The Importance of Retaining Testing Evidence in the Financial Industry

BEST METHODS, GUIDELINES AND APPROACHES
SUMMARY

In the financial industry, the consumer has zero tolerance for low quality. Regulatory agencies require financial institutions to present that measures were taken to check the software systems for vulnerabilities, as inattention can lead to damage to the trust in the corporate brand. Despite the importance of retaining test evidence for financial institutions, there is an apparent lack of best practices and proven methodologies.

This white paper will outline the best practices and various available approaches for the recording of test evidence. A final section will provide approach recommendations based on short-term, mid-term and long-term views.

INTRODUCTION

The recent economic downturn and high-profile reports of security breaches and fraud in the financial world have put financial institutions like banks and credit unions under the scrutiny of the public. The financial institutions need to fix various vulnerabilities in their system, but need to also provide complete transparency in regards to their processes.

To ensure customer trust, financial transactions must comply with the industry requirements. Financial IT systems should adhere to the highest quality standards, as any compromise on quality is completely unacceptable. The financial institutions realize this and are heavily investing in testing their mobile applications, and as a result this has become the backbone of their businesses. They want to ensure they cover all aspects of IT systems in order to minimize their exposure to risk. In the event that something goes wrong, they do not want to be found guilty of not taking the necessary measures to ensure quality. However, proving that all necessary checks and tests have been performed is not always easy, as companies do not yet understand the importance of retaining test evidence.

In fact, test evidence can bail financial institutions out of situations that could otherwise deal a fatal blow to their brand.

The software quality and assurance (SQA) team designs and drafts various artifacts to be produced as part of the SQA process. Some of these artifacts include a test strategy, test plan, test cases, test data requirements and test execution results. To confirm and authenticate the actual testing effort, test documentation must be retained. Test documentation includes the test plan, test results and test evidence that must be recorded in a central repository system.

The retention of the test documentation serves several critical purposes, including the following:

1. Validation of the testing efforts
2. Root-cause analysis of QA environment issues and post-production issues
3. Supporting evidence for legal requirements
4. Evidence of support for internal auditing and compliance review
INDUSTRY REQUIREMENTS

Information Technology systems in every industry establish auditing processes to ensure both transparency and reliability. The nature of the financial industry and recent developments make these goals even more critical. Internal governance bodies such as risk assessment and control, operation control, the business disaster recovery team, as well as external bodies like SOX compliance drive the review and audit of different aspects of the IT processes.

At a very high level, the various governing bodies that require the collection and storage of test evidence include:

SOX COMPLIANCE

» Mitigates the risk of fraud; increases transparency and process control
» Ensures consistent, controlled and documented corporate behavior
» Password management and file access privilege
» Network security, virus protection
» Backups, disaster recovery
» Risk evaluation, security training
» Change management system (CCB)
» Consistent logging

BUSINESS RISK / OPERATIONS RISK MANAGEMENT

» Provides required controls to ensure compliance with laws and regulations as well as corporate risk management programs and policies
» Assesses the business risk and provides feedback in the SQA process
» Prioritizes risk reduction techniques

SECURITY COMPLIANCE

» Builds and maintains secure networks
» Protects user information
» Designs a vulnerability management plan
» Provides strong access control measures
» Monitors and tests security regularly

NETWORK MONITORING

» Monitors network traffic, especially for transaction-based services
» Records transactions

OUT-OF-BOUND AUTHENTICATION

» Validates the out-of-bound authentication mechanisms
» Verifies and records the procedure of two-factor authentication
GUIDELINES FOR RETENTION OF TEST EVIDENCE

We provide the basis for modeling different approaches for the retention of test evidence. The goal is to optimize the process of retention of test evidence, while at the same time, collect adequate and accurate information.

Here is how you can achieve this goal:

EVIDENCE COLLECTION PROCESS CHARACTERISTICS

» Adaptability:
The process should be easy to implement across various teams, not only in SQA but also in business team as well as risk management team.
» Minimal Training:
The required training to adopt any approach should be almost none to very minimal.
» Self-Explanatory:
The documents and evidence collected should be very easy to understand.

TEST CASE SELECTION CRITERIA

» Critical Factors:
Test cases can be selected based on the several critical factors such as business critical, compliance critical, etc.
» Risk-Based:
Test cases can be selected based on the different risk factors. The risk factors can include legal issues, functionality complex, page flow, etc. Refer to: HP Quality Center’s built-in risk-based quality management (RBQM).
» Functionality Coverage:
The test case should include critical functionalities from across the application and its ecosystem.

ENVIRONMENT SELECTION

» QA Environment:
Generally, the QA environment is dynamic in nature with builds deployed daily. Because some backend services may run via simulators, retaining evidence from this kind of environment is not highly desirable.
» User Acceptance Testing (UAT) Environment:
The UAT environment, far more stable than QA environments, is usually a controlled environment with access limited to a select group of team members.
» Pre-Production Environment:
The environment offers a very small testing window. Recording the test evidence may or may not be permitted as production data might be used as part of the testing procedure.

INFORMATION TO BE RETAINED DOCUMENT ARCHIVES
[THE VARIOUS PIECES OF INFORMATION TO BE RETAINED INCLUDE DOCUMENT ARCHIVES, TEST LOGS AND SIGN-OFFS. THESE THREE CATEGORIES ARE FURTHER SUBDIVIDED AS FOLLOWS]

» Document Archives:
  • Test Strategy Document
  • Test Plan Document
  • Test Case Document along with test data needed
  • Environment Information (Build Info, Software Info, Backend System Info, etc)
  • Digital Signature

» Test Logs:
  • Automation Logs (Environment, Screen Shots, Client Logs, etc)
  • Test Execution Details (Excel, QC, MS Word)
  • Screen Shot for critical steps
  • Test Data used for each step of the test case
  • Back-end server logs

» Sign-Offs:
  • Sign-offs (e.g., email, digital signature in QC) from all the stakeholders
  • Approvals for exceptions as well as known issues
Collecting test evidence and retaining it for later purposes requires the combined effort of different groups within the organization. Each team needs to work in conjunction with other groups to meet the objective.

The following diagram depicts some of the groups involved:

**DEVELOPMENT**
- Code Instrumentation
- System Logging

**QA**
- Functional Log
- Coverage

**UAT / PRE-PRODUCTION**
- Compliance Test Cases
- Controlled Test Environment

**AUDIT / RISK**
- Periodic Review of Compliance
- Enhance Test Scope

**PRODUCTION**
- Review Production Issues
- Feedback to QA / Audit Team

Five different approaches can be implemented for testing and collecting test evidence. They are:

1. Manual Recording
2. Semi-Automated Recording
3. Automated Testing
4. Backend Snapshot
5. Application Instrumentation

### Levels of Detail by Approach:

<table>
<thead>
<tr>
<th>LESS DETAILED</th>
<th>MORE DETAILED</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTRUMENTATION</td>
<td></td>
</tr>
<tr>
<td>BACKEND SNAPSHOTS</td>
<td></td>
</tr>
<tr>
<td>AUTOMATED TESTING</td>
<td></td>
</tr>
<tr>
<td>SEMI-MANUAL TESTING</td>
<td></td>
</tr>
<tr>
<td>MANUAL TESTING</td>
<td></td>
</tr>
</tbody>
</table>
THE APPROACHES IN DETAIL

MANUAL RECORDING

Testing software manually requires a tester to play the role of an end user, using the features of the application to ensure they run as intended. With this approach, the tester records the necessary screen shots or videos based on the guidelines defined by the SQA team.

ADVANTAGES

» Define the guidelines for what and what not to record
  • Easier to implement
» Ability to reduce or increase scope of testing according to project progress
  • No Special Training Required
» Windows system provides some of the necessary tools

DISADVANTAGES

» Time Consuming
  • Risk of failing to record critical evidence due to manual error
» Not suitable for regression purposes
  • Training and implementation challenges

During the manual process, it is important to collect evidence of software or component behavior from the end user point of view. The evidence can be in the form of documents, logs, screen shots or videos.

In addition to the basic screen capture capabilities of the Windows system, these tools can be used to collect test evidence details:

» QMetry:
  This tool provides an effective means of storing the test evidence in a centralized repository. Documents, logs, screenshots and videos can be attached to the test cases or test execution results.
» HP Screen Recorder:
  This is available as part of the default installation of HP Quality Center as an add-on. Refer to HP’s site for more information: HP Screen Recorder Screenshot.
» Snag IT:
  This popular alternative records screenshots and video.

SEMI-AUTOMATED RECORDING

This hybrid approach combines manual and automated testing approaches and requires minimal effort on the testers part in order to capture the required information.

ADVANTAGES

» From the tester’s point of view, no process change
  • Mostly automatic evidence collection
» Enhanced test coverage that comes from automation side
  • Efficient test runs for evidence data collection
» Information is stored directly in Test Management Tools, such as QC and QMetry

DISADVANTAGES

» Limited tools available in the market that provide this kind of facility
  • Training and additional licensing costs

AUTOMATED TESTING

Test automation automates a manual process already in place that uses a formalized testing process. Using this technique, a test engineer executes the script on any testing tool and uses software to control the execution of tests.

ADVANTAGES

» Reduced manual effort
  • Faster; saves time in QA Cycle
» Simultaneous execution of test cases across multiple platforms
  • Covers large test matrix
» Easily takes care of regression suites
  • Better and faster ROI
APPLICATION INSTRUMENTATION

In this process, the user application is instrumented to properly monitor the application level transactions and data flow. It provides the information necessary for the internal functioning of the application, which can then be used as test evidence. Using this approach, the testing team will work closely with the development team to identify the required instrumentation for achieving the desired outcome.

ADVANTAGES

» Provides control over data collection for evidence
  • Capture transaction-level details
» Collects data evidence that is unavailable using an external pool

DISADVANTAGES

» Time consuming
  • Requires skill for application instrumentation
» The ball landing into development team’s court may impact application performance
  • Complicated Process

The numerous automation tools available in the market include:

» Micro Focus Silk Test
» HP QC-QTP
» Selenium
» Sahi

BACKEND SNAPSHOT

This technique of testing provides control over the testing environment and data and evidence collection. Using this approach, the testing team co-ordinates with the back-end infrastructure team to create the necessary snapshots. The snapshots may include database levels, server logs, etc.

ADVANTAGES

» More control and flexibility over the data environment
  • Pre-defined test suite
» Easier implementation due to control over data environment
  • Captures all transactions and data evidence

DISADVANTAGES

» High maintenance cost
  • Selective test coverage; does not cover all testing paths
» Need to write programs to parse and analyze the details gathered for evidence
  • Retrieving the necessary information is difficult
CONCLUSION

The level of information captured varies for each approach. For example, the manual testing approach captures less information due to the fact that it is done entirely from the front-end of the application—no backend information is captured. On the other hand, instrumentation of the code captures more information since the organization can decide what and how much information must be captured based on the type of system being recorded. The diagram below illustrates this detail.

Taking into account the various criteria and different factors, the InfoStretch team recommends the following approaches along with the deployment and rollout plan.

SHORT-TERM (1 TO 3 MONTHS)

» Manual Recording
  • Easier to implement
  • Satisfies the current audit process
  • Enables the review of recordings and confirmation with internal auditing team
  • Fine-tunes the process time progresses
  • No major investment

MID-TERM (4 TO 6 MONTHS)

» Semi-Automated Recording
  • Newer process with additional tool features
  • Integrated into the manual testing
  • No specific training/steps required of the testing team

LONG TERM (6 TO 9 MONTHS)

» Automated Testing
  • Standard benefits of automated regression
  • Evidence collected for more sets of test cases
  • Centralized approach for evidence collection

ABOUT INFOSTRETCH

InfoStretch is a leading mobile application lifecycle management company with a focus on development, testing, sustenance and monitoring. We have been providing expert mobile solutions and services since 2004 to various enterprises to help them mobilize, monetize and thrive. Our focus is to provide domain specific, end-to-end packaged mobile solutions in retail, travel, banking, digital entertainment and media.

INFOSTRETCH HEADQUARTERS

3200 Patrick Henry Drive, Suite 250
Santa Clara, CA 95054

Phone: (408) 727-1100
Fax: (408) 716-2461
info@infostretch.com
www.infostretch.com