Testing the Reporting Process – Validating Critical Information

Abstract
The report testing process can be critical to providing management with the confidence necessary to rely upon the integrity of data housed in key financial applications. This white paper aims to provide a common working definition for report testing, explain why it is important, and offer useful guidance on how to scope and execute report testing. This paper addresses the following questions:
1) What is report testing?
2) Why is it important?
3) How is report testing scoped?
4) How is report testing conducted?
5) How often must companies conduct report testing?
6) How do companies operationalize the report testing process?

What Is Report Testing?
Reports are the basis for many processes used to manage and communicate results from business operations. In business today, the reporting process is often incredibly complex. It can include reports derived directly from information systems, custom reports developed from data warehouses, and reports based on spreadsheets that compile various system and manual inputs, among many others. Most key reports not only assist corporations in understanding pertinent financial information, but also are critical components of the control framework of the organization.

Knowing which reports support critical elements of the financial reporting process and determining their reliability is collectively referred to herein as “report testing,” a subset of the broader process of testing processes and controls.

When management identifies a report as a “key report” and uses it in the financial reporting process, it is making two key assertions, namely that the report is accurate and complete. (It is assumed throughout this white paper that the timeliness of the reports is sufficient for management’s reporting activity.)

Report testing is the process of assessing accuracy and completeness of key reports:
• **Accuracy** is a precise representation of source documentation on the report (i.e., items that appear on the report can be traced back to source documentation and confirmed).
Completeness is a comprehensive collection of intended data on the report (i.e., source documentation that should appear on the report, according to the reporting parameters, does, in fact, appear on the report).

Why Is Report Testing Important?

Report testing provides management the assurance it needs to rely on system-generated reports for key financial processes. For system-generated reports, report testing can be used to “baseline” newly created reports and establish reliance going forward.

Baselining a report means verifying it in terms of both the accuracy and completeness assertions, so that the report may be relied upon going forward as a critical process component. Assuming the existence of effective IT general controls processes (e.g., change management and security), a baselined report may only need to be tested periodically, rather than annually, for accuracy and completeness. In environments with strong general IT controls, report baselining is vitally important because the integrity of reports inherently relies on the system of internal controls.

This ongoing reliance is critical, as many key controls rely upon data from reports to satisfy the control requirements. External auditors typically request such evidence during Sarbanes-Oxley compliance procedures, preparation for corporate acquisitions or mergers, or as an input into determining the effectiveness of the overall control environment.

Imagine a scenario where a report has inaccurate information. Management uses it to make critical business decisions and then uses it to record entries in the company’s general ledger. The financial reporting not only is inaccurate, but the ramifications of those business decisions based on bad information can be substantial. Consider the questions below:

- How would you know a report is inaccurate?
- When the process begins to generate inaccurate and/or incomplete reports, how would you know?
- Given the complexity of reporting processes in place at companies today, how hard is it to imagine that a report could have an error?
- How many reports go through multiple input points (system and manual) before the final report is produced?
- How easy is it to relate the final report data to the information originally input into the system?

These often are difficult questions to answer. By their very nature, these questions underscore the importance of assessing the quality of reports to help ensure the accuracy and completeness of the data used to generate them.


The scope of the report testing used for Sarbanes-Oxley purposes should be based on an inventory of those reports used in the process of financial reporting. The easiest way to derive this inventory is to execute a two-step process, as defined below:

- Use a top-down approach to list reports relevant to financial reporting, starting with the general ledger. Evaluate each manual entry and work backward to determine which source
was used as the basis for the entry. Chances are there is a report somewhere that drives the entry.

- Use the bottom-up approach to supplement the top-down approach by working through the flow charts of the enterprise’s key business processes. For each key control in the business process, determine whether the operation of that control relies on a report.

By executing these two steps, management will have a complete inventory of the reports that should be considered in the report testing scope.

While determining the population of reports in scope, it is important to note how the operating effectiveness of the control environment can affect the scope of report testing. The scope of key financial reports for Sarbanes-Oxley purposes can be limited based upon the operating effectiveness of the general IT control environment, underlying business processes and user application control environments. Key financial reports within business processes that have design issues or have experienced breakdowns in operating effectiveness should be evaluated to determine if testing to source documentation could allow reliance at year-end for the control environment. While this may be a more lengthy and difficult process (as described in the manual testing section below), it may be the only option.

Additionally, further consideration should be given to each potential in-scope report to determine the criticality of the report to key financial processes. Criteria that should be considered in risk ranking the reports to determine criticality from a financial reporting standpoint include complexity, frequency of changes to the report, number of users relying on the report, severity of controls the report supports, and materiality of the transaction processing the report supports.

Criticality of the report can help align the level of rigor around the testing of the report. This means critical reports should be considered for more frequent testing or may be subject to larger sample sizes than reports of lower criticality.

**Conducting Report Testing**

Report testing can be broken into three distinct phases:

- **Phase I – Recalculation**
- **Phase II – Accuracy Testing**
- **Phase III – Completeness Testing**

Depending on the availability of data, these phases can take different forms, as discussed below.

**When electronic data is available**

- **Recalculation** – If IT can produce an electronic version of the report (i.e., the data output from the query that produced the report), automated tools (e.g., Access, Excel or ACL) can be used to recalculate the entire report very quickly. This gives 100 percent assurance on the operation of the query analytics.
- **Accuracy** – In terms of electronic data, this test is focused on testing whether the query pulled the appropriate data from the database. For instance, if the report is an accounts receivable aging report, can the auditor independently verify that the data on the report accurately reflects the data in the database? Again, the population can be tested completely by executing similar queries against the population and comparing the result to the report tested.
Completeness – Since the step above uses the electronic population and is able to achieve testing of 100 percent of the population, the act of testing accuracy also satisfies the completeness test.

There often is discussion around whether the data should be tested back to source documents versus using the database. The answer is that it depends on the quality of the control environment. However, in most organizations, many other controls in upstream processes already have been tested to provide assurance that data was collected and entered into the system appropriately. These controls, and the testing that validates their effectiveness, should be considered.

When electronic data is either not available or cannot be used
While the preferred method is to receive the data electronically and execute full testing using automated means, there are instances when – due to the complexity of the environment or the state of controls – the electronic data cannot be considered reliable. Examples of these instances include:

- Reports are generated from multiple or complex queries from multiple databases.
- Change controls and security controls are deemed ineffective for the systems that house the data.
- Change controls and security controls are deemed ineffective for the systems that process the transactions that feed the database.
- Process controls governing the business processes that feed the database are deemed ineffective.

These circumstances are serious. When they occur, the testing process must trace data from the report to the source documentation. As full testing in this type of scenario will not be feasible, a sampling approach should be used. The following sampling approach for testing the operational effectiveness of key financial reports provides management with reasonable assurance that the reports are reliable.

Sampling Approach
When sampling is deployed, the sample size should be determined by the number of line items in the report. (The sample sizes below assume an error rate of zero.) Based on the sample size, an equal sample of data will be both traced and vouched for source and system validation.

Example Sampling Table

<table>
<thead>
<tr>
<th></th>
<th>Line Items Less than 100</th>
<th>Line Items 100 and Greater</th>
</tr>
</thead>
<tbody>
<tr>
<td>Testing</td>
<td>16 records</td>
<td>30 records</td>
</tr>
<tr>
<td>Accuracy</td>
<td>8 records</td>
<td>15 records</td>
</tr>
<tr>
<td>Completeness</td>
<td>8 records</td>
<td>15 records</td>
</tr>
</tbody>
</table>

Testing Approaches

- Recalculation – For most reports, recalculating the entire surface of the report manually is not practical. Depending on the report, recalculation can be conducted on portions of the report or by summing the various hash totals to the report total. A risk basis should be used to determine how much of the report should be recalculated. This helps to ensure that any functionality within the report or reporting package that does calculations is performing as intended. In those instances where it is not feasible to recalculate subtotals manually (e.g.,
the number of line items is too great) or in instances when there are no subtotals to recalculate the grand total, management should determine a feasible solution on a case-by-case basis. The sampling approach for these instances can be documented within the testing documentation. Business management must identify key values within the report that are critical to the financial process. All key financial totals should be recalculated by summing the values that comprise the totals.

- **Accuracy Testing** – This testing involves “back-tracing” of sample transactions through re-performance testing from the report to source data. Using the example sampling guidance provided above, the appropriate number of records can be selected from the report and vouched to source data. Note that going back to the original hard copy or paper source for a record on a report may not be required unless the controls over entry of the data are deemed ineffective. There are likely other controls in place that help provide governance over the receiving and input of paper documentation into application processes. This source is the originating application data being pulled to appear on the report. Validating that the sampled transactions appearing on a report can be sourced to the appropriate data elements instills confidence that the report is displaying accurate information to the end user.

- **Completeness Testing** – This testing involves “forward-tracing” sample transactions from source data to the report. Using the example sampling guidance noted above, the appropriate number of records can be selected from source data (e.g., invoices) and traced to the records on the report. Again, the source is the originating application data that is being pulled to appear on the report. Validating that sampled data elements that should be appearing on a report are, in fact, appearing on the report being tested provides confidence the report is displaying a complete set of information to the end user.

**Other Key Points**

- When testing summary-level reports, a detailed report can be tested and tied back to the summary report.
- Management may use successfully tested reports to support its conclusion of the operational effectiveness of the financial reports provided. When a successfully tested report is used, evidence can be provided in the future to support the underlying premise that no changes have been made.

**How Often Must Companies Conduct Report Testing?**

Assuming the controls that feed the database are operating effectively, and the controls governing the database and reporting also are operating effectively, reports should only need to be tested every three to five years unless other changes take place in the environment. The exact frequency should be based on the risk ranking of the individual reports.

**How Do Companies Operationalize the Report Testing Process?**

Companies are continually missing a prime opportunity to baseline their reports as part of their normal operating procedures. If done appropriately, this practice completely alleviates the need for separate testing of individual reports. The steps are relatively simple and already may have been done in the organization.
For example, when applications are tested, upgraded or implemented, the existing systems development lifecycle processes already require that a certain level of testing and documentation be performed. If the testing and documentation processes were designed to ensure the test cases covered the three requirements of report testing – recalculation, accuracy and completeness – and capture the evidence of the testing sufficiently to provide a trail for audit purposes, the report could be “baselined” effectively before it is put into production.

As with electronic testing, this approach assumes that controls exist and are operating effectively around change management and security matters, including segregation between the ability to develop changes and promote them to production.

**A Critical Business Process**

Confirming the accuracy and validity of reports by testing the data supporting it should be a critical business process for organizations today. Even seemingly minor errors can cascade quickly into major ones, leading to noncompliance with laws and regulations and inaccurate financial reporting. By implementing a formal reporting testing process, management can be confident in the integrity of the data in its key financial applications and in the reports generated from this data.
About Protiviti

Protiviti (www.protiviti.com) is a global business consulting and internal audit firm composed of experts specializing in risk, advisory and transaction services. We help solve problems in finance and transactions, operations, technology, litigation, governance, risk, and compliance. Our highly trained, results-oriented professionals provide a unique perspective on a wide range of critical business issues for clients in the Americas, Asia-Pacific, Europe and the Middle East.

Protiviti has more than 60 locations worldwide and is a wholly owned subsidiary of Robert Half International Inc. (NYSE symbol: RHI). Founded in 1948, Robert Half International is a member of the S&P 500 index.

About Our IT Internal Audit Services

Protiviti’s IT internal audit services help organizations understand their key technology risks and how well they are mitigating and controlling those risks. We also provide insight into the threats inherent in today’s highly complex technologies. Protiviti provides a wide range of services for IT internal audit outsourcing and co-sourcing. The Protiviti methodology, which is both COSO- and CobIT-based, facilitates an overall IT internal audit management team (either Protiviti-led, client-led, or in combination) with execution of individual projects by subject-matter experts in each IT audit area.

Contacts

David Brand
+1.312.476.6401
david.brand@protiviti.com

Gordon Braun
+1.913.661.7406
gordon.braun@protiviti.com