IT Process Conformance Measurement: A Sarbanes-Oxley Requirement

Rafik Ouanouki[1], Dr. Alain April[2]

[1] RONA, Quality Assurance, 220 Chemin du Tremblay,
Boucherville, Québec, Canada
rafik.ouanouki@rona.ca
[2] École de Technologie Supérieure, 1100 rue Notre-Dame Ouest,
Montréal, Québec, Canada
alain.april@etsmtl.ca

Abstract. In 2006, the most important Canadian distributor and retailer of hardware products was faced with formalizing its internal processes in response to the requirements of the Sarbanes-Oxley Act. This publication is a follow-up information to our first paper on process conformance and audits [7]. The software testing process and how conformance to the documented process was achieved within 3 months is described. This research paper presents an introduction, the testing process itself, the process conformance measurement and the results obtained during the first three months of measurement.

Keywords: Quality Assurance, Testing Process, Process Conformance, Conformance Measurement, and Quality Audit

1 Introduction

At the end of 2001, financial fraud and misconduct in the United States sowed doubts as to the integrity of the financial markets. The side effects of these scandals were felt throughout the world's financial markets. Since then, regulating bodies and governments have endeavored to restore the confidence of investors, their efforts being related mainly to reinforcing the means of communication of information and the quality of the verification processes of public companies.

The Sarbanes-Oxley Act, and its equivalent in Canada named Bill C-198 [1], was adopted with the objective of enhancing internal control with respect to the financial information of all publicly traded companies. Today, many Canadian companies are aware that they have to respect the requirements of Bill C-198; however, some of them have not yet understood the precise obligations, how to interpret the law, how to set up a suitable control system and the associated procedures for the communication

of information to respect the requirements imposed by recent changes to the law regarding civil liability. As a result, any company which is publicly traded is obliged to comply with the regulations set out in the bill, and must document its processes and internal controls (including its IT processes).

For the Information Technology (IT) department this means documenting IT processes and controls surrounding the financial systems. Internal auditors use the Control Objectives for Information and related Technology (CobiT) [2] framework to implement Bill C-198 in the IT processes. Theoretically, conformance is a rather simple issue and management typically plans a year to meet the requirements of Bill C-198; however, in this specific organization, process documentation was incomplete and missing. Also employees were executing a personal process. For the particular company we helped, we started to document the existing software development life-cycle processes using process models from international standards like ISO12207 [3] and the Software Engineering Body of Knowledge (SWEBOK) [4]. The resulting enhanced process documentation was placed on an Intranet which helped with the communication and training. Senior management supported the initiative and internal auditors also helped by conducting audits and reviews of the new processes to assess the completeness of the internal controls.

Our process improvement team opted to describe the current software development life-cycle activities, as done by the IT employees, and progressively harmonize the differences between the five IT sections. This was done using an iterative experimental process, where we conducted:

- The analysis of the existing documentation;
- Work session with the representatives of each of the five IT sections to describe their software development process, roles and responsibilities, activities and deliverables;
- Harmonization of the differences between the many roles, activities and deliverables;
- Review the existing controls and the new requirements of Bill C-198 with the internal auditors;
- Create and publish the new process maps on the new Intranet for experimentation;
- Knowledge transfer on the new roles, process and deliverables.

This experimental approach created little employee resistance as employees had to assess if the process description reflected well the actual activities they carry daily.

The resulting four IT life cycles all call on a testing process in their stage 3 (refer to Figure 1). It is that testing process that we will use to describe how the Bill C-198 conformance was achieved for this organization.

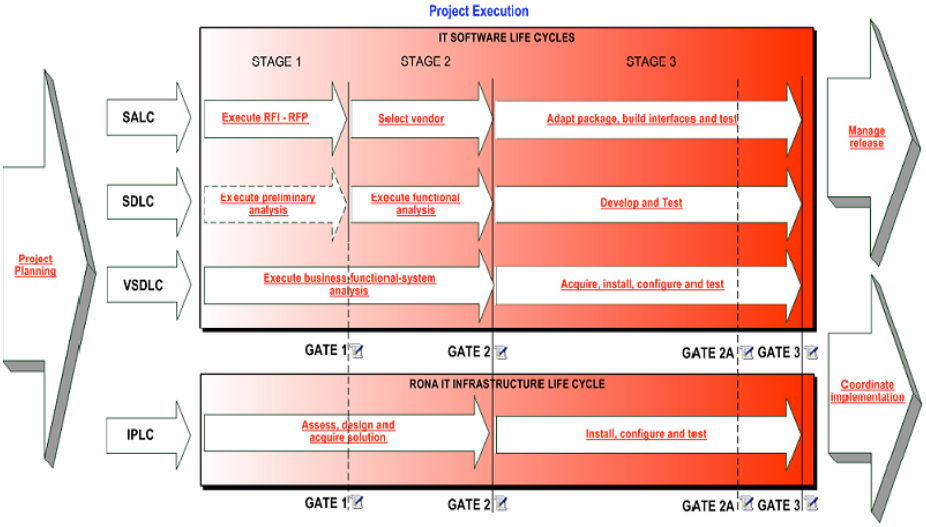


Fig. 1. Overview of the IT software life cycles. Resulting four life cycles of the IT division. The first is a software acquisition life cycle (SALC). The second is a Software development life cycle (SDLC). The third is a Vendor software development life cycle (VSDLC). The fourth is an Infrastructure project life cycle (IPLC). Each life cycle calls a test process in their stage 3

1.1 The Testing Process

No readily available testing process can be found in the literature. Each company has to create its own. Using industry standards such as the SWEBOK [4], the Certified Software Test Analyst Body of Knowledge (CSTA) [5] and Daniel Galin's book on Software Quality Assurance [6] we documented a theoretical software test process for this organization. The process is summarized as follows: The typical execution of software testing follows four successive stages (also called levels): 1. Unit tests; 2. Integration tests; 3. System tests; and 4. Acceptance tests. This is often described as "different levels of testing" in the software engineering standards. In order to simplify the testing process, it was decided that one test plan would be used to record the results for each test level.

We documented the proposed software test process in three steps: 1. Prepare Test, 2. Execute Test and 3. Analyze test Results. Step one and two can be viewed in figure 7 and step three in figure8. This three-step process describes all the detailed activities and controls associated with a specific test plan. Many test plans templates existed in this company. We tried to harmonize all the differences into one. This resulting template was created using an Excel spreadsheet and contains the following information: History section, test planning details, test cases and test results and approvals.

Process integration is strongly based on the proposed use of this template. Supporting documentation, proof of execution as well as the names of the people who prepared the tests, carried them out and even approved them, are mentioned in the test plan. Each section of the test plan template has mandatory fields. Filling in all the mandatory fields constitutes the minimum condition for conforming to the Bill C-198. Before describing how the conformity of a software testing process is measured, we must explain the three steps of the test process. Figures 2 and 3 describe the activities, while a summary of their content is presented in the next sections.

1.2 Prepare Test

The 'Prepare Test' process is the first step of an IT test. It is initiated when a test organizer prepares the test plan by performing two activities:

1. Update the version changes log, which is used to keep a record of individual changes to a specific test plan;
2. Prepare the test plan: Using a test plan template, where there are many data items that have been identified as mandatory fields; for example, the project name, the change request number and the planned test levels.

In software development there are many types of tests that take place before the product can be promoted to a production status. The four types of tests are:

1. Unit testing: is a process used to validate that an individual unit of software working properly. A unit is the smallest testable part of a software application;
2. Integration testing: is a process in which individual software units are combined and tested as a group;
3. System testing: is a process on a complete, integrated system to test the system's compliance with its specified requirements;
4. User Acceptance testing: is one of the final tests of a software that occurs before a client or customer accepts the software.

In preparing the test plan, the organizer must:

- Define testing roles: for example, some unit testing activities may not require an independent test approver. Integration and user tests, where the Bill C-198 auditor requires independent signatures on the test acceptance results;
- Identify whether or not the information system (IS) to be tested is listed as a critical Bill C-198 system (4);
- Identify test cases, which will be designed and executed at a later stage. Designing test cases will require access to functional requirements (5);
- Identify the physical environment where the tests will be executed (i.e. CobiT states that IT tests can be executed in the development environment or the test environment, but not in the real production environment). The process indicates clearly that, if there is no separate testing environment, a manager must be consulted in order to decide on the options (6);
- Identify the conditions of entry and exit of the tests. This activity requires that a specification of test success/failure be described before preparing and executing test cases.

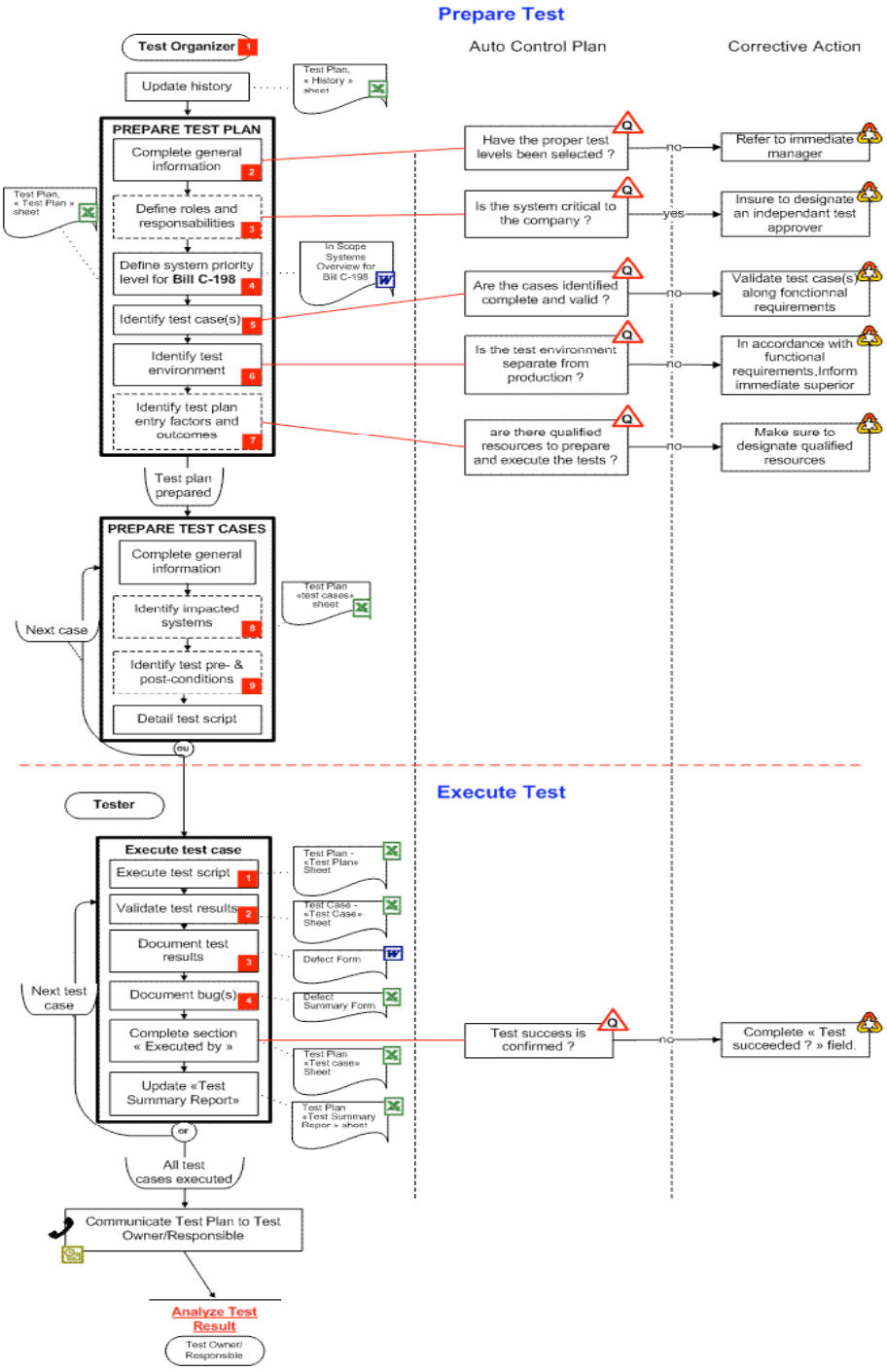


Fig. 2. Process map of the first and second step of a software testing process, which is named Prepare test. Activities are represented in the left column. Ruling C-198 controls are derived from CobiT and located in the auto control plan column. Corrective actions are documented in the right column

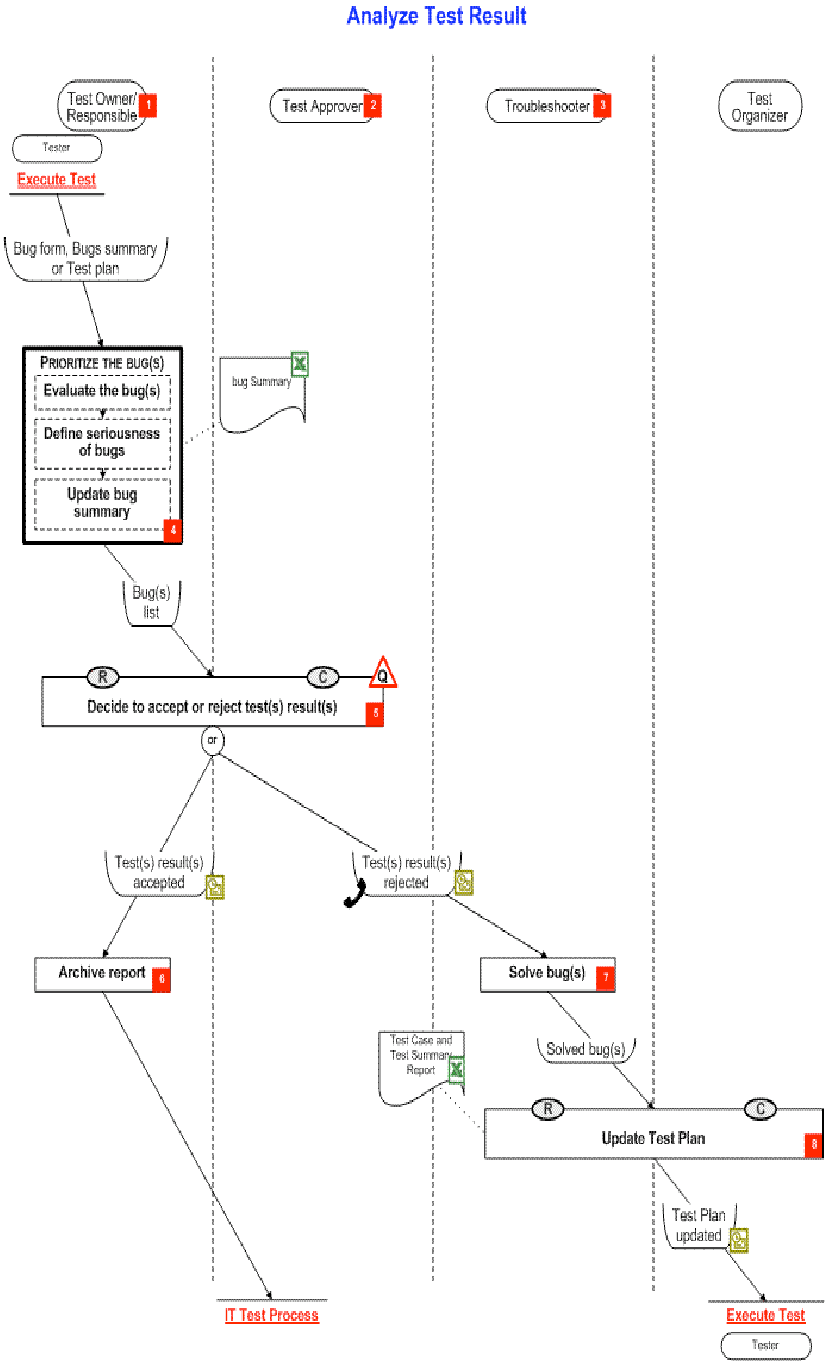


Fig. 3. Process map of the third step of a software testing process, which is named Analyze test results. Based on the list and severity of the bugs the test owner and the test approver must decide and document if the tests are conclusive or if changes are required.

Once this series of activities has been carried out, we consider that the test planning process has been executed. Once this has been approved internally, the test organizer is ready to design the many test cases that have been identified in the plan.

There is a section in the test plan template to help document the test cases, which is often referred to as the test script. Each test case will need to be described, explaining its pre-condition (how to set up the system before conducting the test), what entry to give the system and the post-conditions (explain the expected results of the system after test execution). To satisfy the C-198 internal auditor's recommendation in each test case, two identification fields are mandatory, the first for the person who prepares the test case and the second for the person who executes the test case. Once these activities have been completed, the software test case step can be executed.

1.3 Execute Test Case

The second step of the software testing process deals with the execution of the test cases identified in the test plan (1). The tester begins with the execution of each item in the test script in order to validate the results (2) of the tests (whether or not they were successful); then, each defect is documented (3) in a bug report.

There may be many bugs, and another form is needed to provide a list of those defects (4). It is critical that the person who documents the defect information update the test plan section in which the individual who has carried out the tests is mentioned and that he or she state whether the test has passed or failed.

This activity is considered completed once all the test scripts have been executed and a summary report of the test plan template filled in.

Once these activities have been performed, the software test results can be analyzed and a decision made on what action should be taken next.

1.4 Analyze Test Results

There are many individual roles involved in analyzing the test results. Each must perform a specific task to analyze the results of the tests (as shown in Figure 8).

The individual in charge of the tests begins by reviewing each defect in order of its importance (4) and decides, with the test approver, whether or not the test results meet their exit requirements. For example, in a final acceptance, the results of the tests would be reviewed with the user.

If the tests are accepted, an approval email needs to document this decision. The person in charge of the tests will file this approval email later. It should be noted here that approval constitutes a very important control in terms of the C-198 requirements.

If the results of the tests are rejected, the test owner records the decision in the test plan, which is then transmitted to the project team to correct the defects; once the defects are corrected, the test plan is updated and transmitted again to undergo another test cycle. Once these activities have been completed, the conformance of an individual test plan can be measured against the C-198 criteria.

2 Process Conformance Measurement

2.1 How can the C-198 conformance of the testing process be verified?

A conformance assessment needs to be a formal process, so that it can be explained in detail to the personnel who are conducting the testing. Quality assurance analysts will have the independent task of assessing how project teams conform to the organizational process.

This process is initiated when a project sends a production release email to the change manager. Before the project can move to production, there must be a verification of the project quality records, including the tests. If defects are found, the project team needs to correct them before permission is granted to move to production status.

To keep this process agile, urgent production fixes are treated in order of priority, and can be promoted to production first and the quality records can be adjusted.

To assess test plan conformity, the quality assurance analyst inspects two documents: the test plan and its approval. The latter can take various forms, but the email remains the favored method because it is easily filed with the corresponding test plan, which makes it easier for the internal auditors to access them when needed.

The first verification step carried out by the quality assurance analyst is to find the test plan and the approval records for this request. Once located, their contents are analyzed to verify that:

- all the mandatory fields of the test plan have been correctly filled in;
- there is coherence in the various sections of the test plan (i.e. the test cases listed during planning stage are those that were carried out during execution, and were the roles assigned during planning activities subsequently carried out);
- the defects were documented;
- the test approval email:
    - mentions a specific change request number to enable a link to be made between the test plan and a specific request;
    - clearly mentions an approval decision;
    - respects the email naming convention, since the email now becomes a quality record, which must be stored in the project documentation.

Now that the conformance verification has been explained, we can now explain the rating assigned to each of these verification steps in order to give a specific test its C-198 conformance rating.

2.2 How can we rate the C-198 conformance of the test plan and its records?

A conformance rating can be represented as a traffic light [7]. The quality assurance analyst begins the process of rating the test records by giving them a score of 100%,

which corresponds to a hundred points. The conformance rating principle consists of subtracting points with each anomaly found during the verification process.

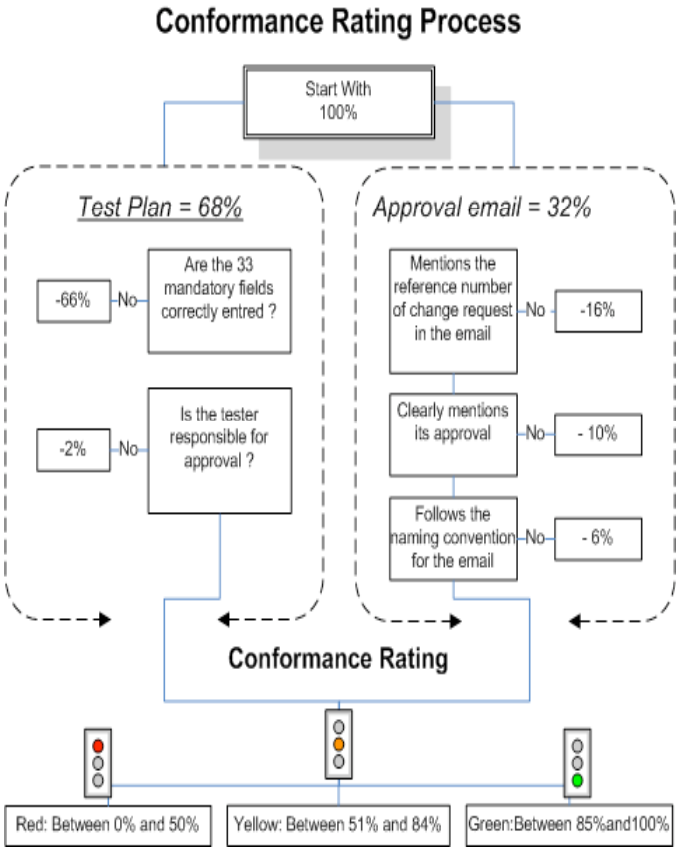


Fig. 4. The conformance rating process translates the many individual controls, which sum up to a high-level traffic light indicator.

Points are removed based on the relative importance of the missing information. With two documents in hand to be evaluated (the test plan and the approval email), we decided that 68% of the points would be allotted to the test plan and 32% to the approval email. In a test plan, there are 33 mandatory fields, which must be present and completed. For each field missing (or not filled in correctly) two points are removed from the total score. Similarly, if there is an error in enacting a role (i.e. for example, if the tester also played the role of test approver), two points are removed.

The most important element in the approval email is the clear presence of an approval statement and the reference to a specific change request. Twenty-six points are removed if this is not the case. Finally, six points are removed if the standard naming convention is not respected.

At the end of this rating exercise, the project will be assigned a percentage. Conformance intervals can be defined using a color scheme. In this case, the following intervals were chosen: red [0..50], yellow [51..84] and green [85..100]).

3 2007 C-198 Conformance results

3.1 Conformance progression in three months

The quality assurance analyst has been collecting measures of conformance for each individual using the software test process by IT sector. These results are used to inform management for the transition allowed before external auditors will come for a formal C-198 conformance assessment.

Conformance is indeed improving. Proportions of Red are getting smaller as each individual goes through the rating process and as the quality analysts train them to understand the defects and correct them. Figure 5, shows the level of conformity of software testing during Mars 2007. The first column (on the left are green) shows 29 test plans that met all the internal controls identified in the new testing process. The second column (in the middle are yellow) shows 21 test plans with average conformity. The last column (on the right in red) shows 15 test plans with many problems. In each case where a test plan has obtained a rating of red or yellow the quality analyst had to explain the defects to the individual and ask him to re-submit the test plan after correction. This cycle ensured additional training. Each individual must reach green status before being allowed to move the software change or project to production.

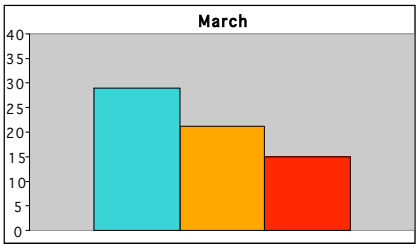
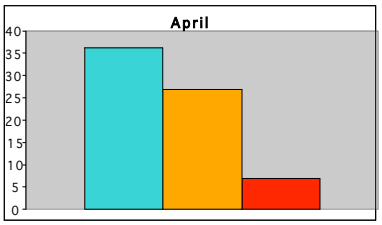


Fig. 5. C-198 Conformance rating of all the test plans submitted, before production go ahead, during the month of March 2007.

Figure 6 shows the progression of conformance results for the month of April 2007. We notice an improvement as red dropped 9 points and green increased 7 points. Similar improvements are also noted during May 2007.



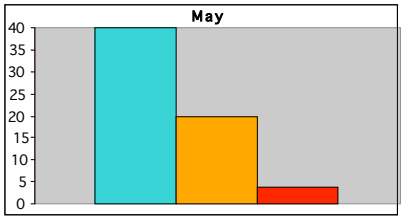


Fig. 6 and 7. Progression of C-198 Conformance rating of all the test plans submitted, before production go ahead, during the month of April and May 2007.

3.1 Individual test plan conformance results

Another measure is also tracked during the conformance review. The goal of the individual conformance measure is to describe the evolution of conformity results by employee. Test conformance of six IT employees are depicted in Figure 8.

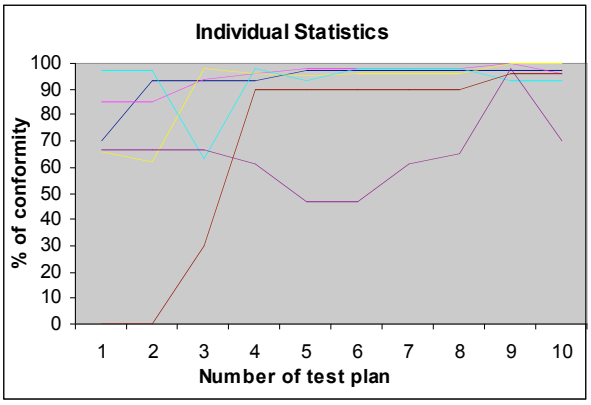


Fig. 8. Individual C-198 conformity progression of 6 employees. This figure shows the learning curve of these employees.

As we can see, in Figure 8, most employees move quickly to C-198 conformance after using the new process 3 to 4 times. Employees had only received a one-hour knowledge transfer on how to follow this new testing process and test plan. Experimenting the new process is an important step as some questions arise. In some cases an employee can become very good at one type of test that they conduct it very often (like unit test). It is when they try another type of test (for example: integration test) for the first time that conformance can dip lower temporarily.

4 Conclusion

Sarbane Oxley (Ruling C-198 in Canada) is forcing internal controls on IT processes. Consequently IT management needs to clarify and define formally its internal processes. Employees need to conform and demonstrate that they follow a documented process, which conforms. We have shown how one Canadian organization has achieved this goal using an experimental process that required many successive iterations. One can conclude from the preliminary measures, that conformance is achievable given that: 1) a precise description of the process is available to employees, 2) a measurement process to rate the conformance is created, 3) knowledge transfer is offered and 4) mentoring and surveillance is applied consistently by the quality assurance analysts during the transition. In this organization, employees have achieved good C-198 conformance, of the IT testing process, within 3 months.

Acknowledgments. Thanks to Linda Michaud and Carole Boudreault for supporting this R&D project.

References

1. MK3, La loi C-198, en quelques mots, On-Line at: Http://www.m3ksolutions.com/francais/loi_c198.htm
2. International Organisation for Standardization. Standard for information technology: software lifecycle processes. ISO/IEC Standard 12207. International Organisation for Standardization/International Electrotechnical Commission: Geneva, Switzerland, 1995; 87 pp.
3. Abran, A.; Moore, J.W.; Bourque, P.; Dupuis, R.: Guide to the Software Engineering Body of Knowledge (SWEBOK) – Ironman version. IEEE Computer Society: Los Alamos, CA, 2004; 202 p. On Line at: Http://www.swebok.org.
4. Central Computer and Telecommunications Agency. Service Delivery. Application Management, Service Support Information Technology Infrastructure Library (ITIL). Controller of Her Majesty`s Stationary Office: Norwich, UK, 2001.
5. Guide to the CSTE Common Body of Knowledge, Quality Assurance Institute, Florida, USA, 2006, http://www.qaiworldwide.org/bookstore/index.html.
6. Galin, D., Software Quality Assurance : From theory to implementation, Pearson Education: Edinburgh, England, 2004, 590 p.
7. April, A., Merlo, E. Process Assurance Audits: Lessons Learned, Proceedings of the 1998 International Conference on Software Engineering, pp. 482-485, IEEE Computer Society Press / ACM Press, 1998.