-party application & covered by a SOC report.
- **Custom Report** – The report comes from an in-scope system but has been edited through the change management process.
- **Ad Hoc Report** – The report comes from an in-scope system but is generated through a SQL or data query.

Key reports require both management and the auditor to ensure the data is complete and accurate. From management's standpoint, their obligation is to ensure they are understanding what they are generating by retaining and inspecting the input parameters. The other main component for management is verifying the report was built following the company's change management process. When any key report is created or changed, it should go through user acceptance testing, which allows management to confirm the report is pulling the intended data completely and accurately for its anticipated use in the control.

Beyond the change management process, management should be designing their control review procedures to ensure they are checking the completeness and accuracy of each report they generate. As most management key reports are used in review controls, a common procedure for obtaining comfort over the completeness is tying the report out to the general ledger. For comfort over the accuracy of the report, management should be reviewing the details of the report and making sure they tie to source transactions. Management should also understand what controls create the transactions that populate their report to gain further comfort over the completeness and accuracy of the report.

Understanding and Assessing Management's IPE Controls

Before the auditor designs any independent testing procedures to validate a key report, the auditor should obtain an understanding of the design and effectiveness of management's IPE controls. This consideration includes four critical steps:

- Assess management's IPE controls for the completeness of the data utilized in the operation of the control
- Assess management's IPE controls for the accuracy of the data utilized in the operation of the control
- Develop testing attributes over the design and operating effectiveness of the IPE controls performed by management
- Evaluate whether the IT General Controls over systems utilized in the production of IPE have been tested and the results of that testing. If controls over IT General Controls are ineffective, additional considerations must be performed by the auditor. For example, the auditor may need to perform independent substantive testing procedures for completeness and accuracy.

Managing Key Report Risk

Once the auditor has assessed management's control, the auditor still may be required to perform additional testing procedures which should be coordinated with the external audit team to ensure the procedure are sufficient. The first step in determining additional procedures must first be to determine the type of key report used in the control.

Standard Reports – For standard reports, the report can be relied upon as complete and accurate without the need for additional testing procedures as management has never modified the data as long as the last change date is obtained and confirmed to be a standard report.

Third-party Reports – The SOC report should be obtained and reviewed for all in-scope third parties. While the report comes from a third party source system in which management cannot directly edit the data of the report, management should still perform procedures to inspect the input parameters and ensure the parameters match the intended purpose of the control.

Custom / Ad Hoc Reports – Each external audit firm has their own guidance on what procedures are required to gain sufficient comfort, but typical testing procedures to confirm the completeness and accuracy of a custom/ad-hoc report include:

- **Performance of the Control** – Most key reports used by management are utilized through a review control where management is inherently validating the completeness and accuracy of the data as a control objective and so the auditor can point to management's review if it is designed effectively to verify the report details (accuracy) and report totals (completeness).
- **Additional Samples** – The auditor will select samples from the report to trace back to source transactions (accuracy) and then select source transactions to trace into the report (completeness). This method can be very time consuming and should be looked at as a last resort to gain comfort.
- **SQL Inspection** – Some scripts are able to be documented in detail as to how the data is being extracted but SQLs can also become complex very quickly and so this method is less frequently relied upon. If management or the auditor is reviewing the script, keep in mind the most important sections are typically the SELECT, FROM and WHERE statements within the script. The SELECT section should directly tie to the column headers, the FROM section identifies the database tables that houses the data, and the WHERE statement is how the data can be filtered to only be included in the report if it fits a certain criterion.
- **Sample Transaction** – Depending on the situation, the auditor can work with management to process a transaction and observe how it then appears on the report. This is especially helpful when dealing with exception reports that only populate data when certain actions occur. This method is oftentimes performed through management's TEST environment and then the additional step of verifying PROD is a mirror of TEST is completed to show how the testing is applicable to the PROD environment.
- **Understand Compensating Controls** – Typically this method is not enough to gain completeness and accuracy comfort by itself, but when used in conjunction with other testing procedures, it can provide comfort over the data. This technique involves understanding the entire control universe and which controls provide comfort over the source transaction that your report is populating.

The testing methods do not have to be used individually either. Depending on the key report, performance of the control may be used to gain comfort over the completeness of the report, but a sample transaction could be used for the accuracy of the report. Regardless of which type is used, the auditor should always obtain input parameters or SQL screenshots to verify how the report was generated along with obtaining a screenshot to verify the report's last change date and who last edited the report.

Ultimately, the amount of testing required is at the discretion of the audit team performing the procedures, which is why it is so important to coordinate the testing approach with the external audit team.

Summary and Other Considerations

While identifying and documenting IPE can be complex, there are a few things both management and auditors can do in order to help reduce the risk associated with IPE.

Both management and the auditor should be creating an inventory of IPE used for key SOX controls. This should include the report name, report type, source system, key control, IPE vs. Population designation, etc. By creating this listing, it can help all parties budget and plan for the expected time it will take to assess each key report and help identify reports that may be used in more than one key control.

Once a key report has been verified as complete and accurate, as long as the report's last change date has not been modified or the script has not changed, the report can be benchmarked, which typically can last for 3-5 years depending on the risk associated with the data.

The most important consideration is making sure to coordinate between all parties. This includes management, internal audit and external audit. Conducting joint walkthroughs and agreeing on the inventory of key reports will help set the stage for the testing required each year on key reports.

About Schneider Downs Risk Advisory

Our team of experienced risk advisory professionals focus on collaborating with your organization to identify and effectively mitigate risks. Our goal is to understand not only the risks related to potential loss to the organization, but to drive solutions that add value to your organization and advise on opportunities to ensure minimal disruption to your business.

For more information, please contact our team at **contactsd@schneiderdowns.com** or visit **www.schneiderdowns.com/risk-advisory-services**.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

www.schneiderdowns.com

TAX
AUDIT AND ASSURANCE
CONSULTING
WEALTH MANAGEMENT

PITTSBURGH
One PPG Place
Suite 1700
Pittsburgh, PA 15222
P 412.261.3644

COLUMBUS
65 E. State Street
Suite 2000
Columbus, OH 43215
P 614.621.4060

METROPOLITAN WASHINGTON
1660 International Drive
Suite 600
McLean, VA 22102
P 571.380.9003