State of Colorado
Office of the State Auditor

Colorado Judicial Department's Integrated Colorado Courts E-Filing and Judicial Paper on Demand Systems

Independent Verification and Validation Review

July 2012

WDS WYANT DATA systems, inc.

245 Century Circle •Suite 106•Louisville, Colorado •Tel 303 604 6254•Fax 303 665 4453

[This page intentionally left blank for reproduction purposes]

LEGISLATIVE AUDIT COMMITTEE
2012 MEMBERS

Representative Cindy Acree
Chair

Representative Angela Williams
Vice Chair

Senator Lucia Guzman
Representative Jim Kerr
Senator Steve King

Senator Scott Renfroe
Representative Su Ryden
Senator Lois Tochtrop

Office of the State Auditor

Dianne E. Ray
State Auditor

Jonathan C. Trull
Deputy State Auditor

Manjula Udeshi
Legislative Audit Manager

Julie Chickillo
Legislative Auditor

Wyant Data Systems, Inc.
Contract Auditors

[This page intentionally left blank for reproduction purposes]

WDS WYANT DATA
systems, inc.

245 Century Circle, Ste. 106
Louisville, CO 80027

July 2, 2012

Members of the Legislative Audit Committee:

This report contains the results of an independent software verification and validation assessment of the Judicial Department's development of the Integrated Colorado Courts E-Filing and Judicial Paper on Demand systems. The assessment was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits and assessments of all departments, institutions, and agencies of state government. The State Auditor contracted with Wyant Data Systems, Inc., to conduct this assessment. The report presents our findings, conclusions, and recommendations, and the responses of the Judicial Department.

Respectfully submitted,

T.D. Villani

Thomas D. Villani - Vice President, Business Services
Wyant Data Systems, Inc.
245 Century Circle, Ste. 106
Louisville, CO 80027
Phone: (303) 604-6254
Direct: (303) 376-4443

[This page intentionally left blank for reproduction purposes]

TABLE OF CONTENTS

PAGE

PAGE

Definition of Terms and Abbreviations

Agile – A commonly used description of software development methodologies that have evolved in the past 10 to 15 years as ways to improve the overall success and efficiency of software development projects. The agile methodologies generally employ incremental and iterative approaches to the development life cycle. Agile methods include very high levels of communication and involvement by business stakeholders, as well as continuous refinement of project goals and requirements. Some adjectives that are often used to describe agile methods include adaptability, transparency, visibility, and simplicity. The agile principles that have worked well in software development methodologies have recently inspired similar movements in project management methods and general business approaches.

Application Development Stage – One of three phases defined in the Governmental Accounting Standards Board (GASB) Statement No. 51, in which GASB categorizes the development of software. This stage includes software configuration and interface design, coding, installation of hardware, testing, and data conversion. Current industry best practices for software development have the “phases” or “stages” defined by the GASB statement overlapping and happening concurrently in an iterative approach.

Burn Charts – Burn charts, “burnup” and “burndown,” are used in agile project management such as SCRUM to track the amount of work completed or the amount of work remaining.

Cactus – A simple unit testing framework for server-side Java code.

Change Advisory Board - The primary purpose of the Change Advisory Board (CAB) is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes in order to minimize the impact of change-related incidents upon service quality, and consequently improve the day-to-day operations of the Department’s IT infrastructure.

Configuration Management – The process of identifying and defining the components of the information system requiring control and management, controlling the release of the components during the system life cycle, documenting and reporting the status of configuration components and change requests, and verifying the completeness of the configuration items.

Functional Requirement – A requirement that specifies a function that the information system must be capable of performing.

ICCES – Integrated Colorado Courts E-Filing System.

ICON/Eclipse – The statewide case management system used by Colorado state courts since 1997.

IEEE – Institute of Electrical and Electronics Engineers. IEEE is the professional association responsible for establishing and maintaining the international standards for performing software verification and validation assessments.

IV&V – Independent Verification and Validation. Software verification and validation is a systems-engineering discipline designed to build quality into the application software during the software development life cycle. An IV&V assessment is considered independent when the agency performing the assessment is not under the control of the organization that is developing the software.

Definition of Terms and Abbreviations

jPOD – Judicial Paper on Demand.

JUnit – A regression testing framework for the Java programming language.

Preliminary Project Stage – One of three phases defined in the Governmental Accounting Standards Board (GASB) Statement No. 51, in which GASB categorizes the development of software. This stage includes determination of system requirements, development of alternatives, vendor demonstrations of their software, evaluation of alternatives, and final selection of alternatives.

Requirements Traceability Matrix (RTM) – A standard software development matrix used to track the life of a requirement and providing bidirectional traceability between various associated requirements. Used to find the origin of each requirement and track every change that was made to the requirement. The traceability matrix can also tie use-cases to the code that implements the use-case and allows impact analysis when defects are discovered and fixed.

SCRUM – Name of a current agile project management methodology.

Unit Testing/– Testing conducted to find errors, better known as "bugs," in the code unit/module. Unit testing can be done by developers or testers. Modern development practices typically use automated unit test frameworks where code is written specifically to test the interfaces and function of code that becomes part of the system. The advantage of automated unit test frameworks is that the tests on the whole system can be run repeatedly with little effort to ensure that modifications to the code base do not have unintended impacts on other system areas.

User Acceptance Testing– In this type of testing, the developed product is handed over to the user/paid testers to test the software in a real-time scenario. The product is validated to find out if it works according to the system specifications and satisfies the requirements.

Use-case – A use-case is a method of defining a way in which a system will be used. In many current object-oriented analysis and design methodologies, primarily the "unified modeling language", use-cases are the method for defining functional requirements of a system. They are typically defined in a way that describes how an actor (either a person or an external system) will interact with the system to produce some desired end result. Use-cases are not always identical to "stories," though they are similar in their statements.

User Story – User stories are narrative texts that describe an interaction of the user and the system, focusing on the business value a user gains from the system.

WDS WYANT DATA systems, inc.

IV&V JUDICIAL DEPARTMENT ICCES/JPOD

PURPOSE

Conduct an independent verification and validation review of the Colorado Judicial Department's (the Department) Integrated Colorado Courts E-Filing System (ICCES) and Judicial Paper on Demand (jPOD) system development projects.

BACKGROUND

- In 2009, the Department obtained the necessary authorization and appropriation to build a new, in-house e-filing system known as ICCES.
- ICCES and certain modules of jPOD need to be ready by January 1, 2013, to replace the current vendor e-filing system.

OUR RECOMMENDATIONS

The Department should:

- Take immediate steps to comply with State cyber security policies and related statutory provisions by maintaining an up-to-date cyber security plan and performing a security risk assessment and vulnerability scans.
- Strengthen its project management practices.
- Ensure a smooth transition to enterprise-level application support for ICCES and jPOD system.
- Implement a strong quality control assurance program.
- Reevaluate and reassess its capacity planning and infrastructure performance based upon the projected utilization and capacity needs of ICCES and jPOD system.
- Ensure that project costs are appropriately capitalized as required by accounting principles.

OVERALL CONCLUSION

The Judicial ICCES/jPOD system development projects are following best practices to ensure the successful outcome managerially, financially, and technically.

KEY FACTS AND FINDINGS

Overall, based on an industry proven assessment methodology, WDS concluded that the Department faces a low to medium risk of failure for the ICCES/jPOD development projects. On a high level, a project is considered a failure when it cannot be delivered as intended.

- The Department does not maintain an up-to-date cyber security plan, is noncompliant with statutes, and is delinquent in performing a security risk assessment and vulnerability scans (since 2009).
- The Department does not have documented project artifacts and processes as recommended by industry best practices to help ensure that activities related with project scope, schedule, and budget are monitored and controlled.
- The Department does not have adequate policy, procedures, and plans to operate the ICCES and jPOD systems at an enterprise-level.
- The Department does not have a quality assurance plan and currently is not able to support configuration management functions.
- The Department did not perform a complete capacity/performance assessment of established hardware architecture for ICCES and jPOD.
- The Department did not capitalize the software development cost for ICCES/jPOD as required by accounting principles.

[This page intentionally left blank for reproduction purposes]

RECOMMENDATION LOCATOR
Agency Addressed: Judicial Department

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
1	15	Take immediate steps to comply with State cyber security policies and related statutory provisions by (a) developing a robust set of implementation plans, practices, and guidelines as outlined in State cyber security policies; and (b) performing a periodic vulnerability, threat, and risk assessment of the Judicial Department's policies, procedures, systems, and network infrastructure.	a. Disagree b. Partially Agree	b. September 2013
2	19	Strengthen the Judicial Department's project management practices by (a) generating and/or improving project documentation artifacts as well as tracking and documenting project activities;(b) collecting project metrics and perform "earned value analysis" or an equivalent metric on the project so that the exact status of the project based on fine-grained work breakdown can be reported to any interested stakeholders on a regular (minimum monthly) basis; and (c) tracking actual versus planned effort by adopting a more standardized software development methodology such as an agile process like SCRUM.	Agree	a. September 2013 b. January 2014 c. January 2014
3	22	Ensure a smooth transition to enterprise-level application support for ICCES/jPOD by (a) developing, staffing, and managing plans to support the Judicial Department's transition to an enterprise service model with 24-hour support operations; (b) developing and maintaining service level agreements with users of ICCES/jPOD; and (c) developing or enhancing documented operational processes and procedures that address specific sub-processes.	Agree	a. October 2012 b. September 2013 c. September 2014

RECOMMENDATION LOCATOR
Agency Addressed: Judicial Department

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
4	25	Implement a strong quality control assurance program by (a) developing a Requirements Traceability Matrix and performing a traceability exercise to link use-cases to business rules; (b) reviewing the business requirements rules of each component of development; (c) developing additional requirements, design specifications, use-cases, and test scripts; (d) developing testing mechanisms and processes that ensure creation of a unit testing framework, performing extensive system testing, documenting the confirmation from sponsors/stakeholders that the system satisfies the approved requirements, and developing tests to evaluate pre- and post-conditions; (e) developing a configuration management plan to incorporate an agile method process and project management measurements; and (f) establishing an independent quality assurance role or function to oversee quality management and compliance.	a. Agree b. Partially Agree c. Partially Agree d. Agree e. Partially Agree f. Agree	a. September 2013 b. September 2013 c. September 2013 d. July 2013 e. June 2013 f. February 2014
5	30	Reevaluate and reassess the Judicial Department's capacity planning and infrastructure performance based upon the projected utilization and capacity needs of ICCES/jPOD including (a) revisiting system architecture, i.e., the hardware and network supporting ICCES/jPOD system; and (b) developing plans for load/pilot testing and validating the system capacity and capability.	Agree	August 2012
6	32	Ensure that project costs are appropriately capitalized as required by established accounting principles by (a) establishing a plan to capitalize the project in the correct accounting period and re-stating financial records as needed; and (b) estimating and recording the value of the project on an annual basis since the preliminary stage of the project.	Agree	a. August 2012 b. April 2013

Overview of ICCES/jPOD System Software Development Project

Overview

Colorado's court system consists of the Colorado Supreme Court, the Court of Appeals, district courts, the Denver probate and juvenile courts, and county courts. All of these courts are funded by the State, with the exception of Denver's county courts which is funded by the city and county of Denver. The supreme court justices, who are responsible for overseeing the regulation of attorneys and the practice of law in Colorado, appoint a State Court Administrator to oversee the administration of the Judicial Department (the Department) and provide administrative and technical support to the courts and probation.

For Fiscal Year 2012, the Department was appropriated $370 million and 3,493 full-time equivalent staff.

Background on the Department's Development of Major Information Technology Systems

In Fiscal Year 2011, approximately, 337,000 civil cases were filed in the state court system, including 200,000 (59 percent) in county courts, 126,000 (37 percent) in district courts, 10,000 (3 percent) in small claims county courts, and 1,000 (1 percent) in civil cases in the court of appeals. For each of these cases, the parties involved, or the parties' legal representatives, are required to file legal documents such as pleadings, discovery requests, or exhibits with the courts. Today, approximately 96 percent of all civil documents that can be e-filed are e-filed in the district courts across Colorado.

To address the high costs of receiving, retrieving, copying, and mailing court documents, the Department issued a request for proposal for a vendor-based electronic document management system, also known as an e-filing system. In 1999, the Department selected a third-party vendor to implement the e-filing system. The resulting e-filing system was piloted in July 2000 and implemented statewide in district and county courts by February 2001, in county court (money and eviction case types) in early 2007, and in the Court of Appeals in July 2008. According to the Department, the system has made it easier and cheaper for attorneys to file cases, increased the speed and reliability of retrieving documents, reduced the time required to distribute court orders, and reduced court staff workload. The current contract for the e-filing system expires December 31, 2012.

In April 2008, the Joint Budget Committee requested that the Department study the feasibility of implementing the e-filing system in-house, as opposed to using the third-party vendor's system. In order to fund the development of the e-filing system, the Legislature in early 2009 approved the development and migration of the public access system from a private entity to the Department. The Department began work on its new public access system in the summer of 2009, and implemented the system in July 2010. In 2010, the Department obtained the necessary authorization and appropriation to build a new, in-house e-filing system known as the Integrated Colorado Courts E-Filing System (ICCES). ICCES must be ready by January 1, 2013, to replace the current vendor e-filing system. Along with the development of ICCES, the Department is also developing the Judicial Paper on Demand (jPOD) case management system, which is expected to interface with ICCES and is integral to day-to-day court case management.

The ICCES project will not require any general fund expenditures. The jPOD project is funded through ongoing general fund expenditures to support and maintain critical case management and financial operations of the Department. The Department Information Technology Cash Fund, established through a Joint Budget Committee-sponsored bill in 2008, allows the Department to retain fees and cost recoveries related to information technology services, including providing public access to court records and e-filing services. Pursuant to Section 13-32-114(2), C.R.S., monies in this fund may be appropriated to the system using existing cost recovery fee revenues as well as fee revenue related to the Department's new public access system. The Department anticipates that once ICCES and the public access system are implemented, the General Assembly could consider using revenues generated from these systems to reduce user fees, continue to improve information technology supporting the state court system, or reduce Department general fund expenditures related to information technology.

Integrated Colorado Courts E-Filing System (ICCES)

Once completed, ICCES will primarily consist of (1) an e-filing system for documents filed for some court proceedings and (2) a document management system to track documents filed. The development project has been separated into three phases:

Phase I: The first phase of ICCES went live in April 2011 and included e-filings for small claims courts.

Phase II: This phase is expected to go live January 1, 2013, when the Department's contract with its third-party vendor expires. Phase II is expected to include e-filing of court documents for the following case types: county and district civil, general jurisdiction domestic relations, civil probate, water, and court of appeals civil cases.

Future Phases: The Department hopes to continue to expand ICCES in the future to add additional functionality, such as online filing services for the criminal and juvenile court systems in Colorado and the ability for pro se filers to e-file.

ICCES will also integrate with the Department's current case management system (ICON/Eclipse) and jPOD, the new case management system that is currently under development. The mechanism integrating ICCES with jPOD and ICON/Eclipse has already been developed and is currently in production.

Judicial Paper on Demand (jPOD) Case Management System

The jPOD system is expected to replace the Department's current case management system (ICON/Eclipse). jPOD will include the following functions:

- Trial court case management for all case types in all state-funded courts
- Appellate court case management for all case types in both the Court of Appeals and the Supreme Court
- Jury selection and management
- Probation case management
- Alternate dispute resolution management
- Court-appointed counsel
- Financial case management
- Electronic filing by attorneys and pro se litigants
- Public access to court data and records
- Data exchanges with Colorado Integrated Criminal Justice Information System in criminal cases, Strengthening Abuse and Neglect Courts Act in dependency and neglect cases, Division of Motor Vehicles in traffic dispositions, Data Information Sharing in child support cases, Statewide Traffic Records Advisory Committee in electronic traffic tickets, the U.S. Federal Bureau of Investigation in mental health cases, Alcohol and Drug Abuse Division in alcohol-related cases, Attorney Registration, Denver County Court in state offenses, and a company providing drug-testing results.

The Department plans to complete jPOD by the end of Fiscal Year 2015.

ICCES/jPOD Project Governance

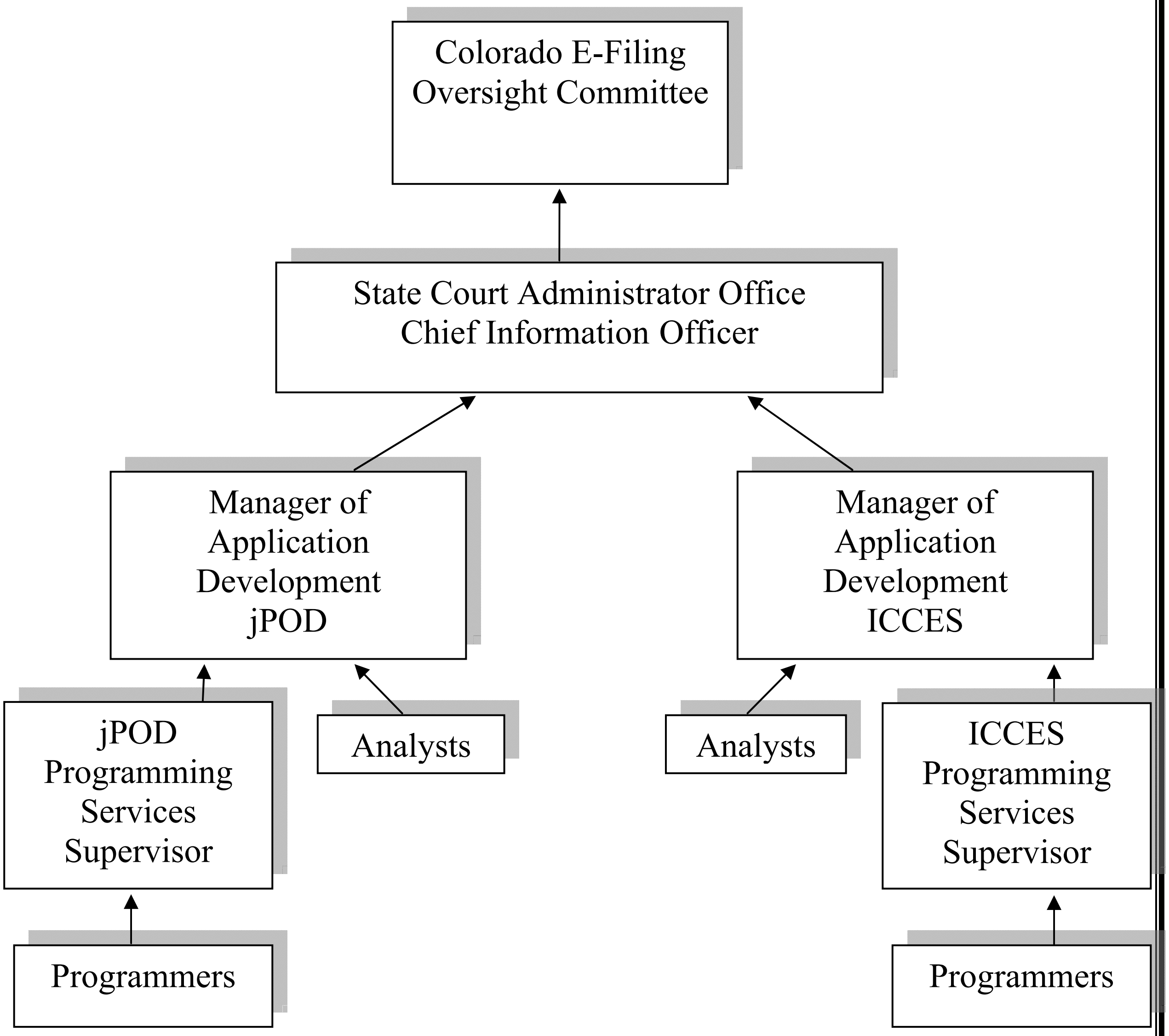
The Supervisor of Application Services manages jPOD development, and the ICCES development project manager is the manager of e-filing services. The Judicial Branch Chief Information Officer (CIO) supervises both projects. The figure on page 9 outlines the overall project management and reporting structure for jPOD and ICCES. We describe the management and oversight responsibilities of key individuals and committees below.

- **Chief Information Officer (CIO)**: The Department's CIO supervises and manages ICCES and jPOD. The CIO's specific responsibilities for ICCES and jPOD include final policy decisions and compliance with statutory requirements; general project management policy requirements; and review and approval of changes to the scope, deliverables, architecture, design, test plan, or deployment options.

- **Colorado E-Filing Oversight Committee (EFOC)**: The oversight committee was created for the purpose of supporting the Department's efforts to improve the management and administration of the Colorado courts, in a manner that serves the needs of the Department's customers, through e-filing technologies. Specifically, the committee has been charged with identifying which elements should be included and integrated into the e-filing and case management systems as well as integrated with other State agency systems. The committee is composed of Department employees ranging from judges to clerks and administrators, and employees of other agencies and entities such as the Colorado Bar Association, the Colorado Office of the Attorney General, and IT representatives from law firms and collection agencies. The Department's CIO chairs the EFOC.

- **Project Teams**: The jPOD and ICCES project teams are each made up of an application development manager, a programming services supervisor, analysts, and programmers. These staff members are responsible for carrying out the day-to-day tasks necessary for project implementation.

Judicial Department's Project Management Structure


Colorado E-Filing Oversight Committee
State Court Administrator Office Chief Information Officer
Manager of Application Development jPOD
Manager of Application Development ICCES
jPOD Programming Services Supervisor
Analysts
Analysts
ICCES Programming Services Supervisor
Programmers
Programmers

Source: Organizational documents provided by the Department

Judicial Department's System Development Methodology

Software development methodologies have evolved significantly in recent decades to accommodate the increasingly dynamic requirements and growing complexity of information systems. Older methodologies followed what is called a "waterfall" approach, where the life cycle of a development project would progress through distinct and nonoverlapping stages or phases. For example, in these approaches, all of the requirements for a system would be specified and finalized before moving on to the development phase, and all development would be completed before moving on to an integration and test phase, etc. Modern methodologies use approaches that are characterized by terms such as "incremental," "iterative," "spiral," "rapid," and "agile." The primary difference between the older, "waterfall" approach and modern approaches is that the modern approaches have the different phases overlap to varying degrees. While there are named and systematized methodologies such as the "rational unified process" or "extreme programming," most organizations and projects use a combination of the principles and practices from several different approaches.

Like most organizations, the Department's software development team uses a combination of different project management, development life cycle, and analysis and design practices. The business practices of the Department as a whole show a lot of characteristics of an agile business process such as high level of involvement from the State Court Administrator's office and high levels of communication and involvement by business stakeholders. The lower-level software development life cycle is more traditional, with a combination of characteristics of both "iterative" and "waterfall" approaches. For example, the requirements are more fluid and are finalized late in the process to ensure that the Department stays more responsive to the business needs, thus making the process "iterative." However, on the detailed level, development of code is managed in a more traditional way, with a micro-waterfall taking place once a use-case is specified. Iterative processes exist within the life cycle to allow re-work and feedback to be incorporated.

Scope and Methodology

The development of new software comes with significant inherent risks, including that the system will fail to achieve the results it was originally intended to achieve at the budgeted costs and on schedule. In some cases, the consequences of that failure can be catastrophic to the entity and those relying on that system. The successful implementation of ICCES and jPOD in Colorado is critical to the efficient and effective operations of state-funded courts. Because of the importance of the successful implementation of ICCES and jPOD system to the

State's judicial system and the citizens of Colorado, the Office of the State Auditor contracted with Wyant Data systems, Inc. (WDS) to conduct an independent verification and validation (IV&V) review of the ICCES and jPOD development projects. IV&V is a process used to evaluate the integrity and quality of the process and products during the course of a systems development effort. The purpose of IV&V is to identify problems early in the development process, thereby enhancing the quality of ongoing development efforts.

WDS conducted the IV&V review in accordance with the Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) Standard 1012-2004, the authoritative standards for evaluating software development projects. In addition, the IV&V employed practices from the Capability Maturity Model Integration, the Project Management Institute's A Guide to the Project Management Body of Knowledge (PMBOK), and the PMBOK—Government Extension as additional standards.

To accomplish the IV&V review objectives, WDS evaluated software development processes and practices according to industry standards and best practices in the following areas:

- System requirements
- Adequacy of functional and technical design
- Project management processes, plans, and practices
- Security
- System architecture
- Quality assurance processes, plans, and practices
- Budgetary management

WDS performed the review of detailed software development artifacts at a very granular level. For example, for requirements specifications, the entire body of requirement document (use-case) and user interface design specifications were surveyed at a high level to determine breadth and coverage, and then a sampling was done at a detailed level of individual documents. The detailed sampling included between 10 and 15 percent of the documents to determine quality, level of detail, and consistency. If inconsistency was found in the documents inspected, the sample size was increased. For actual software code artifacts, a code review was performed with one of the lead developers. WDS inspected the logic paths through the code for several common use-cases, which touched on the major modules and subsystems. The code analysis looked at structure, organization, adherence to coding standards, consistency, and overall technical design.

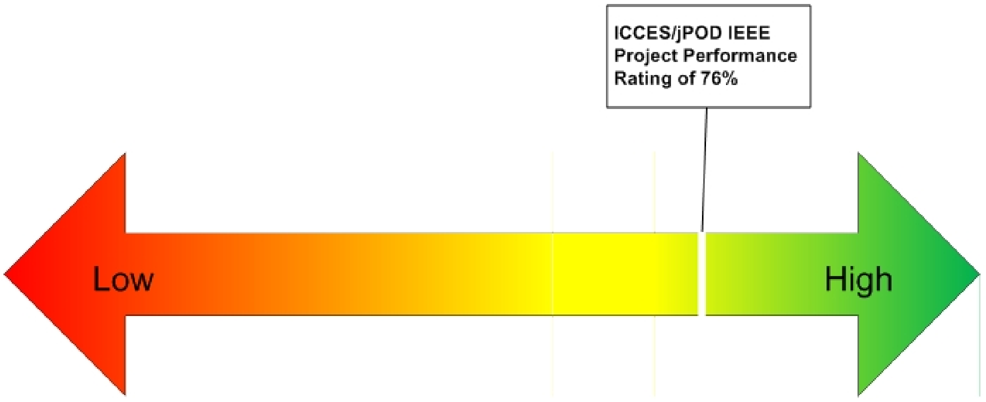
We acknowledge the cooperation and assistance provided by management and staff at the Department.

Overall Project Status

Overall, based on the IEEE 2012-2004 software verification and validation assessment matrix (Matrix) methodology (see Appendix B), WDS concluded that the Department faces a low to medium risk of failure for the ICCES/jPOD development project. On a high level, a project is considered a failure when it cannot be delivered as intended. The Matrix provides an industry-proven standardized approach for determining whether the software development projects are on track to be completed within the estimated schedule and for identifying and quantifying any issues and risks affecting project components. The Matrix includes an assessment of approximately 150 project-related activities for the areas of planning, project management and oversight, quality management, training, requirements management, operating environment, development environment, software development, and systems and acceptance testing. Each of these areas was further broken into subprocesses and practice areas.

Using the Matrix, WDS assigned a numerical score for each item reviewed. Based on the analysis, the ICCES/jPOD project received a project quality assessment score of 76 percent. The final quality assessment scorecard can be found in Appendix B.

Project Quality Assessment Score



Source: Based on the IEEE 2012-2004 software verification and validation assessment matrix.

It is important to note that this assessment was conducted at a specific point in time during the project life cycle. Therefore, the results are only representative of the project practices as observed during the evaluation period. As described in Appendix B, a score of 76 percent signifies that there are some compliance and / or implementation concerns that may hinder, but not prevent project completion from occurring. The score also indicates that additional management attention is warranted in the improvement of project management practices. Specifically, the Department should implement the recommendations mentioned below to ensure continued success.

Findings and Recommendations

The following section presents the detailed findings and recommendations identified during the IV&V review of the ICCES and jPOD systems development project at the Judicial Department (the Department). Appendix A provides the criteria for assigning the risk level to the individual finding based on the categorizations, which are listed in the following order of severity: High, Major, Moderate, and Low.

Cyber Security Plan

The Department does not maintain an up-to-date cyber security plan, is noncompliant with statutes, and is delinquent in performing a security risk assessment and vulnerability scans.

The IEEE 2012-2004 clauses [5.4.2 Requirement, 5.4.3 Design, and 5.4.4 Implementation] identify assessment criteria for verifying and validating sound security practices in the protection of computer hardware or software from accidental or malicious access, use, modification, destruction, or disclosure. The security assessment standard also pertains to personnel, data, communications, physical protection of computer installations and the protection of information and data so that unauthorized persons or systems cannot read or modify them and authorized persons or systems are not denied access to them.

In addition, the Colorado Cyber Security Program (Section 24-37.5-404, C.R.S.), requires every state agency to develop an information security plan that identifies how the agency will protect the information and communication resources that support the operations and assets of the agency. State agencies must update the information security plan annually and submit it to the Chief Information Security Officer (CISO) at the Governor’s Office of Information Technology. If an agency fails to complete and submit an information security plan, the CISO shall notify the governor, the chief information officer, and the head of the agency of noncompliance. If no plan has been approved by September 15 of each year, the CISO shall be authorized to temporarily discontinue or suspend the operation of the agency’s communication and information resources until the plan has been submitted and approved. Statute further stipulates that the cyber security plan should include periodic security risk assessments and, at a minimum, an annual testing and evaluation of the effectiveness of information security, such as conducting vulnerability scans.

Together, the security requirements listed above are intended to ensure the security of the information held in information systems and to ensure that security measures are being applied to information technology to achieve a desired level of protection and to minimize the number of successful security attacks that could compromise important information or system functions. The cyber security policies describe the technology and information assets that should be protected and helps to identify mechanisms to prevent and detect security threats to those assets. It also helps establish users' responsibilities and privileges and procedures for responding to incidents that threaten the security of the computer systems and network.

We found that the Department has not updated its cyber security plan since July 2009 and, as a result, the Department is not in compliance with the statutory provisions that require that the plans be updated annually. Further, the dated cyber security plan also lacks comprehensive documentation pertaining to risk assessment, certification, accreditation and security assessments, system services and acquisition, configuration management, system and communications protection, personnel security, awareness and training, physical and environmental protection, media protection, contingency planning, maintenance, system and information integrity, incident response, identification and authentication, access control, and accountability and audit. Additionally, the Department confirmed that it is delinquent in performing a security risk assessment and vulnerability scans required by the State's cyber security policies. In fact, the Department was unable to provide evidence showing the last date when the security risk assessment and vulnerability scans were performed.

Without such an assessment or scan, the Department does not know if the systems are vulnerable to cyber security attacks when they go live. Vulnerability to cyber security attacks can result in significant downtime and user dissatisfaction in addition to compromising sensitive user information. The implementation and management of a mature cyber security program is especially critical because the Department plans to eventually host the systems in-house and provide 24-hour support to the users with agreed-upon performance goals. The essence of solid cyber security is a clearly defined security framework, established in a written plan, and policies and procedures that are well designed and implemented consistently throughout the Department.

Because the Department still has a cyber-security plan—though outdated—in place, the risk level has been lowered from high to major.

(Risk level: Major)

Recommendation No. 1:

The Judicial Department (the Department) should take immediate steps to comply with State cyber security policies and related statutory provisions by:

a. Developing a robust set of implementation plans, practices, and guidelines as outlined in State cyber security policies by creating and submitting updated plans and policies in the following areas: risk assessment, certification, accreditation and security assessments, system services and acquisition, configuration management, system and communications protection, personnel security, awareness and training, physical and environmental protection, media protection, contingency planning, maintenance, system and information integrity, incident response, identification and authentication, access control, and accountability and audit.

b. Performing a periodic vulnerability, threat, and risk assessment of the department's policies, procedures, systems, and network infrastructure. In addition, the Department should take steps to ensure that its vulnerability, threat, and risk assessments are an integral part of the overall life cycle of the infrastructure in place.

Department's Response:

a. Disagree.

The Department is committed to the Cyber Security Program, as well as continuing to seek ways of reducing information security risks and complying with regulatory guidelines. While the Judicial Department was remiss in submitting it's 2010 cyber security plan to the Office of Information Technology (OIT), the Department would like to acknowledge that in 2010 an updated cyber security policy was presented and reviewed by the Department's IT oversight committee. The Department has also verified that a 2011 cyber security plan (ACSP) was submitted to the CISO at the Governor's Office of Information Technology. Accompanying the agency cyber security plan was the Departments plan of actions and milestones, disaster recovery plan executive summary, disaster recovery test results, and the cyber security training progress report. Due to the resignation of the Department's Information Security Officer (ISO) in September 2011, the Acting CIO did not receive confirmation of the ACSP submission as it was delivered to the ISO. The Department has completed a draft of its 2012 cyber security plan and will submit the final draft to the CISO once reviewed by the Department’s IT oversight committee in July.

Reviewer Addendum

During our review period, the Judicial Department was unable to provide our staff with a current cyber security plan. Additionally, when this finding was initially discussed with the Department, Judicial management staff, including the current Chief Information Officer and Information Security Officer, confirmed that an updated cyber security plan did not exist and was never provided to the State’s Chief Information Security Officer as required by statute. Just prior to the distribution of this report, the Department provided an updated cyber security plan to our staff; however, we did not have sufficient time to review the plan to ensure that it was complete, reliable, and met state cyber security policy requirements. In addition, although the Judicial Department was able to produce an updated cyber security plan, we are concerned that Judicial management staff, including the current Chief Information Officer and Information Security Officer, were neither aware of the existence of the plan nor were they able to confirm whether or not the plan was submitted to the State’s Chief Information Security Officer. Although the plan may have existed, the intent behind the plan—to drive the security operations of the Department—was not achieved during our review period.

b. Partially agree. Implementation date: September 2013.

The Department agrees that performing documented penetration and vulnerability scans of its systems and networks is critically important and will focus on these efforts in the near future. A risk assessment was completed in 2011 and the Department can provide a copy of the report if necessary. The risk assessment was conducted to provide a qualitative assessment in the areas of management, operational, and technical security. Based upon the NIST SP 800-30 and SEI Octave Allegro methodologies and guidelines, the risk assessment measured confidentiality, integrity, vulnerability, and availability of critical systems within the Judicial Department. In fiscal year 2014, the Department plans to seek funding for a third party vendor to perform an independent vulnerability, threat, and risk assessment of the Department’s policies, procedures, systems, and network infrastructure.

Reviewer Addendum

Similar to the reviewer addendum to subpart “a” of this recommendation, the Judicial Department was unable to provide our staff with a current risk assessment, which is included as part of an agency’s cyber security plan. Again, prior to report distribution, the Department provided our staff with a copy of an updated risk assessment; however, we did not have adequate time to review it. In addition, we could not verify that the applications under review were part of the risk assessment performed by the Department.

Project Management Best Practices

The Department does not have documented project artifacts and processes as recommended by industry best practices to help ensure that activities related to project scope, schedule, and budget are monitored and controlled.

The Project Management Institute’s A Guide to the Project Management Body of Knowledge (PMBOK) establishes industry-recognized best practices for project management. Several industry-proven project management methodologies exist that establish the overall process for how the software is developed. While these methodologies have significant differences, they are all consistent with the PMBOK.

For projects, PMBOK recommends a written “project management plan” that includes a number of component plans. Each of the component plans describes the management processes that will be followed to execute the project. Specifically, the component plans specify how the activities related to project integration management, scope management, time management, cost management, quality management, human resource management, communications management, risk management, and procurement management will be executed.

Several of the component plans define specific processes to monitor and control a project’s critical constraints, including the scope, schedule, and budget. PMBOK recommends a process tool called “earned value analysis” to analyze these three constraints and to document the results as detailed project metrics. Earned value analysis shows the overall project health/performance at a given point in time. The earned value analysis uses the actual versus planned effort for work units to extrapolate future performance based on past performance. This method ensures that remaining project expectations are accurate.

We observed that the Department does not have a documented project management plan or the majority of the component plans as recommended by industry best practices. For example, the Department does not have a documented risk management plan or a quality management plan. While we observed that attention is being given to the various risks and opportunities that could impact the projects, we believe that the omission of artifacts such as a risk register specified within the risk management plan is a significant deficiency. The risk register records details of all the risks identified at the beginning and during the life of the project, the grades for the risks' likelihood of occurring and seriousness of impact on the project, initial plans for mitigating each high-level risk, the costs and responsibilities of the prescribed mitigation strategies, and subsequent results. The risk register is continuously maintained during the life of the project as specified in the risk management plan. The lack of a quality management plan is covered in a separate recommendation. We noted that the Department does have one component of the project management plan documented, which is the project charter. The project charter documents the business needs, current understanding of the customer needs, and the new product service or results that it is intended to satisfy. A documented project charter is like a mission statement that summarizes some of the details listed in the other components of the project management plan at a very high level. Existence of the project charter partially mitigates the risk of not having a complete project management plan.

We observed that the Department is not rigorously following an industry-approved software methodology. We also observed that the Department does not utilize earned value analysis or an equivalent process to manage and control the ICCES/jPOD project. The actual versus planned effort for work units is not explicitly tracked or used to extrapolate future performance based on past performance. For example, the Department does not reevaluate the hours estimated to develop a particular piece of the software code with the actual hours spent.

To ensure the Department's development of ICCES/jPOD system is successful, we recommend that a proven software development methodology be adopted. Currently, the Department practices many of the components of an agile business process. We believe that the Department can best mitigate the risks to the project by adopting a standard agile software development methodology such as SCRUM, a current agile project management methodology.

(Risk level: Moderate)

Recommendation No. 2:

The Judicial Department (the Department) should strengthen its project management practices by:

a. Generating and/or improving project documentation artifacts as well as tracking and documenting project activities. Documentation of artifacts should include a project management plan and its associated component plans, including a risk register within the risk management component plan.

b. Collecting project metrics and perform “earned value analysis” or an equivalent metric on the project so that the exact status of the project based on fine-grained work breakdown can be reported to any interested stakeholders on a regular (minimum monthly) basis.

c. Tracking actual versus planned effort by adopting a more standardized software development methodology such as an agile process like SCRUM.

Department’s Response:

a. Agree. Implementation date: September 2013

The Department recognizes the need to improve and strengthen its project management practices, particularly from a documented process and artifact delivery perspective. However, the Department must also find a balance between adhering to PMI standards and the delivery of accurate, complete, and timely information that the justices, judges, court, and probation staff needs to make informed decisions. After the successful implementation of the ICCES and jPOD projects, the Department plans to improve and strengthen its documented project management methodologies by utilizing agile principles that incorporate PMI standards along with the SCRUM framework. With four certified Project Management Professionals (PMP’s) in good standing and a commitment to consistently involve court and probation business stakeholders in all application development efforts, the Department has been extremely successful over the last twelve years in its delivery of IT systems. While the Department does lack certain documentation within the various PMI process groups, its success can be attributed to implementing lean principles and a hybrid agile project management (APM) approach that includes an APM framework (envision, speculate, explore, adapt, and close).

b. & c. Agree. Implementation date: January 2014

The Department agrees that it can improve tracking project performance metrics, such as Earned Value Management (EVM), or a SCRUM variant, such as agile burn charts, that are able to track product progress as a percentage of total product size, as well as the cost incurred as a percentage of the total project. Similarly, by implementing a software development methodology such as SCRUM, the Department will be able to produce artifacts that will aid in the development, monitoring, and tracking of actual versus planned effort through agile burn charts. Incorporating a SCRUM methodology within the Departments IT Division will necessitate proper training for project team members that the Department is willing and excited to implement. Proficiency in SCRUM methodologies will take time, but the Department's goal will be to slowly implement these methodologies once the first phase of the ICCES and jPOD projects are live and stable.

Enterprise Operations

The Department does not have adequate policy, procedures, and plans to operate ICCES and jPOD system at an enterprise-level.

The Department identifies eight major business needs that are being addressed though the development and implementation of ICCES/jPOD system. These eight business needs are outlined below.

- Independent funding opportunity
- Reducing costs to the users
- Opportunity to interface more directly with the Department's jPOD (i.e., case management system replacement for ICON/Eclipse)
- Avoid network limitations
- Opportunity to gain improved control over application development
- Opportunity to gain more control over the stability of the technical infrastructure environment
- Opportunity to ensure disaster recovery for e-filing

To meet the needs of its customers and stakeholders, the Department plans to:

- Move to a full support information communications technology service model. Information communications technology includes managing all the information technology- (IT) related functions in house, such as application development and infrastructure maintenance, and moving current hosted data center service to an in-house operation.
- Provide 24-7 enterprise application support services, such as helpdesk.
- Identify and document customer expectations in a formal way, such as with service level agreements.

The Information Technology Infrastructure Library (ITIL) is a set of practices for IT service management that focuses on aligning IT services with the needs of the business. The ITIL and International Service Management Standard for IT service management, and the IEEE Standard for Software Verification and Validation 1012™-2004 address the structure and controls required for an entity to provide enterprise-level services, including defining the necessary requirements for service strategy, service design, service transition, service operation, and continual service improvement.

We reviewed the Department's operational management plans for ICCES/jPOD system and noted that the plans lack a robust policy and procedure structure required for operating at the enterprise level. For example, the operational plan does not include:

- Resource planning to ensure that users can be provided with 24-hour technical support.
- Measures to ensure that agreed-upon customer expectations are met.
- Procedures to document customer service requirements.

Specifically, the current operational plan does not include documented procedures and plans for output management, job scheduling, backup and restoration, network monitoring/management, system monitoring/management, database monitoring/management, and storage monitoring/management.

Further best practices indicate that the Department should also have documented operational processes and procedures. These are needed to ensure a stable, secure information communications technology infrastructure, a current up-to-date operational documentation library and log of all operational events, maintenance of operational monitoring and management tools, and operation scripts and procedures. A comprehensive and complete operational plan is critical to an enterprise-wide application and hence a must for ICCES/jPOD.

(Risk level: Moderate)

Recommendation No. 3:

The Judicial Department (the Department) should ensure a smooth transition to enterprise-level application support for ICCES/jPOD by:

a. Developing staffing and management plans to support the Department's transition to an enterprise service model with 24-hour support operations.

b. Developing and maintaining service level agreements with users of ICCES/jPOD.

c. Developing or enhancing documented operational processes and procedures that address specific sub-processes, such as output management, job scheduling, backup and restoration, network monitoring/management, system monitoring/management, database monitoring/management, and storage monitoring/management.

Department's Response:

a. Agree. Implementation date: October 2012.

The Department has recently approved a plan to provide enterprise application support services between the hours of 6:00 AM and 12:00 AM. The Department is in the process of developing staffing and management plans for application support operations. Between April and June 2012, the Department conducted several meetings with the current vendor to discuss transition plans and enterprise level support. As a short-term enterprise solution, the Department has issued an RFP to solicit a tier 1 customer support call center service to support the ICCES application. The Department hopes to contract with a local Colorado call center and is also in the process of hiring a call center manager that will act as a liaison between the Department's tier 2 support staff and the selected call center. The Department's long-term strategy of providing enterprise support will consist of the call center manager developing an on-premise call center within the Department to support the daily operations of the courts and probation. This would include all public facing applications, as well as fielding tier 1 calls for court and probation business needs.

b. Agree. Implementation date: September 2013.

The Department agrees that developing and maintaining documented Service Level Agreements (SLA's) with users of the ICCES and jPOD applications, as well as future applications, will help ensure service levels meet all of the agreed targets for ongoing software development. With three employees recently certified in ITIL Foundation Service Management, the Department understands the significant value that ITIL best practices and service level management processes can provide. By ensuring IT services are aligned with the business needs, the Department's IT staff can better serve the court and probation users. According to ITIL 2011 best practices, service level managers manage a variety of Service Level Management (SLM) processes. Therefore, based on the project management structure as outlined on page 9 of the IV&V report, the Department will need to balance the duties and roles of service level managers, with that of operational and project oriented roles that the managers of application development must be a part of. The Department plans to begin development and implementation of service-based SLA's after the first phase of ICCES and jPOD is complete. The SLA's can be developed so that they retroactively fit with requested ICCES requirements to-date, as well as current and future modules of jPOD.

c. Agree. Implementation date: September 2014.

The Department understands that it lacks sufficient documented operational process and procedures as outlined in the report under Enterprise Operations. However, the Department would like to acknowledge that there are enterprise operational processes and procedures in place to handle each of the identified areas. By implementing and building upon ITIL□ 2011 best practices, the Department plans to take advantage of the recent findings to refine and document its enterprise level operational processes and procedures.

Quality Assurance

The Department does not have a quality assurance plan and currently is not able to support configuration management functions.

Quality assurance and control processes are the operational techniques and activities that ensure the application code is developed based on established standards, can handle further changes with minimum down time, and provides functionalities required by the business. To avoid costly errors, software development projects should include a quality assurance program. A quality assurance program should include:

- Test planning.
- Data collection.
- Data analysis.
- Implementation of tools and techniques such as coding standards/code review.
- Systematic measurement of quality control activities.
- Feedback loop for error prevention and process improvement.

Quality assurance and control processes are crucial to the success of all phases of the product life cycle, including concept requirements development, design, implementation, testing, and operation and maintenance.

We reviewed the Department's existing quality assurance controls based on the IEEE Standard for Software Verification and Validation1012™-2004 (Revision of IEEE Std 1012-1998) and the Project Management Institute's A Guide to the Project Management Body of Knowledge (PMBOK). During the review, we found that the Department lacked a quality assurance plan, as recommended by IEEE and PMBOK standards and best practices. A quality assurance plan determines management's expectations of a product or process and how they will measure quality before a project begins. This type of plan also explains the project in detail and the strategies and methods the organization plans to use to execute it. As a result, we noted that the Department's project organizational structure and practices do not support the best practice and industry standards for quality assurance and configuration management. Below are the critical elements we found that did not conform to industry standards.

Requirements Management. The Department does not have a Requirements Traceability Matrix to perform a traceability exercise to link test scripts, use-cases, and unit tests with the business requirements to ensure complete and clear rules have been incorporated into the development process.

Additional Requirement. The Department does not have adequate and complete information, such as use-cases and system requirements, for the system, interface, document upload process, payment fee process, and security and performance requirements.

Unit/System/User Acceptance Testing Framework. The Department does not perform unit testing for code pushes or regression. "Code pushes" refers to moving the code from one test environment to another so that different users can test it. "Regression" refers to ensuring that existing code still works well with the new code. The Department does not perform extensive system testing to ensure the new ICCES/jPOD platforms will perform as desired. The Department does not have a user acceptance testing document to validate that sponsors/stakeholders agree that the system satisfies the approved requirements.

Configuration Management. The Department does not have a configuration management plan to incorporate agile method processes and project management measurements. The Department does not test to evaluate pre- and post-conditions to ensure they are correct and complete requirements.

Independent Quality Assurance. The Department does not have an independent quality assurance role or function to oversee quality management and compliance.

Plans and procedures over software quality allow an organization to prevent catastrophic outages or performance degradations that can make a given system unsuitable for use. We would, however, like to acknowledge that the Department performs a biweekly product walk-through with the team members to inform them of new functionalities implemented and to seek feedback. This process mitigates, to some extent, the inherent risks associated with the lack of a formalized quality assurance/quality control program. Hence, the overall risk associated has been lowered from major to moderate.

(Risk level: Moderate)

Recommendation No. 4:

The Judicial Department (the Department) should implement a strong quality control assurance program by:

a. Developing a Requirements Traceability Matrix and performing a traceability exercise to link use-cases to business rules.

b. Reviewing the business requirement rules of each component of development to ensure complete and clear rules have been incorporated into the use-case.

c. Developing additional requirements, design specifications, use-cases, and test scripts for the system, interface, document upload process, payment fee process, and security and performance requirements.

d. Developing testing mechanisms and processes that (1) ensure creation of a unit testing framework, (2) perform extensive system testing to ensure the new ICCES/jPOD platforms will perform as desired, (3) document the confirmation from sponsors/stakeholders that the system satisfies the approved requirements, and (4) develop tests to evaluate pre- and post-conditions to ensure they are correct and complete requirements.

e. Developing a configuration management plan to incorporate an agile method process and project management measurements.

f. Establishing an independent quality assurance role or function to oversee quality management and compliance.

Department's Response:

a. Agree. Implementation date: September 2013.

The Department is supportive of implementing a Traceability Matrix, as it will allow traceability from requirements to test scripts that are necessary to verify that the requirements were fulfilled. While implementing a traceability matrix would simplify the Department's current use-case template structure, the Department is committed to practicing SCRUM methodologies in the future, which would allow traceability of agile user stories, rather than use-case documents. The Department will incorporate a Traceability Matrix into its SCRUM implementation plan.

b. Partially Agree. Implementation date: September 2013.

The Department has created a variety of use-case documents, design diagrams, and user interface (UI) specifications that contain business requirement rules of each component or module being developed for the current ICCES/jPOD projects. These projects are currently in the implementation phase; therefore, there is limited benefit to the Department to review these documents at this time. However, the Department will review the existing documentation for possible value-added improvements for future projects.

Reviewer Addendum

The review was performed at a point in time. The use cases we sampled did not include the business requirement rules of each component of development to ensure complete and clear rules had been incorporated; and as such, we continue to believe our work supports the finding.

c. Partially Agree. Implementation date: September 2013.

The Department agrees that it needs to develop additional quality assurance requirements such as test scripts, as well as security and performance requirement documentation. However, the Department does currently develop and maintain use-case, design specifications/diagrams, and user interface (UI) documents for the various business requirements and product features. This includes documented specifications for the interface, document upload process, and payment fee process. The Department's IT division will investigate ways to incorporate test scripts, security and performance requirements as part of its audit remediation plan, which will include enterprise operations support, ITIL best practices, and SCRUM methodologies.

Reviewer Addendum

The review was performed at a point in time. During the review we noted that the Department did not have adequate and complete information such as use-cases, system requirements, etc., for the system, interface, document upload process, payment fee process, and security and performance requirements. As such, subpart "c" of this finding is supported by the work performed and remains a valid concern.

d. Agree. Implementation date: July 2013

The Department agrees that it needs to develop more efficient and automated regression and unit testing mechanisms to ensure its systems perform as desired. The Department's IT division plans to explore open source testing frameworks such as JUnit and Cactus. The Department would like to acknowledge that it has held many product demonstrations of both ICCES and jPOD for stakeholder feedback. This includes a variety of user groups at the Colorado BAR Association, court staff, Board of Governors, Association of Legal Administrators, Mile High Association of Legal Support Staff, and various collection agencies. Additionally, the Department is currently in the process of configuring a demo site for all ICCES stakeholders to test system functionality.

e. Partially Agree. Implementation date: June 2013.

The IV&V report suggests that the Department is currently not able to support configuration management functions, however, the Department has implemented many processes and practices currently that support the PMBOK's definition of configuration management and change control systems. The Department has an active Change Advisory Board (CAB) with a documented charter. While the change and configuration management processes are not formally documented, all configuration changes are handled through a change request form with tracking systems for reviewing and approving proposed changes. Approved configuration requests are then updated on the Department's SharePoint site within the Schedule of Planned Activities (SPA). As changes are made (during the change window), they are tracked using a detailed—color-coded—task list. The task list is distributed via email to all involved so that everyone is aware of what is complete, as well as the remaining items to be completed. The Department recognizes that it can do a better job at documenting its current configuration management procedures and plans to do so by implementing an enterprise IT Service Management system in Fiscal Year 2013.

Reviewer Addendum

The review was performed at a point in time. During the review a formal configuration management plan was not available for review. In addition, we were unable to verify that the Department was testing to evaluate pre- and post-conditions to ensure that the conditions were correct and complete. Although the Department partially agrees with this finding, we affirm that our work supports our conclusions.

f. Agree. Implementation date: February 2014

The Department is supportive of an independent quality management team to oversee quality planning, quality assurance, and quality control processes. However, the Department is constrained by FTE allocations that would be necessary to develop an independent quality management team. As an alternative solution, the Department would like to begin training and certifying current IT business analysts through the International Software Testing Qualifications Board (ISTQB) or another variant such as Software Quality Engineering (SQE). The Department is in the process of requesting Fiscal Year 2014 funding to support this effort.

Capacity/Performance Planning

The Department did not perform a complete capacity/performance assessment of established hardware architecture for ICCES and jPOD system

IEEE Standard for Software Verification and Validation 1012™-2004 (Revision of IEEE Std 1012-1998) suggests that it is prudent to review system capacity prior to making changes to existing systems, to determine the capacity of the existing hardware and software infrastructure and the capability of that system to handle the potential processing load associated with the implementation of any new systems. The system architectural decisions must be well documented to understand why certain trade-off decisions were made as well as how the decisions were balanced against other competing functional needs of the systems. Capacity management is a process used to manage existing systems to ensure that IT capacity meets current and future business requirements in a cost-effective manner. Capacity management includes the management of:

- **Business capacity**—The main objective of business capacity management is to ensure that future business requirements are translated into quantifiable IT services. Business capacity planning is used to determine whether or not operational output can be increased without straining current resources.
- **Service capacity—**IT services include email, Internet, telephone, text messaging, etc. It also includes monitoring end-to-end service capacity against the agreed service level agreements with users.
- **Component capacity—**One of the prime objectives of component capacity management is monitoring components, such as hard disks, network bandwidth, processors, workstations, and network connections, to ensure that sufficient capacity is on hand to perform functions optimally. Forecasting future component requirements plays into this as well.

As the usage of IT services within an organization changes and functionality evolves, the amount of processing power and memory required also change. Ongoing evaluation of existing systems and infrastructure and how that will interact with planned system improvements or new systems makes it possible to better plan for IT service growth and enables the entity to better prevent problems when making system improvements. For example, capacity planning in advance can prevent significant downtime, increases in maintenance cost, and operational inefficiencies and can ensure that customer expectations are met.

We requested the Department's capacity assessments and noted that the Department did not perform a complete capacity/performance assessment of established hardware architecture prior to completing the design and moving forward with production for ICCES and the jPOD system. As a result, the

Department cannot be sure that when ICCES/jPOD are launched that the existing IT infrastructure and service environment will meet expectations and provide service levels equal to or better than those currently experienced from the third-party vendor service. Further, the design of the hardware infrastructure does not have any supporting analysis to determine capacity and the capability to handle the potential processing load that ICCES/jPOD will add to the existing hardware infrastructure. Without such an analysis, it is possible that once live, these systems may experience poor performance resulting in user dissatisfaction. Making capacity changes once the systems are live can result in significant cost, downtime, and operational delays.

Best practices suggest that system architectural decisions should be based on functional aspects such as reliability, maintainability, security, and performance. It is recommended that the Department revisit and reanalyze the potential changes to capacity assessment for determining the necessary hardware (computer/network) and, ultimately, decrease the risk that may exist given the implementation of ICCES and jPOD system.

(Risk level: Moderate)

Recommendation No. 5:

The Judicial Department (the Department) should reevaluate and reassess its capacity planning and infrastructure performance based upon the projected utilization and capacity needs of ICCES/jPOD, including:

a. Revisiting system architecture, that is, the hardware and network supporting ICCES/jPOD system, to validate and verify that the current design will support the projected processing load for ICCES and jPOD. Identify and document risks and a related mitigation strategy as necessary.

b. Developing plans for load/pilot testing and validating the system capacity and capability. Obtain operational performance information, either from the current third-party vendor or survey the potential stakeholders to validate/confirm anticipated system performance design and functionality.

Department's Response:

a. & b. Agree. Implementation date: August 2012

The Department has begun identifying and documenting the risks associated with load and capacity planning, as well as determining mitigation strategies for each of the identified risks. Load and capacity testing plans are currently under development with an expected completion date of August 2012. During several meetings that took place with the current vendor between April and June 2012, the Department was able to obtain high-level operational performance information, as well as perform its own analysis on the number of documents the Department receives on a nightly basis from the current vendor for backup purposes. Based on the information gathered, the Department was able to meet with its hardware vendor to establish best effort configurations in order to meet the projected processing, load, and capacity levels necessary to achieve optimal performance for both the ICCES and jPOD systems.

Capitalization of Software Development Costs

The Department did not capitalize the software development cost for the ICCES/jPOD system as required by accounting principles.

Capitalization is an accounting method used to convert a cost into an asset instead of an expense. The Governmental Accounting Standards Board (GASB) Codification of Governmental Accounting and Financial Reporting Standards, Section 1400, paragraphs .126 through .129 states that the development cost of internally developed software should be capitalized. The standard stipulates that all software developed in house by government personnel should be capitalized.

The ICCES and jPOD system are both being developed in house by the Department's staff. Further, the standard states that the Application Development Stage should be included in the capitalization calculations for software developed in house:

- Preliminary Project Stage. Activities in this stage include the conceptual formulation and evaluation of alternatives, the determination of the existence of needed technology, and the final selection of alternatives for the development of the software.
- Application Development Stage. Activities in this stage include the design of the chosen path, including software configuration and software interfaces, coding, installation to hardware, and testing, including the parallel processing phase.
- Post-Implementation/Operation Stage. Activities in this stage include application training and software maintenance.

Additionally, the capitalization of costs should begin after management authorizes or commits funding to the project, and once the preliminary project stage has been completed.

We reviewed the Department's procedures for capitalization and noted that the Department did not capitalize the software development costs for the ICCES/jPOD system. Because the Department has run the development of ICCES and jPOD as operational functions and not as a discrete, capital project, the Department did not identify and track all the costs associated with the development of these two systems. As such, we were unable to determine the total cost of this project or compare costs to established budgets. Additionally we are unable to determine the total cost that should be capitalized. According to the Department and contrary to accounting standards, all development costs for ICCES/jPOD have been expensed as the costs were incurred.

The Department's treatment of the costs associated with developing ICCES and jPOD system is not in compliance with established accounting principles, which suggests that all appropriate software development expenses be tracked and accounted for, and a project is capitalized and meets the accounting cutoff time so that accounting assertions are followed for the project. As a result, the Department's assets and expenses have been improperly categorized.

(Risk level: Moderate)

Recommendation No. 6:

The Judicial Department (the Department) should ensure that project costs are appropriately capitalized as required by established accounting principles by:

a. Establishing a plan to capitalize the project in the correct accounting period and re-stating financial records as needed.

b. Estimating and recording the value of the project on an annual basis since the preliminary stage of the project.

Department's Response:

a. Agree. Implementation date: August 1, 2012.

The Department will amend the current property management fiscal rule to create criteria for identifying what level of projects require capitalizing and establish a process to capitalize intangible assets. The Department is working on compiling data to capitalize the appropriate expenditures associated with the ICCES and jPOD projects in accordance with government accounting standards (GASB 51). The Department will capture these costs from the application development phase and make the corresponding accounting entries as part of the Fiscal Year 2012 year-end process.

b. Agree. Implementation date: April 1, 2013.

   The Department will begin to identify and track all expenditures associated with ICCES and jPOD projects. The Department will also develop a fiscal rule requiring all projects over a certain dollar threshold to identify and track all direct and indirect costs. Further, the Department is evaluating the use of a time keeping system to enhance the accurate and timely collection of personnel costs associated with projects.

[This page intentionally left blank for reproduction purposes]

Report Findings by Classification
Appendix A

Table 1 provides a legend for categorizing the finding levels and their potential impact.

Table 1: Classification Severity Level Description

IV&V Finding/Observations/Concern Categorization Level Definitions	
High	The project issue, process, task, or software component affects performance of the system and threatens the successful implementation of ICCES/jPOD at the enterprise level or may lead to violations of legal and/or statutory requirements.
Major	The project issue, process, task, or software component affects performance of the system and threatens the successful implementation of ICCES/jPOD at the functional level, with no violations of legal and/or statutory requirements.
Moderate	The project issue, process, task, software component, or lack of best practice impacts the usability of the system while still meeting the required system functionality and related regulations and statutory requirements.
Low	Failure of the project task, process, software component, or lack of best practice will have a minimal impact to the functional operations of ICCES/jPOD and any related regulatory and/or statutory compliance.

Table 2: Finding Identification Summary

Finding No.	Page No.	Finding	Classification of Findings			
			High	Major	Moderate	Low
1	15	Cyber Security Plan		X		
2	19	Project Management Best Practices			X	
3	22	Enterprise Operations			X	
4	25	Quality Assurance			X	
5	30	Capacity/Performance Planning			X	
6	32	Capitalization of Software Development			X	

ICCES / jPOD Project Scorecard Quality Assessment Appendix B

IEEE IV&V 2012-2004 Project Quality Evalauation Summary

ICCES/jPOD
Project Score
76.00%

Project Quality Score Dashboard	Percent Scale	0-49%	50-79%	80-99%	100%
	Rating Level	RED	YELLOW	GREEN	
Key Attributes of the categories relating to the Project Quality Assessment Score		Minimum progress has been made towards achieving the identified objective. One or more critical tasks may at risk of not being completed.	Significant efforts are underway and specific examples of progress in this area can be identified.	Efforts within this development project are mature. Few gaps or barriers to success remain. None are significant.	Indicates that the objective and elated VV practices are fully achieved with regard to the project performance and requirements.
GREEN: When all elements of the practices outlined in the IEEE 2012-2004 Software Verification and Validation are practiced and at least 80% of all tasks within the respective project meet best practices signifying that there are no significant deficiencies with the respective project structure and quality of performance. YELLOW: When elements of the practices outlined in the IEEE 2012-2004 Software Verification and Validation are identified and between 50 to 80% of all tasks within the respective project meet best practices, signifying that there are some compliance and/or implementation concerns that may hinder, but not prevent project completion from occurring. RED: When elements of the practices outlined in the IEEE 2012-2004 Software Verification and Validation are minimally practiced and less than 50% of all tasks within the respective project meet best practices, signifying that there are significant deficiencies and/or implementation concerns that will prevent successful completion of the project.		Steps may include initial plans to develop this aspect of the capability, allocation of resources, and identification of personnel responsible for achievement of the objective.	Strategies for closing gaps and overcoming barriers to success are being implemented and clear progress has been made.	Practices within this development project are mature. Strengths are robust and likely to be sustained.	All critical tasks have been completed. Strengths are robust and likely to be sustained.
		Strategies for closing gaps and overcoming barriers to success are being developed and initiated.	Some weaknesses or barriers that prevent success persist, but strategies to resolve them are documented and being addressed.	All critical tasks have been completed.	All barriers to success have been overcome. Evidence is readily available attesting to this level of achievement.
		Work may have begun on strategies to resolve weaknesses and barriers that persist and prevent success.		Evidence documenting this level maturity and related progress is readily available.	

The electronic version of this report is available on the website of the
Office of the State Auditor
www.state.co.us/auditor

A bound report may be obtained by calling the
Office of the State Auditor
303.869.2800

Please refer to the Report Control Number below when requesting this report.

Report Control Number 2172

Report Control Number 2172