the Availability Digest

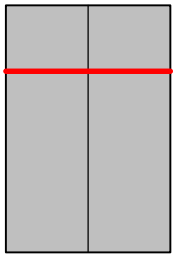
IRS Goof Costs U.S. Taxpayers $300m +

January 2007

The IRS (the Internal Revenue Service, which is responsible for collecting taxes in the U.S.) managed to decommission its fraud detection system for almost all of 2006 before its new system was even tested. The new system subsequently failed its tests with the result that an estimated $300,000,000 or more in fraudulent or improper income tax refunds for tax returns filed in 2005 was paid. This comes out of the American taxpayers' pocket. How could the IRS have let this happen?[1]

The IRS Fraud Detection System

Operational since 1995 and managed by Computer Sciences Corp. (CSC), the Web-based IRS Electronic Fraud Detection System is the second largest repository of taxpayer data in the Department of the Treasury. It holds every filed tax return that claims a refund. Its purpose is to flag potentially fraudulent or improper returns for IRS audit.



Step 1: A Perfectly Good Operational System

In the last few years, this system has flagged anywhere from 40,000 to over 100,000 returns per year and has prevented the yearly payment of something between $300 million to over two billion dollars in fraudulent or improper refunds.

However, tax laws change; and perpetrators get smarter. Therefore, after several years of successful operation, the IRS realized that it had to upgrade the system if it were to continue to be effective at catching fraud.

The Major Upgrade

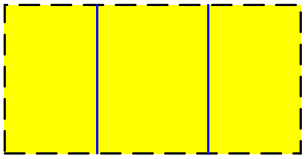
To implement this upgrade, the IRS asked for competitive quotes for a new Web-based system. The IRS designated the new system as a low risk and low complexity project.

---

[1] Material for this article came from the following sources:
USA Today, How the IRS failed to stop $200M in bogus refunds; December 5, 2006.
Washington Post, Software delay said to cost IRS $318 million in overpaid refunds; Saturday, September 2, 2006.
AOL News, IRS didn't use a fraud screening program this year; July 15, 2006.
Zdnet, With no fraud-catching program, IRS loses $300 million; September 5, 2006.
FCW, House chides IRS on failed fraud-detection system; August 8, 2006.
Tennessean, IRS knew risk before refunds; December 5, 2006.
CNN Money, Outdated computers cost IRS $200 million; July 14, 2006.
Foundation for Economic Education, Computer Failure Leads to Big IRS Refunds; December 5, 2006.
GovExec, GAO knocks IRS for gaps in computer security; March 29, 2006.
GovExec, Failure of tax fraud detection system worse than estimated; September 5, 2006.

The winner was DynCorp of Reston, Virginia. DynCorp's bid was in the order of $20 million. Shortly after, CSC acquired DynCorp and became the contractor for the system.

Work on the new system began in 2001 with an expected completion date in late 2005, just in time for processing the 2006 tax returns.



Step 2: Start Development of New System

However, as often happens, the project began to show delays. It was plagued by a high turnover in CSC personnel (over 50% during the course of the project) and by numerous changes in the IRS executive ranks. As a result, the system cutover was delayed until January, 2006, and then to February. Things were getting tight if the 2006 tax returns were to be processed by the new system.

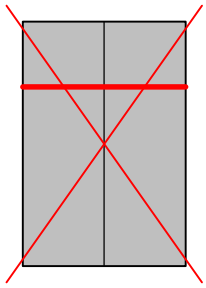
But warning flags were being raised. By November of 2005, it was reported that:

- communication between the IRS and CSC computers was painfully slow, often occurring at a speed equivalent to a dialup line.
- there were repeated delays in setting up an Oracle-based computer network.
- the servers were unreliable and continually shut down.

Despite these warning, IRS and CSC personnel repeatedly voiced confidence that a February, 2006, cutover would be achieved.

Cutover – Bigger Than the Big Bang

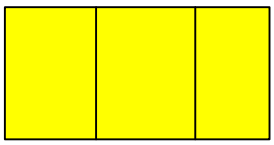
Based on this rosy, optimistic outlook, the IRS decided to shut down the current system in late 2005 in anticipation of the new system becoming available shortly in January, 2006 (subsequently delayed until February). So confident were they in the new system that a contingency plan to recover from a failed cutover was never even created. Thus was laid the groundwork for disaster.



Step 3: Decommission Good System

The ax fell when a March, 2006, test showed that the new system could not even process a day's worth of data in a day. In effect, it could not keep up with the workload and would never work!

No one likes a big-bang cutover in which all processing is suddenly switched to a new system in the hopes that it will work. However, if the new system doesn't work, at least processing could be returned to the old system.



Step 4: Test New System - Oops!

In the case of the IRS Electronic Fraud Detection System, there was not an old system to return to since it would have taken too long to load the pertinent 2005 returns. The IRS had to stop checking the 2005 returns for fraudulent refunds. Initially, they temporarily froze some 500,000 refund requests but eventually released these and processed all returns, whether proper or not.

Even with such an obvious catastrophic outcome, this disaster did not become public until a hearing before the Senate Finance Committee in July of 2006. The IRS did not want to expose this problem until all 2005 returns had been filed to avoid providing a roadmap to those who would abuse the system.

Through other procedures, the IRS was able to catch about $94 million in improper returns. However, the Treasury Inspector General estimates that perhaps $318 million dollars in fraudulent and improper returns were not detected. It is unlikely that most 2005 filers with improper refunds will ever be caught.

In fact, the IRS lacks any comprehensive plan to recover fraudulent refunds. Mark Everson, the IRS Commissioner, said that "we're not going to go back … that's gone."

From the IRS Commissioner

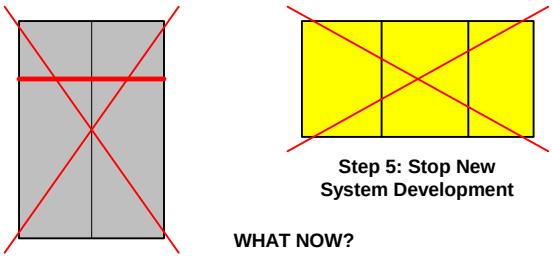
The reaction of IRS Commissioner Mark Everson to this disaster was very insightful. He said:

"Certain key decisions should have been elevated or different decisions should have been taken and brought up the chain at certain points in time. There was not an appreciation of risk or good appropriate communications here. That to me is the beginning and the end of it … There might be some things that contributed at the margins, of course. You've got to have good processes. People have to know what's important to take up … and to exercise good judgment, and it didn't. happen in this case."

From a Never Again viewpoint, the operative words in his statement are "*There was not an appreciation of risk …*" That is an understatement at best.

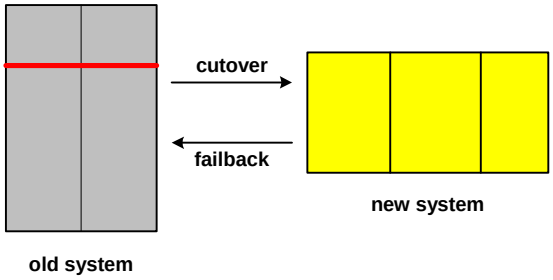
What Next?

As a result of the March, 2006, test that showed that the new system could not keep up with the workload, the IRS directed CSC to stop work on the new system and to restart the old system so that it could begin processing the 2006 tax returns starting in early 2007. The IRS says that improper 2006 tax returns may trigger audits on the corresponding 2005 returns,



The Treasury Inspector General plans a study to determine more precisely the amount of fraudulent refunds that were lost. It will also do a detailed review of the IRS fraud detection procedures.

Lessons Learned



The main lesson to be learned from this disastrous experience seems to be painfully obvious. It is to ***never cut over to a new system without a contingency plan***. Should the cutover fail, there must be a way to continue processing on the old system.

The first step in this process is to fully test the new system before the cutover. Somehow, the IRS thought that the new system would be infallible. As Mr. Everson said, "There

was not an appreciation of risk." To actually decommission the old system before the new system has proven itself to be properly working is pure folly.

In fact, given the industry's years of experience with these sorts of cutovers, it should be obvious that the odds are against a new system becoming operational according to its intended schedule. System developments almost always extend beyond their scheduled times.

Failing back to the old system is not necessarily an easy process. What happens to all of the transactions that have been processed on the new system? Can they be recovered and reentered on the old system? Can the old database be brought up-to-date with the current state of the application?

In the IRS's case, a simple solution could have been the reentry of those refund-claiming tax forms that had been entered into the new system before the failback decision was made. However, missing the first several months of activity robbed the IRS of this opportunity.

Of course, the best contingency plan involves replicating transactions entered into the new system back to the old system to keep its database synchronized. In this way, the old system is immediately ready to be returned to service. The ultimate of this strategy is an active/active architecture in which the new system is brought online and shares the processing load with the old system. In either case, only when the new system has proven itself is the old system retired.