JFMIP

JFMIP White Paper:

Parallel Operation of Software

Is it a Desirable Software Transition Technique?

October 24, 2001

SP-02-20

FOREWORD

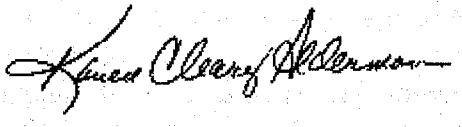
The JFMIP White Paper, "Parallel Operation of Software: Is It A Desirable Software System Transition Technique?" is intended to assist agencies when developing appropriate risk mitigation strategies when transitioning to new financial systems, especially commercial off-the-shelf software where existing business processes must be reengineered to avoid software customization.

This White Paper updates selected information currently contained in the JFMIP *Framework for Federal Financial Management Systems*, FFMSR-0, issued in January 1995, regarding transitioning to a new system. The *Framework* document describes how the various financial management systems covered in the specific requirements documents fit together and how these systems should be integrated.

Since the *Framework* document was last issued in 1995, both technology and implementation practices have evolved. Because the *Framework* document is comprehensive, this white paper, as well as others to come, is designed to update and expand upon selected topics that are of critical interest to agencies and oversight communities. The goal is to provide current information through posting the White Papers series on the JFMIP Knowledebase at www.jfmip.gov and to provide a method to vet topics that will be incorporated into a later update of the *Framework* document.

Comments on this document are encouraged. Respondents should also indicate the capacity in which they are responding. You can reach JFMIP at 202-219-0526 or write to us at:

Joint Financial Management Improvement Program
Suite 430
1990 K Street NW
Washington, DC 20006



Karen Cleary Alderman
Executive Director
July, 2001

INTRODUCTION

The *JFMIP Framework for Federal Financial Systems, January, 1995,* references parallel operations as one of the 3 systems transition techniques. It states: "Running the new and existing system in parallel allows operations to continue in the old system while errors are corrected in the new system". However, in light of the recent transition to commercial off-the-shelf- software (COTS) applications as the primary source of financial systems replacements, there is a need to evaluate the practice of parallel operations as a risk mitigation factor. This "JFMIP White Paper" discusses the appropriateness of "parallel operation of software", as a risk mitigation practice when replacing the agency's Core Financial System. The purpose of the paper is to present an objective discussion of what parallel operations is, issues surrounding it, how it is affected by the changing environment, and problems associated with parallel operations.

ISSUES/QUESTIONS

- What are key testing considerations when implementing new systems?
- What are the benefits and costs associated with operating software in a parallel mode?
- Is parallel operation a good business practice during systems implementation?
- Is parallel operation being mandated to address other requirements such as continuity of operation in the event of a system failure?

DISCUSSION

Parallel Operations Defined. For purposes of this paper, parallel operation is defined as operating both the legacy and replacement system concurrently for a specified period, in order to test the new system. The legacy system is assumed to be the "production" system of record, while the replacement system is assumed to be in a "development", non-production status. During parallel operation, both systems operate concurrently, support the same function, process the same data, and are expected to produce the same result. Data entry and workflow are duplicated and discrepancies between the expected results are reconciled and appropriate follow-up action taken. There is an assumption that when the replacement system has satisfied established test performance criteria and results, the legacy system will be phased out or discontinued and the replacement system will be migrated to "production" status and become the new system of record.

It should be noted that the definition and use of the term "parallel" is inconsistent in literature and reference material. The primary focus of this paper is on the replacement of the legacy core financial management system with a JFMIP qualified core financial management system.

Parallel Operations is an Option of Last Resort. The decision to conduct parallel operations must be made within the context of:

1. A well defined test plan that describes testing to be conducted throughout the replacement life cycle, and

2. The comprehensive risk management strategy and plan.

The test plan should describe the scope, test methods, expected results, authority, roles, and other criteria for testing to be conducted at each phase of the project. The test plan might include the following:

- *pre-implementation testing,*
- *requirements testing,*
- *systems acceptance testing,*
- *user acceptance testing,*
- *application testing*
- *integration testing,*
- *hardware/software testing,*
- *performance (i.e. testing for volume, scalability, security, etc.), and*
- *regression testing associated with configuration management and control.*

In addition to the test plan, the degree to which identified risk is mitigated during other phases of the project should be considered. A review of the following activities may be helpful in assessing the degree of risk:

- *Functional Compliance* - Is the core financial system qualified by JFMIP? Is this version live elsewhere and what are the similarities? What additional pre-award testing and evaluation has occurred.

- *Quality Assurance and Compliance* - Are quality assurance criteria established for measuring compliance at critical points in the implementation life cycle?

- *The Implementation Strategy* - Is the implementation strategy based on an incremental or phased approach that lessens risk, such as implementing first for one appropriation, fiscal year, organization or function? Has the software already been implemented elsewhere in the agency. Does the conversion strategy follow a similar incremental approach to migrating data?

- *The Training Plan* - Can inference about user acceptance be derived from an evaluation of training plan and results?

- *Continuity of Operation/Disaster Recovery/ Security.* Are there appropriate risk mitigation plans or measures in place commensurate with the risk?

- *Independent Review* and *Validation (I,V&V)* - Is there a strong I,V&V process and is independent review being effectively incorporated into the project strategy?

Finally, the feasibility of parallel operations should be considered.

- Can the two systems even be compared? What is the degree of similarity and difference in functionality, processing, and data, between the legacy and the replacement system(s)?

- Is the full scope and workload of the parallel test known and is it cost-effective?

- Is reconciliation expected and attainable?

- Is there discipline to complete the parallel operation as planned ?

Defining Test Objectives. Project planning and testing should follow a disciplined process. Any recommendation to conduct parallel operation should reflect the same discipline. It is important to fully define the objectives, scope, methodology, responsibilities and timelines, in context with overall risk management, so that cost/benefit and return on investment criteria can be objectively applied. What is the objective, scope, cost, and timelines and how does it impact the critical path and resources? What is the cost/benefit? What is considered success and how is compliance defined? How will it be known and who will decide? The specific objective of the test should be stated and the test designed to meet it.

Is parallel operation being prescribed to compensate for something else? What risk aspects addressed by parallel operation may have already been mitigated by other testing or processes? It may be helpful to particularize the specific risks the proposed parallel operation is to address. Does the test objective warrant something other than parallel such as to test software, enhancements, data integrity, scalability, the effectiveness of training, the hardware software platform, etc.? There may be occasions when some type of minimal parallel operation may be warranted, however, considerations for effective risk management when implementing COTS systems might be more appropriately focused on acceptance testing and strong I,V&V.

Focusing on the objective of the proposed parallel operation is critical to a disciplined test process. Once the specific objective(s) are particularized, then a decision model can be followed and the appropriate testing can be applied.

Costs of a Parallel System Operation. Parallel operations are complex and require formidable resources, in both staff and funding. The cost to operate two separate systems in parallel also occurs at a point in the project where resources are already stretched. Parallel operations include the full cost of operating both the legacy and the replacement

system, including platform support and facilities. The workload extends beyond the operation of the systems per se, in that parallel operation requires the participation of the users in order to replicate the accounting processes. Alternatively, it requires the assimilation of additional project staff to the accounting operations environment. Both alternatives are likely to meet strong resistance at a time when project staff are stretched and users are already increasing their workload for training, data clean up, learning new business processes, etc. These factors create the need for much determination and strong oversight to ensure it stays on track.

The added workload of maintaining two complex systems increases the risk of human error from over-extended or inexperienced staff. The resulting increased error rate makes the reconciliation and data clean-up efforts even more time consuming and difficult.

For parallel operation to be to be successful, it is assumed that the data output and reports from both systems will be reconciled. The reconciliation of the two systems may be significantly costly if not impossible. A recommendation to conduct parallel operations should be made with the full understanding of the scope, cost, timelines, and procedures that will be followed along with a realistic evaluation of the expectation that will actually be completed.

Business Process Reengineering - Can the Systems be Compared?

Along with the deployment of a COTS solution is the expectation that agencies will seek software based on "best fit" and adapt business practices. More emphasis should be placed on increased functionality of the replacement software that goes beyond that provided by the legacy system. The processes may have changed so that a parallel operation can not even be done nor will any beneficial results be gained.

Many legacy financial systems being replaced are as many as 20 years old. Both the systems and the way systems are implemented has changed. Legacy systems are frequently main-frame based systems that were highly customized and developed in-house in somewhat of a "stovepipe" manner. Many of the current JFMIP qualified core financial systems include an integrated work flow process that create and post the financial transaction as part of the business process that is being accomplished. The practice of parallel operations dates back to then and may have more validity if a newly developed system is being rolled out for the first time. The current trend is toward implementing suites of COTS based administrative systems in a Client Server or web-based environment. An important tenet of current federal COTS policy is to encourage the purchase of JFMIP qualified COTS systems that are "best fit" and to reengineer business practices around them. The JFMIP Core Financial System Qualification Test Program has, in effect, established "configuration control" for baseline core financial systems software at a government-wide level. COTS, however, still require significant implementation effort, including additional testing (acceptance, user, interfaces, performance, regression), but it has eliminated a high degree of risk regarding the capability of the core software to meet the JFMIP Core Financial System Requirements.

Likewise, the experience of several agencies implementing the qualified version creates a continuous improvement cycle as agency experience is incorporated into new releases. As such, the risk has shifted away from the core financial processing (General Ledger, Accounts Payables and Receivables, Funds Control, Reporting) to the implementation, particularly to integration and enhancement.

The largest proportion of the replacement cost is implementation. Many implementation failures result from customizing software and failure to integrate systems and data within a defined architecture. Some agencies are trying to replace literally hundreds of feeder systems and applications concurrently. Reengineering business practices is the best strategy to reduce the risk of failure. If the agency has been successful at reengineering business practices, it can avoid the enormous risk inherent in customizing software. In taking full advantage of the new system and functionality, the new system will in fact be different from the legacy system. Parallel operations may make sense when replacing an identical "stovepipe" system, but is not feasible when the replacement system is significantly modernized.

Replicating the Results of the Legacy System Raises Questions. While the legacy system does provide a benchmark for measuring improvements, one might question the usefulness of expecting the legacy and replacement system to produce the same result. Inherent in the requirement for a parallel operation is an unstated belief that the legacy system produces correct results. Agencies typically identify numerous points of non-compliance with requirements as justification to replace their system. Examples of non-compliance are FFMIA (SGL, accounting standards, JFMIP requirements), FMFIA deficiencies, qualified audit opinions, etc. It's assumed that the decision to replace the core financial system was predicated on a decision that those limitations are no longer acceptable. Should the new system be required to recreate deficiencies? Since they won't, this may further negate the feasibility of conducting parallel operations.

In addition to being non-compliant, the legacy system may also contains bad data or have systemic data integrity problems. The condition of the data in the system should be factored into the decision, particularly in projecting the scope of the work and whether it's even feasible to expect the results to be reconciled.

How does the agency's data clean up and conversion plan fit in with the parallel operation in terms of the critical path? Data clean up is the process of validating the transactions in the existing system and making adjustments prior to converting the data into the new system. The resources that should be focusing on reviewing the open transactions are most likely same ones conducting the reconciliation. Will data clean up occur before, after, or concurrently with the parallel operation?

Change Management Factors. Conducting parallel operations may present an unintended consequence where "cultural change" is a factor in risk. Parallel Operations may aid in resistance to change and may in fact be a sign of it. Top down commitment to the new system is a critical success factor. Likewise, the commitment should be to reengineer business practices and migrate quickly to the new system. There's a tendency

for agencies to rebuild or preserve the old system. Likewise, there may be resistance to change within organizations or people who feel they have a vested interest in the legacy system or that the new system is wrong. While these issues are outside the scope of parallel operation itself, parallel system operation may send a message to the organization that the old system is still valuable, is the benchmark for the new system, and that the new system in effect "competing" with it for the starting job. This commitment to the old system casts doubt on the viability of the new system. If problems arise in the parallel system operation, the organization will tend to spend resources on keeping the current system operational rather than on solving problems in the new system.

Private Sector Experience. Has parallel operation proven successful in other organizations? The request to undertake a parallel operation arises on a periodic basis, yet there is no evidence that any organization has successfully completed one. The only article that could be found in a literature search was "The Three Phases of Implementation", by Richard Dance, Management Accounting, February 1996. Dance discusses, "... In theory, (parallel testing) it was a good idea. In practice, it was terrible for a number of reasons, the chief being that at the end of the parallel test, the two systems didn't match. After much analyzing we usually found the old system was at fault, and nothing new was known about the new software, in spite of all the time spent on the parallel test."

Is Parallel Operation a Desirable Strategy to Ensure Continuity of Operation (COOP)? A need for parallel operations may actually represent a need for contingency planning. Whether perceived or real, the risk of a system failure may be somewhat higher for a newly implemented system. In fact, requirements for addressing the risks of system failures already exist.

The Computer Security Act of 1987 mandates security planning for all sensitive systems, and all financial systems have been deemed sensitive systems. The sensitive system security plan should identify actions to be taken to ensure that: (1) the confidentiality of the data processed is protected against unauthorized disclosure; (2) the integrity of the data processed or maintained in the system is protected against unauthorized or unintended modification or nonrepudiation; and (3) the availability of the system and the data to authorized users is maintained.

The requirement for security planning pertains to systems under development as well as those in operation. For systems under development, planning for system security begins in the requirement definition and analysis phase, and a viable security plan should be developed prior to implementation of the new system. For operational systems, a security plan should be developed and/or periodically reviewed and updated. While access and other security controls are important elements, the systems security plan should also address plans for the continuity of system operations, disaster recovery planning, and data backup and recovery plans.

Planning for the continuity of operations is an important element for ensuring the ongoing availability of the system. Disaster recovery and contingency planning are often

used interchangeably. While these actions can be overlapping, they are separate and distinct. The COOP generally focuses on the proven availability of an alternate processing system to ensure that financial transactions can continue to be processed and that current financial data can continue to be available to support decision-making. The disaster recovery plan, which should include a data backup and recovery component, focuses on actions that are necessary to bring the primary system back into operations, including any necessary restoration of historical data. A disaster recovery plan without a COOP means that, in the event of a system failure, the organization will not be able to continue to execute financial transactions or to have access to current financial data. A COOP without a disaster recovery plan means that, in the event of a system failure, the financial system operations will be able to continue. However, the organization will likely have great difficulty in restoring the failed system to operation and, without a data backup and recovery plan, will not be able to restore the historical data. The data backup and recovery plan also plans a key role in ensuring data integrity. The corruption of data in the system can occur as the result of intentional or unintentional actions. Periodic data backups are critical for restoring the integrity of the system data if unauthorized or unintended modifications occur.

If you have proper backups and disaster recovery plans in place, there is no need for a parallel operation in order to ensure continuity of operation. Parallel operation is not a cost-effective choice for providing contingency operations, and it should be the option of last choice. The costs of operating and maintaining two systems can represent an onerous burden that could undermine the support for the new system. The implementation of new systems often pushes the data entry beyond the financial offices into the program offices. With parallel operations, these new users would be required to learn to use two systems – the old and the new, and duplicate entry of data would be required. There would also be a significant resource cost imposed to perform the necessary reconciliation and associated correction of missing or incorrect entries.

IV. CONCLUSION

A strong test plan to mitigate risk during the planning and implementation phases for new financial systems is essential. Moreover, executing and taking corrective action prior to going live should preclude the use of parallel operation as an additional risk mitigation strategy. There should be a well-defined plan to evaluate operations after going live with a new system such as ongoing use of regression testing tools and a planned system validation after a specified period of time to assure that the new system is producing appropriate results. While there would have to be a case by case plan for testing and risk mitigation throughout a system lifecycle, the risks for the new system that *could* be addressed by parallel operation are more appropriately and cost effectively addressed through strong testing should occur during earlier system implementation tasks. The cost of parallel operations and the difficulty in reconciling old and new system results when business processes have been reengineered generally make parallel operations an undesirable risk mitigation strategy.

JFMIP Requests for Publications

JFMIP documents may be accessed electronically on the JFMIP Website

http://www.jfmip.gov

The JFMIP uses the General Accounting Office's Document Distribution Center to fulfill publication requests which are made after mail list distribution. The first copy of each publication requested is free. Additional copies are $2 each.Orders for100 or more copies to be mailed to a single address ar ediscounted 25%. Orders should be sent to the following address accompanied by a check or money order made out to the Superintendent of Documents, when necessary.

Orders by mail:

U.S. General Accounting Office
PO Box 37050
Washington, DC 20013

Orders by phone:

Voice: 202/ 512-6000
Fax: 202/ 512-6061
TDD: 202/ 512-2537

1990 K Street NW
Suite 430
Washington, DC 20006

OFFICIAL BUSINESS

Penalty for Private Use $300

Presorted Standard
Postage & Fees Paid
GAO
Permit number G100