A tour of HP Sarbanes-Oxley IT assessment accelerator

White paper

Table of Contents

Sarbanes-Oxley is a US Government legislation that requires corporate management, executives, and the financial officers of public companies to certify their company's financial statements and to attest to both their responsibility for and the effectiveness of internal controls over financial reporting. Penalties for non-compliance are severe, including fines as well as personal liability on these executives that can ultimately result in jail sentences.

To assist customers with Sarbanes-Oxley compliance, HP has produced a number of Sarbanes-Oxley accelerators that work with our Business Technology Optimization (BTO) solutions and allow customers to more easily and efficiently achieve Sarbanes-Oxley compliance. HP Sarbanes-Oxley IT Assessment Accelerator provides pre-defined content based on the IT Governance Institute's (ITGI) Control Objectives for IT (COBIT) for HP Quality Center software, and ease the testing required to validate Sarbanes-Oxley compliance. This paper describes that accelerator and discusses its implementation.

Introduction

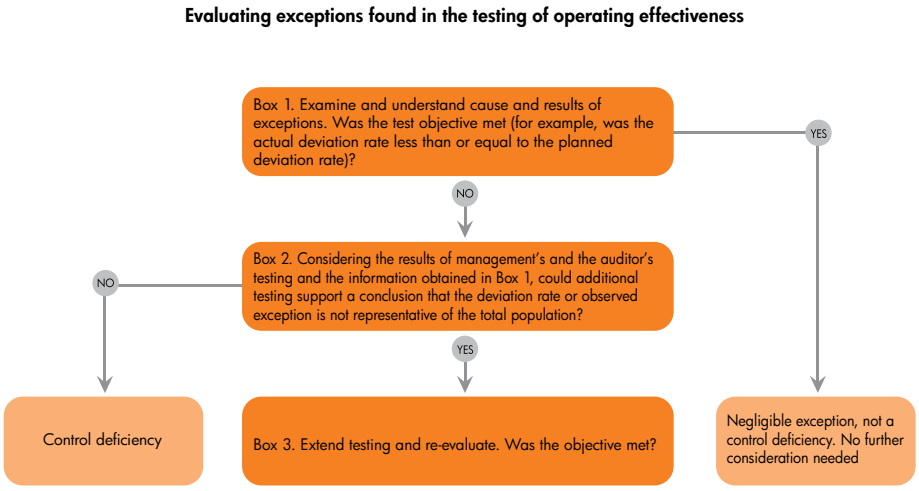
Although Sarbanes-Oxley is a finance-driven initiative, IT plays an integral part given the fact that IT systems support financial processes. As such, these two groups need to work together under tight deadlines to meet compliance goals. Sarbanes-Oxley compliance is an ongoing, evolving effort, impacting both finance and IT, which will cost organizations millions every year. You need automated solutions to meet compliance requirements, to make compliance processes repeatable and more collaborative, and to reduce the costs associated with compliance.

HP Quality Center helps optimize and automate key quality activities. For Sarbanes-Oxley compliance, HP Quality Center, HP Business Process Testing software, and HP QuickTest Professional software (when automation is needed) can help you:

- Define and document requirements for testing controls
- Manage and track defects and map back to the controls
- Test new and existing applications being deployed/updated/migrated that impact financial processes and ensure functionality with every assessment
- Track test results and map to test requirements through traceability
- Automatically generate complete audit trails of testing activities along with reports
- Test security controls

This white paper describes HP Sarbanes-Oxley IT Assessment Accelerator, a template of pre-defined information based on ITGI's COBIT, which is loaded into HP Quality Center to help your organization define and execute Sarbanes-Oxley testing, evaluate the results, and develop remediation plans.

Figure 1: From a framework for evaluating control exceptions and deficiencies, Version 3, December 20, 2004



Note: Individual boxes should be read in conjunction with the corresponding guiding principles.

Sarbanes-Oxley and the ITGC Environment

Sarbanes-Oxley requires management to base its assessment of the effectiveness of the company's internal control over financial reporting on a suitable and recognizable framework that has been established by a body of experts. IT management has adopted the framework presented by ITGI's COBIT.

The COBIT framework provides a tool for providing adequate controls. The framework is a set of 34 high-level processes, one for each IT process, grouped into four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring.

By addressing these 34 high-level control objectives, you can provide an adequate control system for the IT environment. The COBIT framework has been limited to high-level control objectives in the form of a business need within a particular IT process. The control of IT processes that satisfy business requirements is enabled by control statements considering control practices.

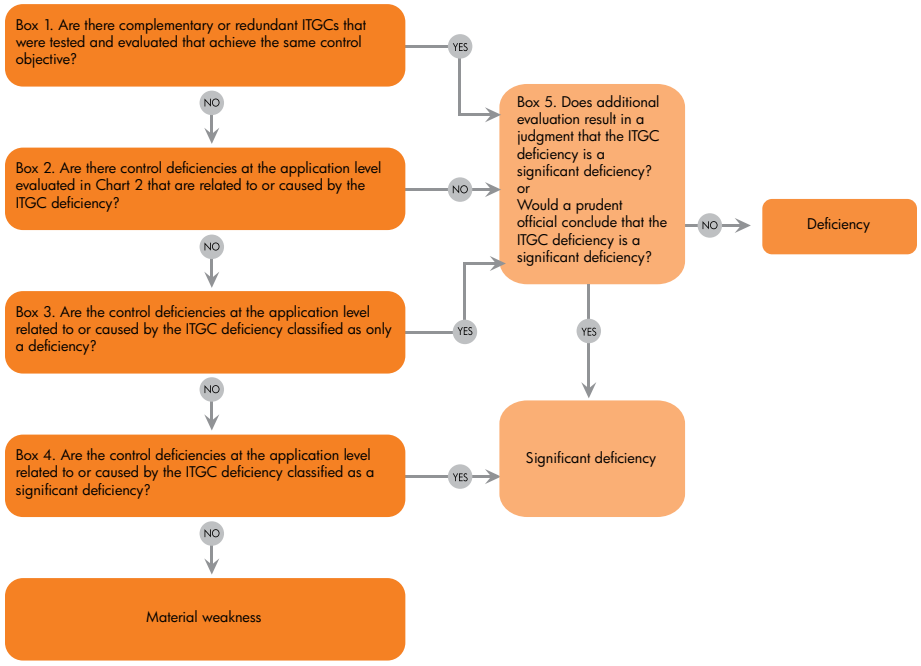
COBIT framework of ITGC

To ensure that management reaches its business objectives, IT must direct and manage IT activities to reach an effective balance between managing risks and realizing benefits. To accomplish this, you must identify the most important activities to be performed, measure progress toward achieving goals, and determine how well the IT processes are performing.

Figure 2: From a framework for evaluating control exceptions and deficiencies, Version 3, December 20, 2004

Evaluating ITGC deficiencies
This decision tree is to be used for evaluating the classification of ITGC deficiencies from the following sources:

- ITGC design effectiveness evaluation
- ITGC operating effectiveness testing (from Chart 1)
- ITGC design or operating deficiencies identified as a result of application control testing (from Chart 2)



Note: Individual boxes should be read in conjunction with the corresponding guiding principles.

Control is defined as the policies, procedures, practices, and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

- **Domain:** A natural grouping of processes often matching an organizational domain of responsibility
- **Process:** A series of joined activities with natural control breaks
- **Control objective:** A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity
- **Control activity:** The policies, procedures, practices, and organizational structures designed to provide reasonable assurance that control objectives will be achieved and that undesired events will be prevented or detected and corrected. Control activities need to be defined so they can be tested

Creating a compliance testing process

In creating a compliance testing process, you should create a process with six discrete steps:

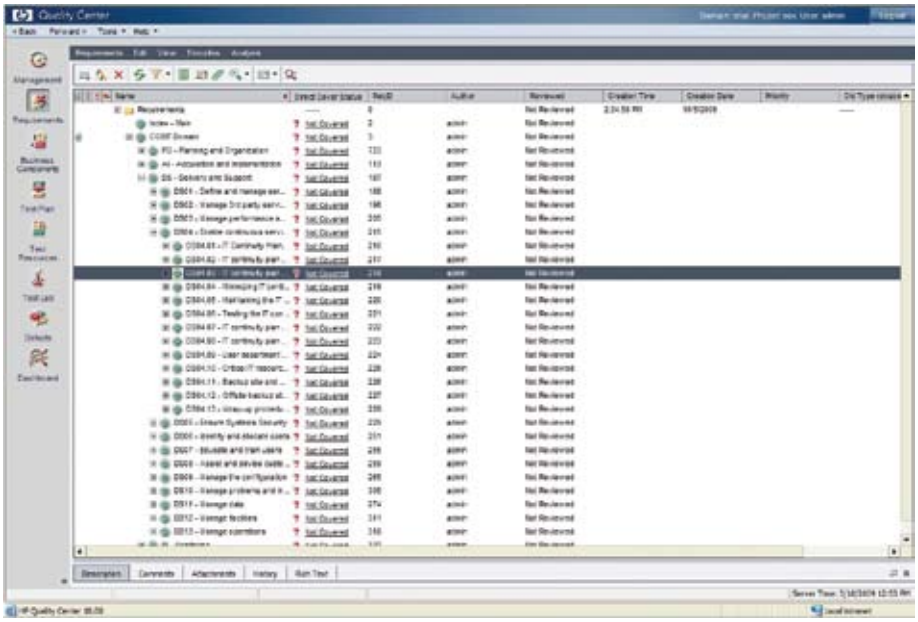
Step 1: Define control environment

In this step, you define the ITGC activities as required by your company's business operations. Each ITGC activity is given a set of attributes, such as control frequency (weekly, daily, or yearly), whether the control test is executed manually or automated, and the number of items to test.

Step 2: Define testing plan

During test planning, you determine the test objective. You also set the allowable deviation rate of the test, used during result evaluation to determine whether or not the objective being tested has, in fact, been met. You translate ITGC activities into specific test steps and document the expected results.

Figure 3: Requirements hierarchy



Step 3: Define test execution
After you have planned the tests, you must lay out the specifics of their execution. In this step, you determine the period under test (for example, Q3 of this year), and the number of test runs required to achieve the minimum sample size. Finally, you lay out the details of the actual execution, such as execution time, tester's name, and so on.

Step 4: Execute testing
Next, you execute the tests. You select samples from the pre-defined population, based upon the period being tested, and then observe and record the results of the tests.

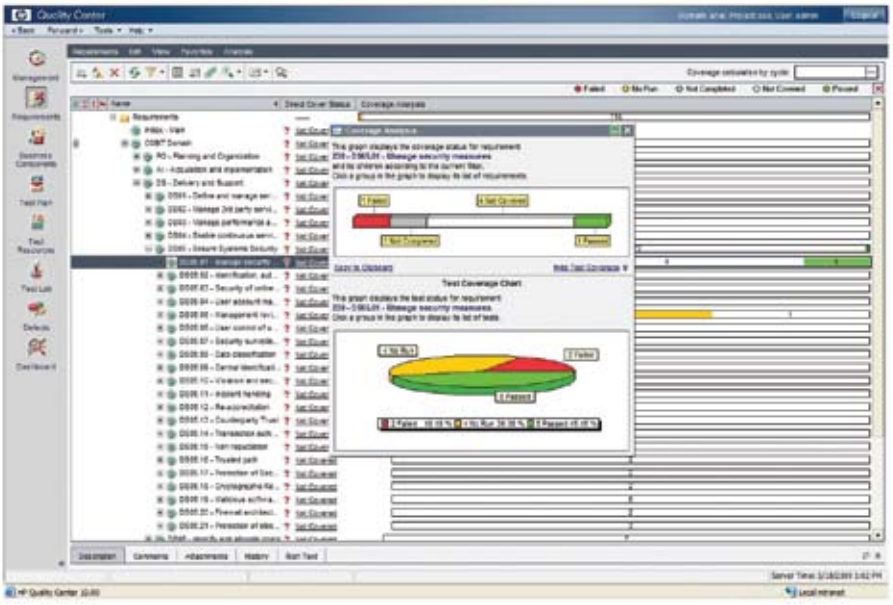
Step 5: Evaluate results and develop remediation plan
Following execution, you evaluate the results. Figure 1, a part of COBIT, helps you determine whether or not the test objective was met. Looking at factors such as the deviation rate and existence of exceptions, you determine whether or not a control deficiency exists. If so, you create a remediation plan. This plan covers items such as new policies and procedure, or additional education and training of relevant individuals.

Step 6: Perform final evaluation
Finally, you re-test and re-evaluate those items covered by remediation (as in Step 5). For items that are still deficient, you evaluate the severity of the deficiency, as shown in Figure 2.

How HP Quality Center supports compliance testing

HP Quality Center is ideally suited to support the process outlined above. HP Quality Center, HP QuickTest Professional, and HP Business Process Testing combine to help your organization determine compliance.

Figure 4: Coverage analysis



HP Sarbanes-Oxley IT Assessment Accelerator provides complete coverage of Sarbanes-Oxley requirements through pre-packaged, detailed test plans for the four COBIT domains, comprising the complete set of more than 320 requirements. These are mapped to Sarbanes-Oxley domains and section numbers.

With HP Sarbanes-Oxley IT Assessment Accelerator, you can achieve testing remediation and visibility with traceability from requirements to defects. Traceability from requirements to defects also helps you understand remediation needs and ensures complete coverage of all requirements.

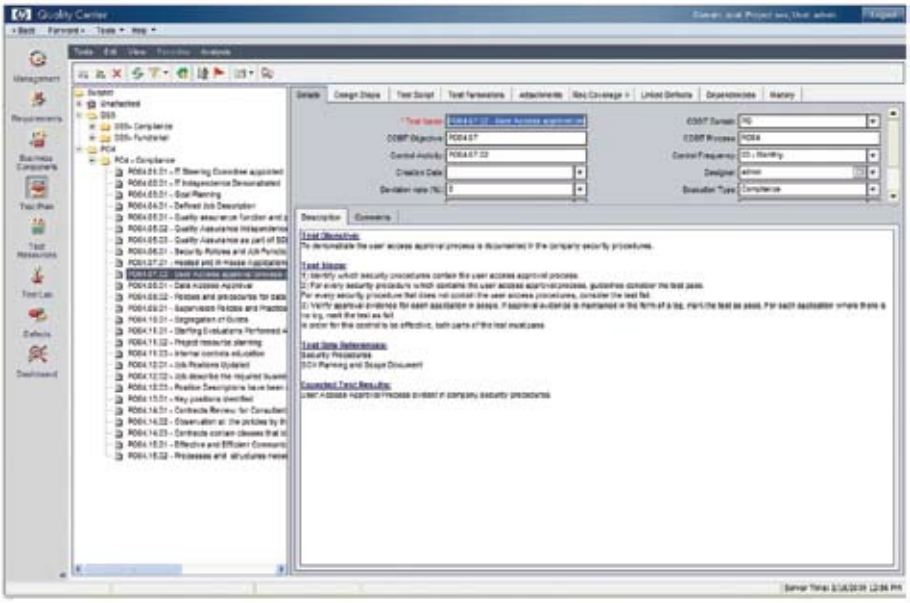
The next several sections of this white paper describe the structure of the data contained in the HP Sarbanes-Oxley IT Assessment Accelerator.

Pre-defined COBIT Requirements

HP Sarbanes-Oxley IT Assessment Accelerator defines nearly 400 requirements covering four COBIT domains, including planning and organizations, acquisition and implementation, delivery and support, and monitoring. Figure 3 displays the structure of the requirements, as viewed in HP Quality Center Requirement Management module. The indented tree structure shows each COBIT domain, such as "planning and organization," at the highest level, followed by the individual processes and their descriptions. At the lowest level of the hierarchy, the control activity is shown, along with its attributes.

HP Quality Center's reports and graphs are used to track the status of these COBIT-based requirements. For example, using the standard Coverage Analysis view, shown in Figure 4, you can see and evaluate current status of compliance testing. This gives users an easy-to-digest view of the status of Sarbanes-Oxley compliance testing.

Figure 5: Test planning



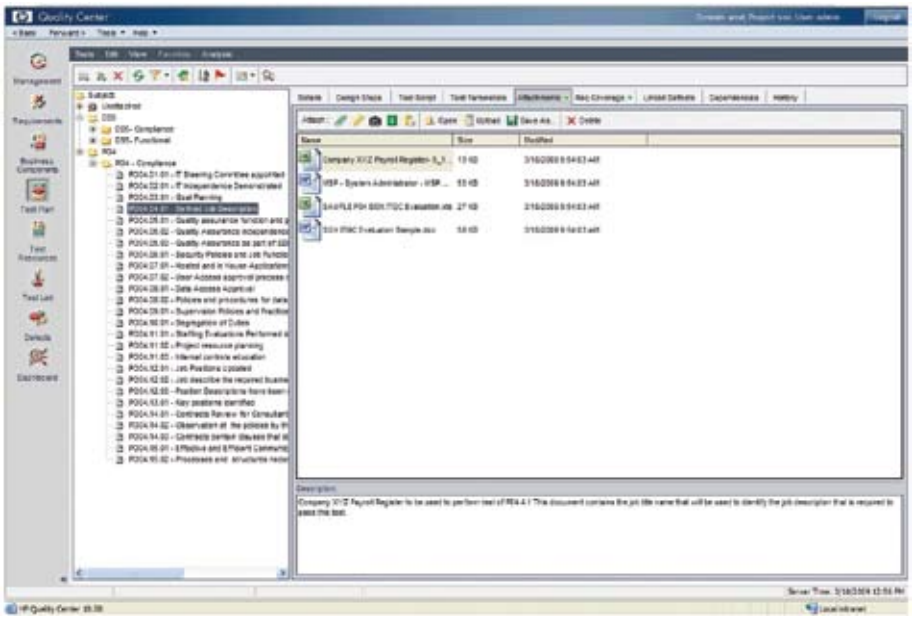
Test planning

The provided content in the test planning modules contains examples of both compliance and functional testing. Compliance testing checks for the existence and operation of various business process, such as the documentation of job descriptions or the existence of steering committees. Compliance tests are always performed manually, as they do not depend on the operation of an IT application. Functional tests check the operation of IT applications and can be automated using the HP functional testing tools, such as HP QuickTest Professional or HP Business Process Testing. All of the example tests provided in the accelerator are manual.

As with requirements, HP Sarbanes-Oxley IT Assessment Accelerator provides you with a head start, using the COBIT structure as a guide. In this case, 149 tests have been written, covering both compliance and functional testing. Using the tree structure in HP Quality Center, the COBIT structure modeled in the requirements is maintained. In addition, user-defined fields have been added to the definition of tests to hold COBIT testing guidelines. As shown in Figure 5, those fields are:

- COBIT domain
- COBIT process
- **Control frequency:** How often the control activity is performed to meet the control objective
- **Planned deviation rate:** Allowance for error
- **Execution type:** Compliance, functional, or both
- **Sample size:** The number of tests to be completed based on the control frequency
- **Tested application:** Application or system name, if applicable
- **Population:** A specific and identifiable grouping from which the tester chooses an incident or sample from which to test. The population must refer to a specific set of values, in a selected timeframe

Figure 6: Attachments to test PO4.4.1



Because tests can be combined into various test sets in HP Quality Center's Test Lab, you can perform the specific implementation of the various control activities on an application-by-application basis.

One example test, PO4.4.1, is used to show additional capabilities of HP Quality Center that you can use during Sarbanes-Oxley testing. As shown in Figure 6, several attachments have been added to the test, including examples of the information required to satisfy this compliance test and example evaluation forms. These forms are discussed below, in the section of evaluating test results.

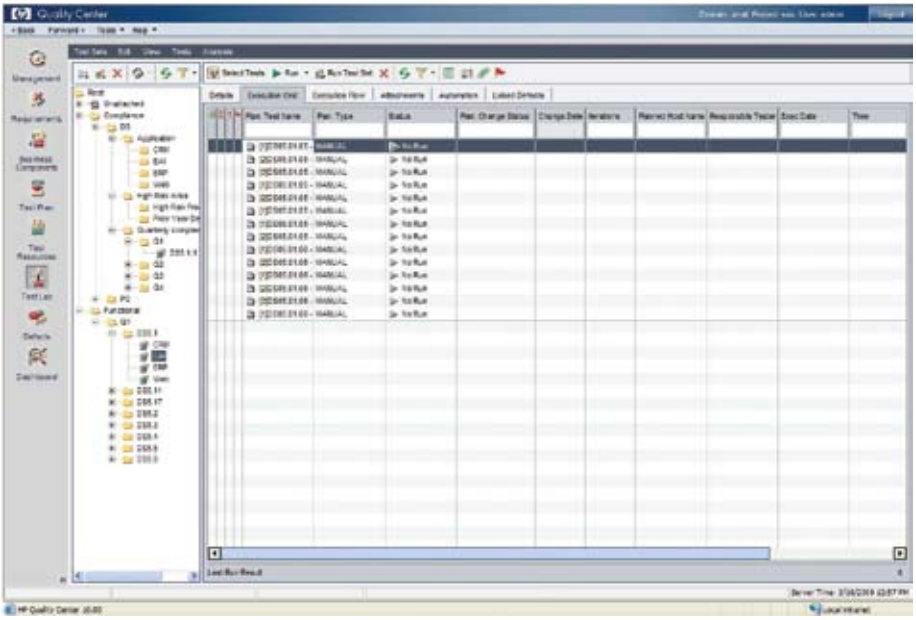
Executing testing

Once test planning is complete, you can begin test execution. HP Sarbanes-Oxley IT Assessment Accelerator provides an example test lab hierarchy, and a small number of example test sets. Again, these examples cover both compliance and functional testing. Figure 7 shows one of these examples.

For the compliance test set example, COBIT's concept of sample size has been used to define the number of times the test must be run. Sample size is defined as a function of the testing frequency. The exact number of tests in each sample size should be aligned with your audit organization's guidelines.

As with requirements, you can create user-defined fields to track the testing guidelines. And, as with all HP Quality Center testing, each instance of a test run is logged, along with its results, including the date and time the test was executed, and the identity of the tester. This data can be aggregated onto a standard or customized HP Quality Center report, and leveraged during the compliance auditing activities.

Figure 7: Test execution



Evaluating test results and developing remediation plan
After test execution, you can inspect test results and make decisions regarding remediation. HP Sarbanes-Oxley IT Assessment Accelerator provides reports that compare the results of testing against the allowable deviation, highlighting areas that require remediation. See Figure 8 for an example of this report. Based on these reports, you determine whether or not remediation is required.

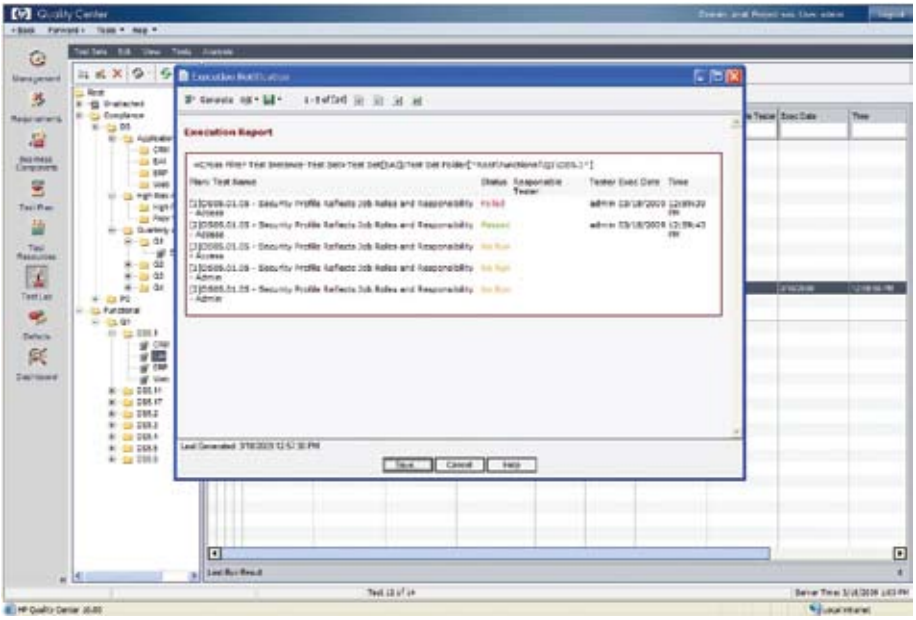
Using the types of coverage graphs shown in Figure 4, you can easily determine the status of compliance testing as it relates to the COBIT objectives and activities. Beyond coverage, you can perform detailed defect analysis, again using standard and customized HP Quality Center graphs and reports, to help determine compliance.

To help with this determination, a worksheet has been attached to Test PO4.4.1. Based on the COBIT decision tree shown in Figure 1, this worksheet provides a method to track all the objectives that have not passed testing. Based on this worksheet, you can create a detailed remediation plan, confident that you have captured all the failed testing and associated control objectives.

To help with remediation tracking, HP Sarbanes-Oxley IT Assessment Accelerator has defined a COBIT defect type. For each objective requiring remediation, you should create a new defect and take it through its lifecycle. Once remediation is complete, re-testing is required, as discussed in the next section.

Remediation and re-testing
Remediation takes place outside of HP Quality Center. However, you should record the effort taken to remediate the identified problem in HP Quality Center, generally against the defect identifying the deficiency.

Figure 8: Test set report



Once remediation has taken place, you must re-test those objectives. As before, test execution takes place and the results are analyzed. Again, you should use the decision tree shown in Figure 1 to evaluate the results. This time, however, if a deficiency still exists, you should use the decision tree shown in Figure 2 to determine the severity of the deficiency. Both decision trees have been captured in the worksheet attached to PO4.4.1. Also as before, you can use the COBIT defect type to track this deficiency; however, this time you should also use the fields found on the "evaluation" tab.

The final evaluation

Similar to the evaluation performed above, you can use HP Quality Center reporting on defects and test status to make a final evaluation of the state of compliance testing. You can then pass this final evaluation along to compliance auditors as determined by your organization's controlling bodies.

Conclusion

This white paper has provided a tour of the HP Sarbanes-Oxley IT Assessment Accelerator. Using the process and tools outlined above, your organization can ease and accelerate compliance testing.

Technology for better business outcomes

To learn more, visit www.hp.com/go/quality

4AA2-5347ENW, April 2009