



**proud past, promising future**

**CLARK COUNTY**  
WASHINGTON

AUDITOR  
GREG KIMSEY

---

## **Clark County's Information Services**

### **Gaps Still Exist Over Key Information Technology Controls**

**Clark County Auditor's Office  
Audit Services  
Report # 07- 05**

**October 31, 2007**



For an alternative format, contact the Clark County ADA Compliance Office.  
V (360) 397-2025; TTY (360) 397-2445; E-mail [ADA@clark.wa.gov](mailto:ADA@clark.wa.gov)

#### **Audit Services**

1300 Franklin Street, Suite 575, P.O. Box 5000, Vancouver, WA 98666-5000

---

(360) 397-2078, Fax (360) 397-6007, [www.clark.wa.gov/auditor/audit](http://www.clark.wa.gov/auditor/audit)

## RESULTS IN BRIEF

The County's Financial Management System (FMS) is supported by a specific group of staff within Information Services (IS). Staff support includes, but is not limited to, troubleshooting and resolving problems reported by users, developing solutions that may result in changes to the system programming or changes to table data, and applying patches and upgrades. IS staff are aligned to the county's business practices, and thus, other staff are responsible for support of applications such as the county's permitting systems, or time entry systems.

Information Services' support for FMS, including the Human Resources and payroll modules, has been reviewed by Audit Services internally twice over the past three years. Specifically, these were reviews of internal controls over any system or data changes. This report follows up on previous recommendations and represents the third review of these support services.

Recommendations were made around four key areas – managing changes made to financial systems, supporting a payroll time entry system, improving management reporting tools, and planning for disaster recovery. While some recommendations have been implemented, gaps still exist over key information technology controls.

There are gaps in providing adequate controls over changes made to the system or system data and for the payroll data entry system. Specifically, we found:

- A lack of controls to adequately document and control programming changes made to the system and/or to data, along with unrestricted programming staff access to the live environment (production), when staff should be limited to development/test only. This allows changes to be made to the system that may not be controlled, authorized, tested, or approved. Access to systems should be limited and controlled by management.
- One payroll time entry system (written internally) has never been fully documented and has six versions, resulting in inefficiencies for staff supporting the system, and increased risk of system failure.

We found improvements in the following areas:

- The county is moving forward with planning for disasters and other emergencies. Enhancements have been made to the county's ability to re-initialize financial systems in case of a disaster. In addition, departmental planning for disasters will be facilitated by a consultant, who will help the county put together a comprehensive disaster plan.
- Currently, limited reporting tools are available. IS has determined that more training is needed by department staff in the use of the tools that are available; training has been provided for one reporting tool.

# TABLE OF CONTENTS

RESULTS IN BRIEF .....	i
TABLE OF CONTENTS .....	ii
INTRODUCTION .....	1
RESULTS .....	2
Change Management: Data Validity and Accuracy .....	2
Time Entry System: Security, Efficiency, and Documentation .....	6
Reporting Capability: Efficiencies .....	7
Disaster Planning: System Security .....	8
CONCLUSIONS .....	9
APPENDIX A: Objective, Scope, and Methodology of Work Performed.....	10
APPENDIX B: Detail, Status, and Further Recommendations Regarding Change Management	11
List Approvers for Authorizing Changes.....	11
Log Data to Record Description of Changes Made .....	11
Review Periodically.....	12
Control Log Access .....	13
System Documentation: Change Management .....	14
Define Staff Roles and Responsibilities .....	15

## INTRODUCTION

The County's Financial Management System (FMS) is supported by a specific group of staff within Information Services. Staff support includes, but is not limited to, troubleshooting and resolving problems reported by users, developing solutions that may result in changes to the system programming or changes to table data, and applying patches and upgrades. Other staff are assigned responsibilities for support of applications such as the county's permitting systems or time entry systems.

Information Services' support for the county's financial management system, Human Resource Management System (HRMS), and payroll system has been reviewed internally by Audit Services twice over the past three years. These reviews were not comprehensive; they focused on internal controls over changes made to the systems or to data.

### First Review: Performed in 2004, Issued in 2005

The county implemented FMS in November 2002. In mid-2004, Audit Services was asked to review system support activities to determine if appropriate and complete data was being captured related to any changes made to system production. Audit Services staff worked with both Financial Services/Auditor's Office (FS) and Information Services/OBIS (IS) staff to determine the type and nature of data being captured.

Recommendations for improvements were provided to both offices as memorandum, dated May 10, 2005. This review found few controls in place to monitor changes made to the financial systems. There was evidence that changes may have been made that were not captured or documented. Recommendations to the department director included having all changes be approved by authorized users and all changes captured, or logged, to ensure they were appropriately approved and tested before being placed into production.

### Second Review: Performed in 2005, Issued in 2006

The county implemented both the HRMS and payroll systems in 2005. After this implementation, internal audit was asked to perform a post-implementation review, which in part was to determine if internal controls had been adequately addressed. For IS, the review focused on those areas where technical support to system operation was necessary for both the "functional" departments of Human Resources (HR) and FS.

Audit Services found the same conditions existing over change management that had been reported earlier, with some improvement in appropriate data capture (through the problem log<sup>1</sup>). Recommendations included tightening controls over

---

<sup>1</sup> The problem log is the tracking mechanism developed for use by the FMS support group and FMS users to record problems, requested changes, requested reports, and other items related to the support and

the change management process, documenting time entry systems, making system reporting more available, and strengthening disaster planning. Other areas, specifically the separation of key duties between staff that develop, test, and move changes to the system's production environment, could not be reviewed at that time because they were being developed and had not yet been finalized.

#### Current Review: Initiated in 2006

IS provided an action plan in response to the memorandum that included estimated timeframes to address the audit recommendations. As agreed, Audit Services initiated a follow-up review beginning in December 2006 and found several action items remained incomplete. This report addresses the results of efforts made and work remaining on the part of IS in responding to all previous recommendations.

Note: All work related to HR and the FS were addressed in a separate memorandum and the follow-up work was completed and reported on to those departments' directors. Recommendations were implemented, or are in the process of implementation.

## **RESULTS**

Recommendations were made around four key areas – managing changes made to FMS, supporting a payroll time entry system, improving management reporting tools, and planning for disaster recovery. These recommendations are intended to meet internal control objectives for system security, data validity and accuracy, security and documentation, and efficiency.

### **Change Management: Data Validity and Accuracy**

[Original recommendations May 2005 and May 2006]

Managing changes made to any system acts as an essential control over that system. This allows users to rely on data processed by the system, knowing it is handled consistently, the data is both valid and accurate, and is recorded in line with any requirements set by management. A change management system would contribute controls related to (1) accuracy and completeness of data and other information, (2) security of the information, (3) compliance of data to requirements, and (4) reporting.

---

maintenance of FMS. The log consists of a database that has been placed on FMS user's computer desktops at the user's request.

Our previous review resulted in the following recommendations for strengthening internal controls over FMS processing, specifically regarding management of changes made to the system or to the system's data.

#### List Approvers for Authorizing Changes

- Good change management would include processes to ensure that all changes are appropriately authorized. Maintaining a list of authorized approvers helps to ensure that staff are aware of, and can readily determine, who is authorized to approve changes. Changes requested by other than authorized individuals should not be addressed until they are properly authorized

#### Log Data to Record Description of Changes Made

- In addition to ensuring that all changes are appropriately authorized, a change management system should also require a sufficient description of the change that would allow staff to replicate that change should it be lost. This creates efficiencies, as staff do not have to recreate solutions to problems.

#### Review Periodically

- Logs or tracking mechanisms that record information about requested and resolved changes should be reviewed periodically by management to ensure that entries are completed appropriately and that any changes made have been appropriately authorized, tested, and approved for movement to the production environment.

#### Control Log Access

- Access to the problem log (current tracking mechanism for changes) is not delineated and anyone with the log icon on their desktops can add or close entries. As processes are refined, the log should have more controlled access by users, with fields restricted to authorized staff.

#### System Documentation

- Processes involved in change management should be well documented, with that documentation available to staff responsible for the work.

#### Define Staff Roles and Responsibilities

- Staff roles and responsibilities, including access to FMS, should be well defined and documented so that management can determine if appropriate separation of duties exists between the development of a problem solution and the movement of that into the production environment.

**Current Status:** We reviewed efforts made for each of the issues raised by our recommendations (above) and found limited improvements. For example, the list of approvers has been created and support staff use it to obtain appropriate approvals for changes to be made to the system.

However, we found areas where improvements were still needed. Because IS has not moved to a change management system, there may be no documentation for processes involved in making changes. For example, in spite of the fact that management is reviewing the problem log more frequently, we found that many logged entries, when closed, do not contain adequate documentation to allow the change to be repeated if it were lost. Specifically, of 29 log entries reviewed, 15 did not have a solution description in the solution field. Of the 15, ten entries did contain information about the solution; this information had to be inferred from the total log entry.

We also noted that staff roles and access “responsibilities”<sup>2</sup> are in conflict with an appropriate separation of duties. For example, programmers responsible for making changes to the system have access to the development, test, and production “environments” of the financial systems, and are thus able to make changes to either the programming of the applications/software, or to data contained within the systems. Currently, their actions within the systems cannot be tracked or traced.

We noted that the department has been investigating a service management best practice for managing change from ITIL – the Information Technology Infrastructure Library<sup>3</sup> – which would bring a methodical approach to handling change management. The steps, or controls, outlined in the ITIL practices – which include those recommended by our previous reviews, as well as others -- would lead to more transparency and better communication between users and support staff. Proper documentation of all changes should lead to greater efficiencies for the support function.

Discussions with management indicate a desire to improve controls over the systems, but an acknowledgement that it is difficult and will require some cultural changes. For example, currently support staff handle calls directly from users and are able to resolve issues more quickly because of less restricted access into FMS.

However, doing so leaves both the system’s data and the support staff vulnerable, unprotected by system or process controls. If internal controls are improved in line with these recommendations, support staff would have the

---

<sup>2</sup> Responsibilities is a specific term in FMS for the level of access granted to a user, including support programmers and database administrators.

<sup>3</sup> ITIL is a standard for describing a number of fundamental processes in IT Service Management; it is a collection of best practices developed in the industry. The ITIL philosophy adopts a process driven approach which is scalable to fit both large and small IT organizations.

testing environment to develop solutions, but they would not have access to the production environment. Programming or data changes would more appropriately go through the database administrator, who has been given the responsibility to place changes into production.

**We commend** management's investigation of the ITIL methodology and encourage implementation of controls that would help make processes more transparent, result in better communication, separate duties of creating changes and placing them into production, limit access to production, as well as to ensure adequate documentation especially as it relates to the previous recommendations, listed above.

**We continue to recommend** improvements in controls, specifically:

**We encourage** Information Services to maintain the list of authorized approvers and to periodically solicit updates.

**We recommend** that problem log entries representing changes to the system should be completed with the requested information and that those parties responsible for the completion of selected fields be identified and notified of their responsibilities. Management indicates that log data will be complete by the end of the 2007.

**We continue to recommend** that management review the logs on a periodic and routine basis. In addition, **we recommend** that management expand their review to include closed entries, to further ensure that adequate data is being provided.

**We continue to recommend** that the department consider securing segments within this problem log since the current version of the log allows anyone with access to alter information within the log – to include closing an entry before work is completed.

**We recommend** that IS document the change management process, to include identification of the roles and responsibilities for staff – both FMS support and department users – to help ensure that the problem log is completed appropriately.

**We recommend** that the department review IS staff access levels to the financial systems to determine if adequate separation of duties exists, specifically for programmer staff, to prevent unauthorized changes to the system and as a protection for the staff. If duties cannot be separated, some type of compensating control, such as a tracking report of IS staff activity within the financial systems, be created, reviewed and monitored, so that management is aware of and can act on any actions taken by staff that do not conform to expectations.

**We also recommend** that IS implement a uniform change management process that applies across all applications and platforms.

Details on each of these recommendations are contained in appendix B, attached to this report.

### **Time Entry System: Security, Efficiency, and Documentation**

[Original recommendation May 2006]

Regarding Clark County Time Entry (CCTE), we recommended that IS (1) ensure that passwords are safeguarded for any and all systems that process information flowing into or from financial systems, and passwords should not be visible to any users or administrators or timekeepers; (2) versions be condensed, whether to a web version or not, to increase the efficiency of maintenance and support of the system; (3) IS enhance, maintain, and update all system flowcharts and other documentation throughout the system's life.

**Current Status:** The time entry system was, initially, under the same manager as the FMS support group. As of this time however, the system has been moved to another support group, and is no longer under the same management as the FMS support group. This division is based on the platform that the system is based on; in this case the time entry system is based on VB6, unlike the FMS systems that are Oracle based. The VB6 "language" is no longer supported, which makes supporting this application even more difficult.

We learned that

- there have not been many changes made regarding this time entry system, but additional "versions", created to meet various user requests and the addition of other users, have been put into place;
- there are six different databases based on this system compared to the three that existed when we looked at the application in 2006;
- consequently, versions have not been condensed or consolidated;
- passwords are now unavailable to other users; and
- system documentation will not be completed.

IS staff charged with maintaining this time entry system report that they are getting requests from various county departments for other time entry software products. The manager noted that he is unclear as to the "ownership" of the system and this has held them back from making substantive changes to this system, although it has not held them back from creating new versions at user requests. However, at this time IS staff has begun looking into creation of a new time entry system. The programmer charged with developing a new entry

system is soliciting requirements from users; he indicates that a new system will address the concerns expressed in our recommendations.

**We recommend** that the department consult with the Auditor's Office to determine what type of time entry system would be acceptable as a replacement for this CTE system. Consultations with user departments would be needed to work out specific department requirements; however, since this system feeds the payroll process, the Auditor's Office, who produces payroll for the county, should logically have a lead role in the development and roll-out of any time entry system (as they did when the payroll portion of HRMS was originally implemented).

**We recommend** that the department, *in developing or bringing in a new system*,

- ensure that proper system documentation exists that allows support staff adequate information to support and maintain that system – to include flowcharts of processes and other documentation on the essentials of the system;
- ensure that any system put into use contains adequate safeguards, including passwords that are restricted and not available to other users; and
- ensure that any system developed to replace the current time entry system be developed so as to contain efficiencies for users and those who need to maintain and support the systems, in addition to adequate internal controls to maintain the integrity, completeness, and accuracy of the time data.

Finally, **we suggest** the department examine having this time entry system under the same management as the rest of the time entry/payroll systems. Having the time entry system under another manager increases the likelihood of the system being viewed as a separate technical challenge, rather than being part of an overall payroll system that has an existing cross-departmental management structure; further it separates this portion of the payroll system from the strategic management of the system as a whole. This may have contributed to the current situation where the system has been neither fully documented nor re-written, but has been expanded to include three additional departments. This situation serves to increase the scale and consequences of any problems with the system that might occur, such as a failure to have reported time reach payroll so that employee paychecks can be created.

### **Reporting Capability: Efficiencies**

[Original recommendation May 2006]

We recommended that progress continue towards making report-generation available to users as a way to meet user's needs without

having IS staff develop each report for each user. This may require some in-house training by IS staff.

At the time of our original review, many county users reported that they were unable to generate needed reports on their own. Reports related to employee or payroll were only available from IS, HR, or FS and could not be generated ad hoc by managers in other departments. Ad hoc reporting created further inefficiencies for IS staff due to conflicting priorities in responding to user requests.

**Current Status:** IS reported that they now have a good sense of what reports are needed by departments. The problem log tracks all requested reports, and management monitors these on a routine basis. In addition, IS identified training needs for departmental staff; training has been provided to staff for one reporting tool that can be used to produce reports out of FMS.

**We commend** the work that IS has done in this area and encourage the department to continue providing appropriate and periodic training to users.

### **Disaster Planning: System Security**

[Original recommendation May 2006]

Disaster planning is a *security control* for any system containing critical county data such as the financial management and payroll systems. Over the past four years there has been increasing awareness on the part of IS and county management of the need to be able to re-initialize systems as one part of the county's overall disaster plan.

We encouraged IS to continue investigating options and strategies that would allow them to re-initialize systems in case of a disaster, making use of remote locations as necessary. We further encouraged IS and county management to work with departments to ensure each develops plans for manual operations – business continuity plans -- as well as addressing other disaster related considerations.

**Current Status:** IS has established an offsite location for back-up equipment and data that can be used to re-initialize systems in case of disaster. This is a first step in their planning to assist departments in being able to bring operations back on line.

We understand that the County has engaged an outside contractor to assist departments in the creation of business continuity plans that would include developing manual procedures that may be necessary in an emergency. This planning process should result in individual departmental plans that will also

identify “gaps” in critical processes that need to be filled. IS plans to bring on an infrastructure manager to assist with this.

**We commend** IS for their actions to date that better secure recovery efforts in emergencies, and we encourage the department to continue investigating options and strategies that protect the county’s ability to recover from a disaster or other emergency.

## **CONCLUSIONS**

Information Services continues work toward implementation of stronger controls over changes made to FMS. Work progresses slowly. Management has been unable to meet timeframes they have set for themselves that move them closer to a better controlled process that will help ensure processed financial data complies with requirements and is accurate, valid, and complete.

Management generally agrees with the findings in this report and indicates that they would welcome further review in six months to help ensure progress continues.

We appreciate the support and assistance of all staff in the FMS support group, along with that of the new manager. Management has actively worked to support improvements in system controls.

## **APPENDIX A: Objective, Scope, and Methodology of Work Performed**

Information Services' support for financial systems, including the Human Resources and payroll modules, has been reviewed internally twice over the past three years. Specifically, these were reviews of internal controls over any system or data changes. This report follows up on recommendations made in the previous two review memoranda.

Generally, a follow-up review requests updates on changes from the department under audit and does not result in additional audit testing. However, in this case, with the agreement of management, additional audit procedures were performed. For example, we looked at the staff roles and responsibilities in more detail because this information was not available during the period of our prior audit work. We also performed several audit tests to determine if procedures recently implemented were being followed by staff. We asked management to provide status reports and supporting documentation as appropriate; we interviewed staff and facilitated a control self assessment; we observed some of the new procedures in action; and we performed analysis of items in the problem log.

Work was performed between December 2006 and September 2007, in accordance with generally accepted governmental auditing standards, except for having required peer review.

## **APPENDIX B: Detail, Status, and Further Recommendations Regarding Change Management**

### ***List Approvers for Authorizing Changes***

[Original recommendation May 2005 and repeated in May 2006]

A list of authorized approvers should exist. The FMS support team, in conjunction with the system owners and users, should update the existing list of those individuals who have the authority to approve changes and to set priorities for FMS and to create approver lists for other systems, as needed. Approver lists should be available to those staff with responsibilities for making changes and updating information in the system to use in soliciting appropriate approvals for changes made to the system or to the data within the system.

**Current Status:** A list of authorized approvers was submitted to Information Services for their use and is now in place.

**We encourage** Information Services to maintain the list of authorized approvers and to periodically solicit updates.

### ***Log Data to Record Description of Changes Made***

In addition to ensuring that all changes are appropriately authorized, a change management system should also include logging an adequate description of the change so as to allow a person to re-create it, if necessary.

[Original recommendation May 2005]

Logs should contain adequate and consistent information. For example, logs should contain the date of request, requestor, authorization for a change, nature of the problem, actions taken to resolve the problem, date problem was resolved (change/solution moved from development to test, test to production, as applicable), and person performing the work. During our review we found that a specific spreadsheet, used to record work performed by IS staff, contained columns for these items, but they were either not filled in or they contained incorrect data (such as a name instead of a date). In reviewing HRMS/Payroll, we found one principle log used for all FMS issues. Information in this log was not consistent, and items were often closed without approvals or complete information on the nature of the changes.

**Current Status:** We found that the IS FMS support group is generally using the problem log to record all activities including changes made to the system. While management has provided detailed instructions/procedures for the completion of log entries, some fields remain incomplete, including the field for detailed information about the nature of the change made to the system.

Not all recommended data – date of request, requestor, assigned support person, type of problem, actions taken, date of closure, approval before movement to production -- are consistently provided in the log.

**We recommend** that log entries representing changes to the system should be completed with the requested information and that those parties responsible for the completion of selected fields be identified and notified of their responsibilities. Management indicates that log data will be complete by the end of 2007.

Note: There are other logs kept for patches and upgrades. We did not review these logs; patches and upgrades are normally well known and authorized. However, controls discussed above may also be appropriate for those kept for patches and upgrades.

### ***Review Periodically***

Supervisor or manager review of log entries helps to ensure that entries are completed appropriately and changes have been authorized.

[Original recommendation May 2005]

All logs used should be routinely and periodically reviewed by the supervisor or other management personnel for adherence to the defined use, and to determine completeness of information being recorded. This provides management with a tool over the change management process. Exceptions should be noted and the review should be annotated to establish an adequate audit trail. This step allows management to follow their own actions, to determine and assess skills, and to direct activities of the IS staff.

**Current Status:** It is our understanding that the function manager has been periodically and routinely reviewing problem log entries, with a concentration on those items that are open and of a high priority. Our review of closed log entries however, indicates that entries can be closed without appropriate log fields being completed and without adequate data to resolve the problem if it were to re-occur.

**We continue to recommend** that management review the logs on a periodic and routine basis. In addition, **we recommend** that management expand their review to include closed entries, to further ensure that adequate data is being provided. We understand this could be a time consuming activity if the scope was back several years, and that may not be reasonable. Management needs to assess risk, considering time per closed entry to resolve. Some entries may have greater significance, and if not adequately documented, even back to 2005, may require subsequent completion. All currently closed entries, and going forward could be reviewed.

### ***Control Log Access***

Within the current log, there is no delineation for access to fields within the database. So, for example, any user having the system on their computer can open or close an item in the log, even if that action is not authorized.

[Original recommendation May 2005]

Review access levels to ensure that only appropriate staff are allowed access to the logs. In some cases, IS may want to make these files read-only to some staff (such as for other users of the system for tracking purposes, audit (internal or external), or other levels of management), while still making them available for review to those needing to use them. Access levels should be documented and that documentation should be available as needed.

**Current Status:** In discussions with management, we agree that the security over the log itself is of lesser importance than ensuring that all appropriate data is captured related to changes made to the system or limiting access to production. We understand that the problem log is “restricted” to only those users who have been granted access.

However, **we continue to recommend** that the department consider securing segments within this problem log since the current version of the log allows anyone with access to the log to alter information within the log – to include approving an entry or closing an entry before work is completed. Approval fields, and those indicating movement to production could be restricted to use by selected individuals with authority to approve work.

### **System Documentation: Change Management**

As the department moves to a more formalized process for change management, it needs to document that process flow, to include procedures and requirements, along with management's expectations.

[Original recommendation May 2006]

We recommended that an adequate change management system be put into place to track all changes made to the system. If the problem log is to be used for this purpose, the fields should be better defined and there should be written procedures or on-screen guidance readily available to users, to help ensure that data is accurately and completely captured for future use. We recommended that management take an active part in the process and review log entries on a routine basis to help ensure that data is captured and problems and changes are being adequately addressed. Doing so indicates to staff the seriousness of the issues and management's intention that changes and problem solutions are captured.

**Current Status:** We conducted a control self assessment with the FMS support group and its management. From those sessions, a change management system was identified by the staff as a control for risk in many instances. Specifically, staff indicated change management as a control for

- Completeness of both records (being erased) and inaccurate reporting (from faulty patches);
- Accuracy from errors in both programming changes/upgrades and table changes/inaccurate rates;
- Security and Compliance for transactions being deleted instead of reversed;
- Compliance resulting from programming changes/upgrades; and
- Reporting where there could be a lack of reports for compliance.

We found a "change management manual" has been drafted and is now helping to guide the FMS support group's work. We did note some areas where additional clarity could be helpful; for example the document is silent on who should be responsible for completing fields in the problem log. As a result some fields are not completed before an item is "closed" in the log.

**We recommend** that the manual identify the roles and responsibilities for staff – both FMS support and department users – to help ensure that the log is completed appropriately.

Further, **we recommend** that IS implement a change management system across all applications and platforms to ensure that changes made

in any system are clearly documented and authorized, tested, and approved before placing them into the production environment.

### ***Define Staff Roles and Responsibilities***

A written definition of staff roles and responsibilities -- to include the level of access each staff has to the systems -- developed as part of the overall system documentation, can be a tool for management to identify proper separation of duties. The written roles help staff focus their activities on assigned responsibilities.

[Original recommendation May 2006]

In order to determine if there is adequate separation of duties between IS staff who create changes and those who put those changes into production, it is necessary to review staff roles and responsibilities, to include their levels of access to the financial systems. During the 2006 audit, we did not find any documentation of what staff roles and responsibilities were, and we were told that such a document was being generated.

We recommended that IS define the staff support roles as one piece of system documentation and more importantly as the Information Services' business plan for supporting all systems across the networks.

**Current Status:** We reviewed the document drafted on staff roles and responsibilities. We were told, however, that this document is not tied/linked to job descriptions that staff are currently working under as guild employees.

We learned that support staff do have access to both test and production environments. While generally programmer staff do not move changes into production, they have access to production. We learned that for some other applications there are separation of duties between the development of changes and the movement of approved changes into the production environment.

However, this is not uniform for all applications being supported by Information Services. In fact, of the over 65 applications supported by IS, most have little separation of duties between programmers and database administrators, who are generally charged with placing changes into production. Programmers often have access to the production environment – sometimes because the application does not have a test environment, or because it is more convenient for the support staff to have total access.

When appropriate separation of duties cannot be obtained – in some cases due to limited staffing levels, as management believes is true for FMS -- other means of monitoring staff activity, such as through exception reports that track activity within the system, should be developed and monitored by management.

**We recommend** that the department review staff access levels to determine if there are ways to separate duties, and if duties cannot adequately be separated, consider other options to prevent unauthorized changes to the system or the system data.

For example:

- developing exception reports that management monitors and reviews periodically;
- limiting access generally, but granting access to production for special needs; monitoring granted access until work is complete and access is again restricted;
- reconfiguring existing staffing in such a way as to effect better control over programmer access to production; or
- considering additional staffing if all other alternatives have been exhausted.