



# City of Houston

Annise D. Parker  
City Controller

**Municipal Courts Administration Department**

**Integrated Case Management System**

**Application Review**

**Report No. 2007-04  
September 2006**



OFFICE OF THE CITY CONTROLLER  
CITY OF HOUSTON  
TEXAS

ANNISE D. PARKER

October 10, 2006

The Honorable Bill White, Mayor  
City of Houston, Texas

SUBJECT: Municipal Courts Administration Department  
Integrated Case Management System Application Review (Report No. 2007-04)

Dear Mayor White:

In accordance with the City's contract with Jefferson Wells International (JWI), JWI has completed an Application Review of the Integrated Case Management System (ICMS) at the Municipal Courts Administration Department (MCAD). This review was requested by MCAD management so that any weaknesses in the application or with its implementation could be identified. The objectives of the engagement included:

- Assessing automated controls built into the ICMS application, focusing primarily on those related to the correct and reliable recording and posting of business transactions affecting general ledger accounts
- Validating that automated controls related to the business processes supported by the ICMS application are working as expected (operational perspective)
- Confirming that the posting of transactions entered, processed and reported by or thru the ICMS application adhere to the user requirements and expected results
- Confirming that the process to manage system security at the application, database and network level provide reliable controls to ensure data availability, confidentiality and reliability
- Assessing the segregation of duties established thru the implementation of access profiles and access privileges granted to them

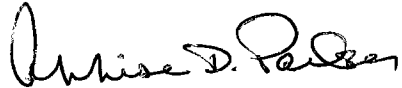
The report, attached for your review, identified various opportunities for improving internal controls supporting the operational and financial aspects of the processes supported by this information system. Key recommendations focused on the improvement of controls at the application, database, and network levels and areas in which segregation of duties and system security should be improved.

The findings and recommendations identified during the review are included in the body of the report. Draft copies of the matters contained in the report were provided to Department officials. The Views of the Responsible Officials as to actions being taken are appended to the report as Exhibit II.

Page 2

We commend Department management for their timely efforts to take action to remedy many of the deficiencies identified by JWI. We also appreciate the cooperation extended to the JWI engagement team by Department personnel during the course of the review.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Annise D. Parker". The signature is fluid and cursive, with the first name being the most prominent.

Annise D. Parker  
City Controller

xc: City Council Members  
Anthony Hall, Chief Administrative Officer  
Michael Moore, Chief of Staff, Mayor's Office  
Richard Lewis, Director & Chief Clerk, Municipal Courts Administration Department  
Berta Mejia, Presiding Judge, Municipal Courts Judicial Department  
Judy Gray Johnson, Director, Finance and Administration Department



October 3, 2006

Controller Annise D. Parker  
City Controller  
City of Houston  
901 Bagby, 8<sup>th</sup> Floor  
Houston, TX 77002

Dear Controller Parker:

We have completed the High Level Application Review of the Integrated Case Management System at the Municipal Courts Administration Department, as outlined in the engagement letter dated March 17, 2006, under contract No. 56545, approved by City Council Ordinance No. 04-1296.

This project was performed as a result of a request from the Municipal Courts Administration Department to the Controllers Office' Audit Division.

The attached report contains the result of our review. Our work does not constitute an audit conducted in accordance with generally accepted auditing standards, an examination of internal controls or other attestation or review services in accordance with standards established by the American Institute of Certified Public Accountants (AICPA). Accordingly, we do not express an opinion or any other form of assurance on the implementation or use of the Integrated Case Management System.

Jefferson Wells is pleased to have assisted the City Controller, and we appreciate the cooperation received during this engagement from the Municipal Courts Administration Department, as well as your office.

This report is intended solely for the information and use of the City, the Municipal Courts Administration Department, and the City Controller's Office, and is not intended to be used for any other purpose.

A handwritten signature in blue ink, appearing to read "Ernesto Reza-Garduno".

Ernesto Reza-Garduno  
Technology Risk Management Director

*Jefferson Wells is not a certified public accounting firm.*  
1000 Louisiana, Suite 5300 Houston, Texas 77002  
Telephone 713/860/3900 Fax 713/860/3902

# Table of Contents

---

EXECUTIVE SUMMARY .....1

    BACKGROUND .....1

    OBJECTIVES AND SCOPE .....2

    CONCLUSIONS .....2

    KEY RECOMMENDATIONS .....3

DETAILS OF FINDINGS AND RECOMMENDATIONS .....EXHIBIT I

MANAGEMENT RESPONSE – VIEWS OF RESPONSIBLE OFFICIALS .....EXHIBIT II

# EXECUTIVE SUMMARY

## BACKGROUND

The Municipal Courts Administration Department (MCAD) had been working with a third party provider (Maximus) towards the implementation of the Integrated Case Management System (a.k.a. ICMS or CourtView).

For many years, information systems supporting the City of Houston, Municipal Courts core business processes were not updated. These systems were old, paper dependent, labor intensive and not integrated. In addition, communication and transfer of information between departments supporting these core processes were not effective.

Based on the situation described above and other business decisions, in 2003 the City of Houston decided to acquire and implement an integrated system to support its judicial and administrative responsibility and other related processes. The information system that was selected by the City was the Integrated Case Management System, also known as CourtView. This information system was developed by Maximus, a third party provider, who was also hired by the City's Municipal Courts Administration Department to assist them with the implementation.

CourtView was selected because it is a real-time interactive Windows and Web browser-based information system that allows for the rapid creation of cases, linking of related cases, integrated receipting and automatic bookkeeping, imaging of documents onto magnetic or optical storage media, and scheduling of various court activities.

Through this application, case information is automatically updated at the time of data input, providing up-to-the-minute information about all aspects of the case. Case management functions allow court cases to be entered, updated, queried, and reported.

The desired outcomes of the project include:

- Better operational improvements
  - Improve data integrity, access and usability
  - Decrease time between citation issuance & disposition
  - Create a near paperless environment with document management
  - Improve business processes
- Increased public access to Court information
  - Allow phone access through the IVR system
  - Improve web payment ability
  - Permit public access to specific data
- Improved communication between City departments
  - Provide enhanced user access to case histories for MCJD, MCAD, Prosecutor and Houston Police Department (HPD)
  - Interface with HPD systems and City general ledger, and several external entities
  - Provide electronic document views to any City department, as necessary

In October 2005, the Parking module of the application was released into production, while the Traffic and Ticketing module was released into production on April 1<sup>st</sup>, 2006.

## OBJECTIVES AND SCOPE

The Municipal Courts Administration Department requested the Controller's Office Audit Division to perform a high level review of the application implementation. The objectives of this review were to:

- Assess automated controls built into the Integrated Case Management System (ICMS) application, focusing primarily on those related to the correct and reliable recording and posting of business transactions affecting general ledger accounts.
- Validate that automated controls related to the business processes supported by the ICMS application are working as expected (operational perspective).
- Confirm that accounting recording/posting of transactions entered, processed and reported by or thru the ICMS application adhere to the user requirements and expected results.
- Confirm that the process to manage system security at the application, database and network level provide reliable controls to ensure data availability, confidentiality and reliability.
- Assess the segregation of duties established thru the implementation of access profiles and access privileges granted to them.

The scope of our review included:

- Automated controls built-into the application and specifically those ensuring the appropriate and correct recording and posting of transactions affecting the general ledger and/or financial information.
- Application, Imaging Software and Database layers related to the ICMS automated application
- System security administration related to the ICMS application and databases supporting it.

The scope of our review did not include:

- Review of the General Computer Controls supporting this application (computer operations, change control, entity level IT controls, System Security (network level), physical security, disaster recovery, back up, etc).
- Review of the Data Conversion controls.
- Manual controls built into the business process supported by the application.

We conducted our review between May 5 and June 16, 2006.

## CONCLUSIONS:

Based on the analysis of available information, interviews developed with key personnel supporting this information system and the results of our testing procedures over key areas of control, we conclude that:

- a) System security at the application, database and operating system levels must be improved in order to ensure data and information confidentiality, security, integrity and availability. Controls in this area have not been fully implemented and/or are not in place at all. This situation exposes the City of Houston to unauthorized access, use and modification of information.

- b) The application was not fully implemented when it was released into production. Completing pending development and releasing it into production must be done promptly, but always following MCAD's change management process.
- c) No formal change control process is in place to ensure adequate segregation of duties between the third party consultant and MCAD Information Systems Group. Third party vendor without participation and/or knowledge of MCAD INFORMATION SYSTEMS GROUP can execute changes to programs and/or information in the production environment.
- d) Segregation of Duties has not been properly analyzed, documented and implemented, which increases the exposure to unauthorized transactions and fraud. Defined profiles in the application must be reviewed and improved or redefined, to impede the users of the application from performing actions outside their job description.
- e) Areas for improving controls related to the correct posting of general ledger transactions exist in the application (configuration) as well as the business process (monthly closing of the books and reconciliation).

## KEY RECOMMENDATIONS

During our assessment, we identified areas for improving internal controls supporting the operational and financial aspects of the processes supported by this information system. Our key recommendations are focused on the improvement of controls at the application, database, and network levels. In addition we identified critical areas in which segregation of duties and system security must be improved.

Our main recommendations are as follows:

- Generate a list of the deliverables originally agreed upon and not yet released into production, and have Maximus commit to a delivery schedule acceptable to MCAD, to ensure a complete implementation.
- Establish a transition process and plan to have Maximus provide knowledge transfer to MCAD staff, to eliminate the dependency on the vendor.
- Establish an effective and reliable change management process in which no segregation of duties conflicts exist. Currently Maximus has full access to modify, change, etc. programs in production which represent a high risk to system availability and exposure to unauthorized changes to data.
- Implement a control in the accounting process to ensure a month end process can only be executed once all Post Sets have been "Posted as Final".
- Modify the "CourtView to GL" monthly reconciliation process, to include the verification of Post Sets, to ensure no Post Set is missing from the closing month.
- Correct configuration inaccuracies, to avoid erroneous booking and distribution of money. i.e. 5 specific accounts associated to incorrect Payee Names.



- Ensure that all digital signatures used by the application are correctly linked to and can only be accessed by their owners, to prevent that official documents are wrongly stamped with incorrect signature or that unauthorized personnel are using those signatures without proper approval.
- Formalize, implement, communicate and enforce Security Policies and Procedures reflecting MCAD expectations regarding use, protection and availability of information technology assets and services.
- Develop Segregation of Duties and Lethal Combination matrices to help in the definition of user profiles without conflicting access.
- Remove unnecessary users from the production environment, and delete functionality assigned to users and user profiles that is not required for their roles and responsibilities.

Details of our findings and recommendations are in Exhibit I, attached.

## **DETAILS OF FINDINGS AND RECOMMENDATIONS**

**AUDIT OBJECTIVES:** Assess automated controls built into the Integrated Case Management System (ICMS) application, focusing primarily on those related to the correct and reliable recording and posting of business transactions affecting general ledger accounts. Confirm that accounting recording/posting of transactions entered, processed and reported by or thru the ICMS application adhere to the user requirements and expected results.

- 1. The CourtView application currently allows a large number of MCAD personnel to close cases, even if monies are outstanding from the defendant.**

MCAD personnel are dismissing, closing and deleting cases in CourtView, even if monies are outstanding. As of 6/5/06, the "Case Closed and Money Owed Report" lists thousands of closed cases with payments outstanding totaling \$1,944,696.58.

While the functionality to dismiss and close cases is necessary for the normal operation of Municipal Courts, having this functionality available to people that do not require it becomes a risk, as they would be able to perform such functions outside their responsibility.

In order to minimize this risk, we recommend the Business Process Owners (BPO's) authorize the designation of this functionality only to those people who require it for the execution of their work. In addition, we recommend MCAD System Support develop a report for monitoring transaction usage and that Assistant Directors (AD's) review this report daily to ensure that only authorized cases have been closed or dismissed.

- 2. The monthly reconciliation performed by MCAD's Public Services does not ensure that all CourtView information for the month is included.**

A monthly reconciliation between CourtView and the GL is in place. This reconciliation is used to validate that information sent from CourtView to the GL Application is included in the monthly report received from the GL application. However, it does not ensure that all CourtView information for the month has been sent to the GL. The risk in this case is that some information may be left in CourtView and not transmitted to the GL, remaining unnoticed.

This risk was materialized in the month of April 2006, where a Post Set for April 27<sup>th</sup> was left in CourtView as "In Cashbook Maintenance", totaling \$1,153,401.96. As of June 8<sup>th</sup>, when we reported this issue to MCAD System Support Assistant Director (AD) and MCAD Public Services AD, the mentioned Post Set was still pending.

To eliminate the above mentioned risk, we recommend MCAD's Public Services adjust their reconciliation process and include the verification that all information for the month has been sent to the GL application

### 3. The CourtView interface to the GL does not utilize sub-account numbers in this process.

The CourtView interface to the GL changes the account numbers for accounts 8100 and 8105 to 810010 and 810510, respectively. Further analysis showed that detailed classification is missing in CourtView's Chart of Account for accounts 8100, 8105, 8115, 8120 and 8125. The impact of this issue is that the transactions are presented in the wrong classification at a sub-account level.

We recommend MCAD's System Support correct the interface program in CourtView, to manage the transactions at the sub-account level.

### 4. Maximus configuration contains inaccuracies that can impact the posting and distribution of money.

CourtView is a large and complex application, which required a significant level of effort for its configuration. We reviewed various configuration tables, but our main focus was the review of those related to the financials of the application.

We identified the following configuration errors, which were reported immediately to management:

- 5 incorrect Payee Names, associated to specific accounts. The amount associated to these accounts in the month of April is \$14,883.71.
- 1 CourtView account associated to a GL code that corresponds to the wrong agency.
- 767 Fines have the concept "Warrant Issue Fine" instead of "Local Arrest Fee". Warrant is associated to the account 262900 (State of Texas) and Arrest to 817700 (City of Houston).

State of Texas disbursements occur on a quarterly basis. The disbursement for the first quarter of 2006 was done out of the old system.

Although no financial impact has been materialized as of June 14, 2006, we recommend MCAD's Public Services analysts responsible for CourtView's configuration fix these errors, as well as any subsequent economical impacts.

### 5. Business Process Flows are not documented.

The application was configured based on 195 scenarios documented by Assistant Directors (ADs) or their designees, which were representatives of the different areas of Municipal Courts. These scenarios were used as the specifications from the Business Process Owners (BPO's).

In reviewing the scenarios, we observed that each one covers a portion of what could be considered a business process flow. We were advised that, due to the complexity of the business processes and the functional approach to analyze them, complete business process flows were not documented.

Having business process flows documented allows for the analysis of controls (present and absent) throughout the process. In addition, by not having business process flows documented, there is a high possibility of missing parts of the process, which would only be identified after the application is released into production.

We recommend that MCAD charter a multidisciplinary team to document the business process flows supported by this application and analyze the internal controls associated to these processes. This activity should be developed once the application is stabilized in the production environment, in order to reflect the actual business process in place.

**AUDIT OBJECTIVE: Validate that automated controls related to the business processes supported by the ICMS application are working as expected (operational perspective).**

**6. The CourtView application was released into production before proper completion of the System Development Life Cycle Process.**

During our review we observed that important functionality of the application supporting specific business processes was not ready when the application was released into production, as we explain below.

The application has ticklers that monitor certain conditions and react based on specific events/conditions. One of these ticklers is to identify tickets that need to be sent to the outside collectors "Linebarger" when they become delinquent. As of June 14, 2006, the ticklers had not been activated yet.

On a quarterly basis the City of Houston has to disburse to the State of Texas the money collected on their behalf. Before authorizing the distribution, the financial group needs to run a report that provides them with the information required for their validation. We attempted to run the report from the application's menu, but the process did not run. We then requested the IT group at MCAD to run the report for us and we were informed that the report was still under development.

Please note that, as a result of these processes not being in production, we were not able to validate them.

We recommend MCAD System Support and Maximus to prepare a document containing a list of deliverables agreed upon and not yet released into production, as well as a final work plan to obtain such deliverables.

**7. CourtView application allows for the closing of a month, without validating proper completion.**

Accounting in CourtView is managed by Post Sets. A Post Set is the equivalent of an accounting batch. CourtView has no restriction on the number of daily Post Sets, as the control is by date and time; the date and time for the closing Post Set is the same as for the next opening one.

Once a Post Set is closed, it is validated by CourtView and set as "Posted as Final" if it is ok, or set as "In Cashbook Maintenance", when issues are found, to allow for its correction.

On April 27th, at 23:46:32, a Post Set was closed and left as "In Cashbook Maintenance", for a total of \$1,153,401.96, and CourtView did not impede the execution of the Month End process. This Post Set was still pending when we reported this point to management on June 8th.

We recommend that MCAD System Support formally request Maximus to develop an automated control in CourtView validating that all Post Sets for the month have been posted before allowing the execution of the monthly processes.

#### **8. Digital signatures stored in CourtView are linked to the wrong person.**

The application uses digitalized images of the signatures of certain MCAD personnel. These signatures are associated to their owners through the user id in CourtView and are stamped to official documents as their signatures.

The risk of a wrong association of a user id with a signature is that a person would be signing official documents with someone else's signature. Our review showed 9 active user accounts in CourtView linked to the wrong signature.

We recommend MCAD's Help Desk correct the above mentioned signature linkages.

#### **9. Segregation of duties is not in place for the Change Control Process.**

The Traffic and Ticketing module of the CourtView application went live on April 1, 2006. Under normal conditions, at Go Live the vendor hands the application to local staff, and supports their work from a test environment.

As of June 14, 2006, Maximus was still in full control of the application and the production environment.

By having full control, Maximus staff can release changes into production without any documentation and without approval from MCAD. They can also input, alter or delete transactions from production without leaving an audit trail.

We recommend MCAD System Support implement a reliable segregation of duties in the change control process ensuring that only authorized programs and data changes are made. MCAD System Support personnel should also develop a "gate keeper" role for the change control process. This individual will be responsible for transporting the changes to the production environment once all control and quality assurance activities for such a change have been properly executed, documented and approved. A key control activity is the formal authorization of the process owner and/or primary end-user affected by the change. Such authorization must take place after executing testing procedures by this individual in the testing environment.

If required, the Change Management Policy and procedures should be updated and communicated to all parties related to the request, development, testing and acceptance of changes to items in the production environment.

Because of the recent release of the CourtView application into production, and the amount of pending corrections and enhancements, we also recommend that MCAD System Support group implement emergency procedures that allow for controlled corrections of elements in the production environment during un-planned and/or urgent conditions.

**10. Maximus has not defined and implemented a transition process to transfer knowledge and control of the application to MCAD's System Support.**

In order for MCAD System Support to take control of the production environment, training and knowledge transfer is required.

According to interviewed IT staff, Maximus has not transferred knowledge to MCAD System Support personnel, which results in a high dependency on the vendor and frustration on MCAD's System Support own personnel.

We recommend MCAD System Support group to request a formal transition plan from Maximus. This transition plan should include the required training and documentation that allows MCAD System Support to take full operational and maintenance control of this application in the production environment.

**AUDIT OBJECTIVE: Confirm that the process to manage system security at the application, database and network level provide reliable controls to ensure data availability, confidentiality and reliability.**

**11. The Municipal Courts Administration Department (MCAD) does not have documented Security Policies and Procedures.**

MCAD does not have documented Policies and Procedures that define the organization's expectations regarding use and access of Information Technology Assets and information. MCAD's Help Desk staff members are currently writing security procedures to support their function, but there is no plan or deadline for completion.

The lack of formal policies and procedures exposes MCAD to unauthorized use of IT Assets and / or lack of prevention of IT exposures and risks.

We recommend MCAD's System Support AD or his designee to develop, communicate and enforce Security Policies and Procedures. We also recommend MCAD's System Support and specific process owners analyze and document access requirements assigned to each end-user (user-id). The implementation of this approach will ensure adequate protection of data and proper segregation of duties. In addition, MCAD System Support group should provide each process owner, at least on a quarterly basis, with an access security report in which all user-ids and access granted to them are reported. The process owners should review this report leaving evidence of such activity and identifying and correcting any issues regarding segregation of duties and/or access not longer needed for the specific user.

**12. System Security at the application, database and network level is not properly defined.**

The results of our security reviews of CourtView, Oracle Data Base and Network are:

- No restrictions assigning Super User profiles. The Developer and Administrator profiles in CourtView have Super User privileges (configuration and business transactions); a total of 29 User Ids have one of these profiles assigned.
- Users blocked in CourtView but active in Oracle, and vice versa.



- Users blocked in both, CourtView and Oracle.
- Active user ids present in CourtView, Oracle, or both, for terminated employees.
- Large number of generic user ids.
- Passwords at Oracle and CourtView level can be of 1 character. Password at network level is not required.
- CourtView users are not required to change their password at first login. 58 users still have the default password.
- Strong password is not enforced at the Oracle or Network layers.
- There is no automatic logoff after inactivity in CourtView. While the application does not provide for this functionality, this could be accomplished through Oracle.
- User accounts are not locked after failed attempts for the network, CourtView or Oracle.
- Oracle DBA functions in production are the responsibility of personnel of the vendor.
- CourtView does not have security logs / audit trails.

We also observed weaknesses in the security configured towards data protection, as we were able to surf throughout the network with a non-powerful user, and gain access to the application servers and other areas that must be fully protected (i.e. access to the directories where all electronic signatures are stored).

While this may be the result of not having security policies and procedures, the risk is extremely high.

We recommend that MCAD System Support enforce security measures provided and available at the operating system, database and application layers to properly protect data and information technology infrastructure and processes.

We also recommend MCAD System Support enable audit trails and logs at the database level. This information could then be analyzed on a regular basis by the DBA and the MCAD Help Desk (group currently performing security administration for the CourtView application) and identified issues could be addressed.

**AUDIT OBJECTIVE: Assess the segregation of duties established thru the implementation of access profiles and access privileges granted to them.**

**13. Segregation of Duties and Lethal Combination matrices have not been defined and users have excess privileges.**

A very important element of the security is the Segregation of Duties (SOD). This is to help ensure that users only have access to what they need to, and that the assigned privileges do not allow them to perform illegal / unauthorized transactions.

To help analyze segregation of duties, a SOD Matrix should be present indicating who should have access to what. It should also indicate the lethal combinations that can exist in the application, to allow the security administration to monitor assigned functionality, and to ensure lethal combinations are not given to anyone.

For the implementation of CourtView, MCAD incorporated a team called the "SCHAPE Team", who analyzed the application functionality and created the profiles, keeping in mind the SOD. We analyzed the defined profiles and the functionality assigned to them. We also interviewed members

of the SCHAPE team, as we were informed that they decided the access to be granted to each profile.

Our analysis of the SOD indicated the following:

- Documentation resulting from the work performed by the SCHAPE team was not available.
- Evidence of the sign-off on the security access granted in production before going live was not provided.
- The rules to assign Case Types and Screen Functions have not been documented.
- A Segregation of Duties Matrix to highlight case types and screen functions is not present.
- A Lethal Combination Matrix in relation to screen functions does not exist.

Since these elements are necessary for the ongoing work of the Help Desk to perform the security administration functions, we recommend the MCAD's SCHAPE team, assisted by a subject matter expert in the assessment of SOD conflicts, develop a Segregation of Duties and a Lethal Combination Matrices.

We also recommend that the Business Process Owners perform a quarterly review of the users and user profiles, in order to ensure that no segregation of duties conflicts exists.



## EXHIBIT II



**CITY OF HOUSTON**  
Municipal Courts Administration  
Department

**Interoffice**

Correspondence  
RL-5-2025.3

To: Annise D. Parker, City Controller

From: Richard Lewis *RL*  
Acting Director and Chief Clerk,  
Municipal Court Administration

Date: September 14, 2006

Subject: Response to Jefferson Wells Audit of ICMS

Ms. Parker,

The Municipal Court Administration Department (MCAD) requested that an audit of its new Integrated Case Management System ("ICMS") be included in the Controller's FY06 Internal Audit Plan, so that any weaknesses in the application suite or with its implementation could be surfaced shortly after the system came live and prior to acceptance testing. Our goal was to ensure that the Court resume normal operations as quickly as possible.

We address each finding/recommendation in the pages that follow, and agree with most of Jefferson Wells' ("JWI") findings. In many cases, we have already taken action to remedy deficiencies JWI brought to our attention during their field work.

In general, the Court will manage JWI's findings/recommendations using the following process:

- Review and respond to each finding/recommendation
- Analyze and prioritize each finding/recommendation
- Determine how best to address each finding/recommendation (initiate resolution)
- Develop a work plan (tasks, staffing, timeline, resources) for addressing each initiative
- Task staff with responsibility for implementing each plan
- Track status of each initiative
- Report periodically on progress being made

I believe this approach will ensure careful consideration and appropriate action for each finding/recommendation.

I would like to acknowledge JWI both for their fine work and for their patience as we worked to bring a very complex system on-line. The audit project was postponed several times; because, we felt strongly that ICMS should be live before JWI began auditing functionality and configuration.

Because ICMS did not go-live until April 1, 2006, because FY06 ended on June 30, 2006, and because we are still stabilizing the system at this writing, JWI never saw the entire system functioning as designed. Fortunately, they did see most of the day-to-day operations, and their findings and recommendations have given the Court an excellent starting point for improving the way we use the new system to do our business.

**Management Response  
Views of Responsible  
Officials**

## EXHIBIT II

### Summary Response

The outline that follows summarizes JWJ's objectives & findings and the Court's response to each.

Note: The outline is formatted as:

- JWJ Audit Objective
  - JWJ Audit Finding
    - Court Summary Response (Agree, Disagree, Agree with Exceptions)
  
- Assess automated controls built into the Integrated Case Management System (ICMS) application, focusing primarily on those related to the correct and reliable recording and posting of business transactions affecting general ledger accounts. Confirm that accounting recording/posting of transactions entered, processed and reported by or thru the ICMS application adhere to the user requirements and expected results.
- The CourtView application currently allows a large number of MCAD personnel to close cases, even if monies are outstanding from the defendant.
  - Agree: A report was developed so the Court Management Team could identify and correct, on a daily bases, any case that was closed inappropriately.
- The monthly reconciliation performed by MCAD's Public Services does not ensure that all CourtView information for the month is included.
  - Agree with Exceptions: Monthly reconciliation does not identify missing post-sets; however, the Management Team and the MCAD Accounting group were aware of one open post set that was created for backlog (4/27). CourtView will not allow supervisors to pass over open post-sets.
- The CourtView interface to the GL does not utilize sub-account numbers in this process.
  - Agree: Account coding was corrected by MCAD Accounting group.
- Maximus configuration contains inaccuracies that can impact the posting and distribution of money.
  - Agree: MCAD Accounting group has corrected known account/payee setup issues.
- Business Process Flows are not documented.
  - Agree with Exceptions: Court has not fully defined and formally documented all business process flows. During configuration, however, Court staff defined 140 business "scenarios" (including swim lanes) which are "strung" together to make processes.
  - Once the system is stable, the System Support Process Management Team will work with Court operational units to review and revise scenario documentation, and compile that documentation into a published set of business processes (including process maps).

*Management Response  
Views of Responsible  
Officials*

## EXHIBIT II

- Validate that automated controls related to the business processes supported by the ICMS application are working as expected (operational perspective).
- The CourtView application was released into production before proper completion of the System Development Life Cycle Process.
  - Agree with Exceptions: The life cycle for software implementation was the basis for initial planning of the ICMS project, but numerous complications inhibited the Project Team's ability to execute the plan as expected.
  - It would be more accurate to say that the Life Cycle Process was followed throughout the implementation, but that poor results did not stop the project.
  - The following outline describes each step in the System Development Life Cycle, whether the activity was undertaken, who was involved in the work, and the Court's assessment of how well it appears the work was done (good/fair/poor).

• Project planning, feasibility study	Done	Court/Deloitte	Fair
• Systems analysis, requirements definition	Done	Court/Deloitte	Good
• Systems design: Implementation	Done	Court/Maximus	Poor
• Integration and testing	Done	Court/Deloitte	Fair
• Acceptance, installation, deployment	Working	Court/Maximus	?
• Maintenance	Pending	Court/Maximus	?
- CourtView application allows for the closing of a month, without validating proper completion.
  - Agree with Exceptions: Monthly reconciliation does not identify missing post sets; however, the Management Team and the MCAD Accounting group were aware of one open post set that was created for backlog (4/27). CourtView will not allow supervisors to pass over open post-sets.
- Digital signatures stored in CourtView are linked to the wrong person.
  - Systems Support Division was made aware of this situation during the initial audit period and has taken steps to ensure both that signatures are properly linked and that signatures are better secured against unauthorized access.
- Segregation of duties is not in place for the Change Control Process.
  - Disagree: The Court has put a formal change management process in place that ensures that:
    - No one has authority to modify the system's configuration without permission,
    - All changes are documented, reviewed and approved by the Court's Systems, Change, Help, Application, and Process Experts (SHAPE Team) before implementation,
    - Authorization to modify the system in production is granted to a defined individual for a limited period, to make the approved change.
  - This process may have become more robust after JWJ's field work was completed.
- Maximus has not defined and implemented a transition process to transfer knowledge and control of the application to MCAD's System Support.

**Management Response  
Views of Responsible  
Officials**

## EXHIBIT II

- Agreed: Prior to the start of any acceptance testing, the Court has required that Maximus transition both knowledge and control over all aspects of the system to the System Support Division.
- MCAD System Support has recruited staff to assume these responsibilities. This staff has been working with HP-UX and Oracle administration tools, and is becoming more familiar with the ICMS environment.
- At this writing, Maximus has not yet prepared a transition plan.
- Confirm that the process to manage system security at the application, database and network level provide reliable controls to ensure data availability, confidentiality and reliability.
- The Municipal Courts Administration Department (MCAD) does not have documented Security Policies and Procedures.
  - Agree with Exceptions: MCAD does have written policies and procedures governing security. During the audit period, these procedures, however, had not been updated to reflect security procedures for the new system. While approval forms and procedures have been reviewed and revised, numerous procedures have not been updated.
  - Once the system is stable, the System Support group will review and revise all security policies and procedures to ensure that they are complete and effective, and that they conform to all City-wide security policies.
  - Security policies and procedures will be reviewed during the annual external audit to ensure they remain current.
- System Security at the application, database, and network level is not properly defined.
  - Agree with Exceptions: Application security has been setup to conform to the needs of the user community, as defined by the Assistant Directors.
  - Because of the application architecture, database security follows application security and has been created according to the same guidelines.
  - All aspects of network security, other than user adds/changes/deletes, are handled by the City's IT Department.
  - JWI advised the Court of inconsistencies between the application and database users and permissions, and of the presence of generic logins. System Support has taken action to reconcile these differences, to eliminate generic login ids, and to restrict "external" access to the database.
- Assess the segregation of duties established thru the implementation of access profiles and access privileges granted to them.
  - Segregation of Duties and Lethal Combination Matrix have not been defined and users have excess privileges.
    - Agree with Exceptions: The Court has not, but will, define and document formal Segregation of Duties and a Lethal Combination Matrix.
    - However, segregation of duties is an integral part of the Court's division of labor and organizational structure and was, therefore, implicit in permissions granted to all users.

**Management Response  
Views of Responsible  
Officials**