



---

**INTEROFFICE MEMORANDUM**

**DATE:** June 1, 2012

**TO:** John H. Armstrong, MD  
Surgeon General and Secretary of Health

**FROM:** James D. Boyd, C.P.A., M.B.A., Inspector General 

**SUBJECT:** Division of Information Technology, *Systems Development Life Cycle*  
Report Number A-1011DOH-021

---

Attached is our report of the internal audit of the Division of Information Technology's, *Systems Development Life Cycle*. This report provides an independent evaluation of relevant internal controls relating to the Division's system development life cycle (SDLC) methodology and associated processes. The scope of our audit included current and past SDLC methodologies used during 2005 through 2010. Project management and information technology governance processes were not included in the scope of this engagement.

This audit was conducted by Michelle L. Weaver, C.I.S.A., and reviewed by Michael J. Bennett, C.I.A., Director of Auditing.

If you wish to discuss the report, please let us know.

JDB/mlw



## OFFICE OF INSPECTOR GENERAL INTERNAL AUDIT UNIT

### Division of Information Technology Systems Development Life Cycle

Report # A-1011DOH-021

June 1, 2012

**PUBLIC VERSION**

## EXECUTIVE SUMMARY

### ***What was reviewed:***

The Division of Information Technology's (DIT) systems development life cycle (SDLC) methodology and associated processes to determine if all phases are sufficiently addressed and it incorporates use of structured analysis, design, and development techniques.

### ***What was found:***

It was determined during our preliminary survey and process mapping that the Bureau of Application Development and Support (ADS) d

oes not adhere to either the Department of Health (Department) application development standards, application requirements standards, or draft application testing standards documents. As a result, we were unable to complete our second intended objective of determining if the SDLC is adhered to during application development, acquisition and changes to existing applications.

Furthermore, the DIT does not have a defined strategic plan for ADS to align goals and performance measures. As a result, ADS has not developed defined performance measures to track and monitor strategy implementation, project completion, resource usage, process performance and service delivery. Because of this, we determined that further testing would yield redundant findings and not provide additional value. All of the identified issues are essential to maintain continuity of operations in the event of high staff turnover as experienced by the DIT and ADS during the past two years.

In addition to the lack of compliance with internal application development standards we identified non-compliance with several external and some internal security and risk management policies.

### ***What is being recommended:***

The Bureau of Applications Development and Support should:

- ❖ Establish and maintain standards for all application developments and acquisitions;
- ❖ Incorporate quality assurance and management within the systems development life cycle standards to ensure all new application developments adhere to the standards;
- ❖ Define test plan documentation standards and incorporate the requirements into the application development standards;
- ❖ Identify, implement, monitor, and report applicable performance measures that are aligned with a Division-wide strategic plan and recommended application development standards; and
- ❖ Design standardized development procedures.

***Details supporting the statements listed in this Executive Summary can be found in the remainder of this report. DOH management agreed with all findings and has submitted corrective action plans, which have been included in this report. The Office of Inspector General will conduct a follow-up six months from the publication date of this report to assess the status of management's corrective actions.***

***All exempt and/or confidential information has been redacted from the public version of this report. Exempt information is only delivered to individuals appropriate to the activity that was reviewed. Requests to review or obtain the results of the exempt report content must submit a request to the Director of Auditing.***

## BACKGROUND

SDLC can be defined as the phases deployed during development or acquisition of a software or information system solution. There are many SDLC methodologies that can be used to effectively develop software or information systems. Some of the most commonly referenced methodologies include: Waterfall Method, Rapid Application Development (RAD), Joint Application Development (JAD), Rational Unified Processes (RUP) Prototyping, Iterative, and Agile.

A SDLC is applied to manage technology projects. It should document repeatable policy, procedures, and guidelines that support business needs and compliments an organization’s unique culture. A SDLC defines standard processes, exceptions to the process, and intended outcomes. Regardless of how the methodology and terminology is applied within an organization or how roles and responsibilities are defined... SDLC models should retain the flexibility to adapt to the size and complexity of systems, development schedule, and the lifespan of the solution. **Table 1** below list common SLDC phases:

**Table 1**

<b>Typical SDLC Phases:</b>	
*Terminology may vary and items may be grouped	
❖ Initiation/Inception	❖ Implementation
❖ Feasibility study	❖ Requirements study
❖ Requirements definition	❖ Detail Design
❖ Programming/Development/Acquisition	❖ Testing
❖ Installation/ Accreditations	❖ Post-Implementation review
❖ Establishing controls	❖ Data conversion
❖ Quality Assurance/ Verification	❖ Reconciliation
❖ Maintenance	❖ Disposal/Retirement

There are many roles and responsibilities involved from inception to implementing technology solutions, with some methodologies extending through the disposal phase. All of these roles and responsibilities do not reside within the organization’s information technology business unit. The business owner must also be involved as the overall manager of the project. The application development team is a member of the project team and is responsible for executing technical development of the business plan. The application development team should generally complete the assigned tasks, communicate effectively with owners and users by actively involving them in the development process, work according to local standards, and advise the project manager of necessary project plan deviations as a result of the technology component of the overall business solution. The application development team may consist of many roles such as analysts, computer programmers, database administrators, network administrators, etc.

It is important to note that though the DIT contains a Bureau whose primary responsibility includes development of software systems, this Bureau is not the only entity within DOH who is currently tasked with this role. There are Department information systems that were developed and are maintained by the organizational units themselves. This is commonly referred to as a distributed or decentralized information system. Decentralization requires coordination and standardization of Department expectations.

The objectives of our audit were to:

- ❖ Evaluate the DIT’s SDLC methodology and associated processes to determine if all phases are sufficiently addressed and it incorporates use of structured analysis, design, and development techniques.
- ❖ Determine if the SDLC is adhered to during application development, acquisition and changes to existing applications.

The scope of our audit included current and past SDLC methodologies. The DIT project management and DOH information technology (IT) governance processes were not included in the scope of this engagement.

ADS is comprised of seven teams, however only three teams were included within the scope of this engagement: the Medical Quality Assurance (MQA) team, the Health Management System (HMS) team, and the Enterprise Applications and Support (EAS)<sup>1</sup> team.

During our preliminary survey, ADS management indicated that IT Governance, Project Management, and the ADS processes are not aligned. There was an effort to improve alignment, however the acting chief for ADS changed three times during our audit engagement. Furthermore, the role of Chief Information Officer changed from two individuals in an acting position role and two individuals in the official position role during our audit engagement. The current Chief Information Officer is acting.

Our planned engagement methodology included conducting a detailed internal risk assessment and control analysis utilizing best practice, laws, rules, and regulations as criteria to establish high risk areas for which to conduct detailed testing. However, it was determined during our preliminary survey and process mapping that ADS does not adhere to Department application development standards, application requirements standards, or application testing standards. Furthermore, the DIT does not have a defined strategic plan for ADS to align goals and performance measures. As a result, ADS does not have defined performance measures to track and monitor strategy implementation, project completion, resource usage, process performance and service delivery. Thus, we determined that further testing would yield redundant findings and not provide additional value.

In addition to the lack of compliance with internal application development standards, we identified non-compliance with several external and some internal security and risk management policies.

---

<sup>1</sup> The EAS team is a recent merger of the .NET formerly known as the AAS team and the Enterprise Software Engineering Team (ESET) team.

## FINDINGS AND RECOMMENDATIONS

The following findings and recommendations address issues that should receive additional attention by management in an effort to help ensure positive and consistent outcomes when developing and acquiring new technological systems.

### FINDING 1

*The Bureau of Application Development and Support does not adhere to the Application Development Standards or the Application Requirements Standards documents.*

#### CONTRIBUTING FACTORS:

- Each ADS section has different business operations for which to align their development methodology.
- RUP was pushed too fast, not enough training was provided, and implementation lacked a plan.
- RUP became a burden due to the extensive processes and documentation.
- RUP did not support a collaborative team atmosphere between the customer and DIT.

#### RECOMMENDATIONS:

**1.1** The Bureau of Application Development and Support should refer to industry best practices to establish and maintain standards for all application developments and acquisitions. Ensuring the standards incorporate key elements such as approvals at key milestones.

**1.2** The Bureau of Application Development and Support should incorporate quality assurance and management within the systems development life cycle standards to ensure all new application developments adhere to the standards. The

#### What is required:

Both the Department *Application Development Standards* and the *Application Requirements Standards* documents indicate that DOH has adopted the Rational Unified Process (RUP) as the standard software development life cycle methodology to be used in all development efforts.

The Department of Health Information Technology, *Application Development Standards*, states,

*“Each project undertaken to develop application software is required to follow the RUP in some capacity... Every project that follows RUP should perform an assessment at the outset to determine the artifacts that are appropriate for use during that project. This enables the process to be flexible for specific needs.”*

#### What is best practice:

ISACA is an independent, nonprofit, global association. ISACA engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. ISACA publishes *Control Objectives for Information and related Technology* (COBIT). COBIT provides a framework of control objectives, management guidelines, and maturity models. COBIT version 4.1 is utilized as a best practice reference during this engagement. COBIT version 5 is scheduled for release in the spring of 2012.

COBIT Control Objective PO8.3 titled *Development and Acquisition Standards*, states,

*“Adopt and maintain standards for all development and acquisition that follow the life cycle of the ultimate deliverable, and include sign-off at key milestones based on agreed-upon sign-off criteria. Consider software coding standards; naming conventions; file formats; schema and data dictionary design standards; user interface standards; interoperability; system performance efficiency; scalability; standards for development and testing; validation against requirements; test plans; and unit, regression and integration testing.”*

#### What this means:

Because ADS does not adhere to any application development standards it is unlikely their current processes are strategically aligned with the Department's business needs. Also, applications delivered may not consistently meet target quality goals, objectives, or service levels.

The objectives of application development standards typically include:

- ❖ Acquire, develop, and maintain integrated and standardized application systems;
- ❖ Acquire and maintain applications that cost-effectively meet the defined business requirements;
- ❖ Establish common expectations about the process and documentation to be prepared;

*standards should be reviewed and revised periodically to ensure they reflect industry trends and actual application and/or system acquisition and development activities within the Department.*

**SEE PAGE 9 FOR  
MANAGEMENT'S RESPONSE**

- ❖ Ensure the development process is timely and cost effective;
- ❖ Define and establish expectations for newly developed, modified, reused and procured software;
- ❖ Defining the minimum requirements during each phase of the system development lifecycle;
- ❖ Define and consider application risk, size, complexity, application developer roles, and application owner roles; and
- ❖ Alignment with IT Governance, Project Management, and Change Management processes, as well as business strategy and security requirements.

**What was discovered:**

The Department's application development and requirements standards are not followed by the EAS, HMS or the MQA teams.

**EXHIBIT A** (pages 14-21) contains process maps drafted by internal audit staff in conjunction and approved by ADS management. Though management is aware of the RUP standards, the maps illustrate each of the development teams have implemented their own methodologies, utilize informal processes and artifacts, or a combination thereof which they feel best suites their customer base and unique development needs. The HMS team has implemented an agile scrum methodology, whereas the MQA team has implemented a hybrid methodology utilizing some of the RUP artifacts, and the EAS team primarily performs prototyping with little to no artifacts or documentation.

As indicated in the background of this report, SDLC models should retain the flexibility to adapt to the size and complexity of systems, development schedule, and the lifespan of the solution. Standards should define how these varying methodologies are applied through baseline processes, intended outcomes, and exceptions to achieve intended outcomes that are strategically aligned with the business need.

**Impact:**

In the absence of development standards, the Department is at risk for the following:

- ❖ Application and information system solutions do not satisfy business needs;
- ❖ Development methodologies and processes are not clear to all project members resulting in overall dissatisfaction; and
- ❖ Key phases of development are not fully addressed resulting in potential lack of functionality, data integrity issues and security risks.

**FINDING 2**

Documented test plans are not developed for all applications and maintenance releases.

**CONTRIBUTING FACTORS:**

- The Division of Information Technology has experienced very high staff turnover and transition for the past two years.
- The Chief Information Officer and the Chief of Application Development and Support positions have been held by varying individuals in an acting capacity for most of the past two years.

**RECOMMENDATIONS:**

2.1 The Bureau of Application Development and Support should define test plan documentation standards and incorporate the requirements into the application development standards.

**SEE PAGE 9 FOR  
MANAGEMENT'S RESPONSE**

**What is best practice:**

COBIT 4.1, Control Objective A17.2 titled *Test Plan*, states,

*“Establish a test plan based on organization wide standards that defines roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.”*

**What this means:**

Application testing ensures the solution meets the intended business purpose and is free from errors before releasing into production. A test plan ensures the business owner and the IT stakeholders agree as to the expected outcomes and test strategy to determine if those outcomes are met.

**What was discovered:**

ADS provided a draft document titled *Division of Information Technology, DOH Application Testing Standards, Global Artifact, Version 1.0*. This document was drafted and last revised in 2006. Its stated purpose is “...to provide a set of software application testing guidelines for Florida Department of Health (DOH) applications to ensure that all applications are properly testing, in order to pursue reliable and quality software. Software testing standards are good reference frameworks. Standards promote a repeatable and predictable software testing process.”

It is our understanding, based upon the development of process maps (See **EXHIBIT A**, pages 14-21) created in collaboration with ADS management as well as interviews, that all new applications and maintenance releases do not have a documented test plan.

In attempt to quantify our preliminary finding we requested a 15% sample of systems documentation associated with initiation, inception, design, development, testing, implementation, maintenance, and enhancements from EAS, HMS, and MQA to determine the level of adherence to the established standards. The Bureau of ADS was able to provide insufficient documentation to support these activities.

**Impact:**

A plan is essential to preparing for software testing. It determines and documents the agreed upon scope or test coverage, methodology, responsibilities, requirements, acceptance criteria and schedule. There are many types of tests that can be executed during the different phases of application and system development. All of these tests are designed to achieve assurance the solution is delivering the intended results.

**FINDING 3**

The Bureau of Application Development and Support does not have defined performance measures. Moreover, the Division of Information Technology does not have a defined strategic plan which the Bureau of ADS can align their goals and performance measures.

**IMPACT:**

- The Bureau of Application Development and Support cannot improve process capabilities and performance without measuring how well they are currently meeting goals.
- The Bureau of Application Development and Support cannot support the value they deliver to the Division of Information Technology or the Department without reliable or valid data that is defined and measured.

**RECOMMENDATIONS:**

**3.1** The Bureau of Application Development and Support should identify, implement, monitor and report applicable performance measures that are aligned with a Division-wide strategic plan and the recommended application development standards. The performance measures should provide value by measuring progress toward objectives and focus on customer needs or agreed upon service levels rather than IT goals.

**Note:** The lack of strategic planning for all of the Department's administrative functions has been identified as a control weakness. This item will be addressed and tracked in a separate project.

**SEE PAGE 9 FOR  
MANAGEMENT'S RESPONSE**

**What is best practice:**

COBIT 4.1, states,

*"Performance measurement is essential for IT governance. It is supported by COBIT and includes setting and monitoring measurable objectives of what the IT processes need to deliver (process outcome) and how to deliver it (process capability and performance). Many surveys have identified that the lack of transparency of IT's cost, value and risks is one of the most important drivers for IT governance. While the other focus areas contribute, transparency is primarily achieved through performance measurement."*

Furthermore, COBIT 4.1 includes performance measurement as one of the five IT Governance focus areas.

*"Performance measurement tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting."*

COBIT also defines goals and metrics at three levels:

- ❖ IT goals and metrics that define what the business expects from IT and how to measure it;
- ❖ Process goals and metrics that define what the IT process must deliver to support IT's objectives and how to measure it; and
- ❖ Activity goals and metrics that establish what needs to happen inside the process to achieve the required performance and how to measure it.

**What this means:**

Performance measurement helps determine actual performance levels and aides in detecting problems before it is too late.

Performance measures are applied differently within the organizational structure. For example:

- ❖ Division goals and metrics define what the business expects and how to measure it;
- ❖ Process goals and metrics define what IT processes (Bureaus and Sections) must deliver to support the Division's objects and how to measure it; and
- ❖ Activity goals and metrics establish what needs to happen inside the process to achieve the required performance and how to measure it.

**What was discovered:**

Though some data is available and performance measures have been historically discussed, neither the Bureau nor the individual sections within have defined and formalized performance measures for applications development.

**Impact:**

Without performance measures, the Bureau of Application Development and Support cannot measure the quality of their activities and services to the Department. Strategies for improvement should be based upon sound quality measurement, deliver measurable results, and align with the Departments objectives.

**FINDING 4**

*FINDING 4 AND THE ASSOCIATED RECOMMENDATIONS HAVE BEEN CLASSIFIED AS EXEMPT AND/OR CONFIDENTIAL IN ACCORDANCE WITH SECTION 282.318(4)(F), FLORIDA STATUTES AND THUS IS NOT AVAILABLE FOR PUBLIC DISTRIBUTION.*

Confidential material is only delivered to individuals appropriate to the activity reviewed.

All others who feel you have a justified purpose to view or obtain the results of this finding must submit a request to the Director of Auditing stating your name, business entity, current title, phone number, and the report number you are requesting. Please provide an explanation as to the reason for your request. Once approved, a time and date will be established for you to view the requested documentation under the supervision of the Internal Audit staff.

**MANAGEMENT'S RESPONSE**

Recommendation	Management's Response
<p><b>1.1</b> The Bureau of Application Development and Support should refer to industry best practices to establish and maintain standards for all application developments and acquisitions. Ensuring the standards incorporate key elements such as approvals at key milestones.</p>	<p>We concur. DIT is re-examining the systems development life cycle standards utilized by the Bureau of Application Development and Support. The primary SDLC methodology currently employed is Agile Scrum. DIT will also review tools currently owned for additional options and functionality. Documentation will be updated to reflect standards for all application development and acquisition.</p> <p>ANTICIPATED COMPLETION DATE: MAY 30, 2013</p>
<p><b>1.2</b> The Bureau of Application Development and Support should incorporate quality assurance and management within the systems development life cycle standards to ensure all new application developments adhere to the standards. The standards should be reviewed and revised periodically to ensure they reflect industry trends and actual application and/or system acquisition and development activities within the Department.</p>	<p>We concur. DIT is re-examining the systems development life cycle standards utilized by the Bureau of Application Development and Support. The primary SDLC methodology currently employed is Agile Scrum. DIT is aware one software development methodology may not be suitable for use by all projects based on technical, project and team considerations. DIT accepts the use of linear and iterative development methodologies as appropriate. Documentation will be updated to address quality assurance and project management activities as part of the development life cycle. DIT will review tools currently owned for additional options and functionality.</p> <p>ANTICIPATED COMPLETION DATE: MAY 30, 2013</p>
<p><b>2.1</b> The Bureau of Application Development and Support should define test plan documentation standards and incorporate the requirements into the application development standards.</p>	<p>We concur. Testing is an integral part of planned software development. DIT will define a standard test plan document and incorporate standards for unit, system and user acceptance testing into the application development standards.</p> <p>ANTICIPATED COMPLETION DATE: MAY 30, 2013</p>
<p><b>3.1</b> The Bureau of Application Development and Support should identify, implement, monitor and report applicable performance measures that are aligned with a Division-wide strategic plan and the recommended application development standards. The performance measures should provide value by measuring progress toward objectives and focus on customer needs or agreed upon service levels rather than IT goals.</p>	<p>We concur. DIT will draft and implement a methodology for performance metrics which adheres to application development standards and our strategic plan. The performance metrics methodology will focus on service level agreements and customer goals.</p> <p>ANTICIPATED COMPLETION DATE: MAY 31, 2013</p>

## SUPPLEMENTAL INFO

Section 20.055, *Florida Statutes*, charges DOH's Office of the Inspector General responsibility to provide a central point for coordination of activities that promote accountability, integrity, and efficiency in government. Audits are conducted to review and evaluate internal controls necessary to ensure the fiscal accountability of DOH.

The audit was conducted in conformance with International Standards for the Professional Practice of Internal Auditing, issued by the Institute of Internal Auditors (January 2009), as provided by Section 20.055(5)(a), *Florida Statutes*, and as recommended by *Quality Standards for Audits by Offices of Inspector General (Principles and Standards for Offices of Inspectors General, Association of Inspectors General, 2004 Revision)*.

The audit was conducted by Michelle L. Weaver, Certified Information Systems Auditor, under the supervision of Michael J. Bennett, Certified Internal Auditor, Director of Auditing.

Our planned methodology included a detailed internal risk assessment and control analysis utilizing best practice, rules and policy to establish high risk areas for which to conduct detailed testing. It was determined during our preliminary survey and process mapping that detailed testing would yield redundant findings and not provide additional value.

## CLOSING COMMENTS

We would like to thank management and staff of the Division of Information Technology, Bureau of Application Development and Support for providing their cooperation and assistance to us during the course of this audit.

Copies of this report can be found on our website at: [www.doh.state.fl.us/ig/Audit.htm](http://www.doh.state.fl.us/ig/Audit.htm)

Questions or comments related to the information provided in this report should be addressed to the Director of Auditing, Florida Department of Health, at (850) 245-4141.

**EXHIBIT 1**

**Enterprise Applications Systems (EAS): New System Development Process**

As of January 18, 2011

Project # A-1011DOH-021, *Systems Development Life Cycle (SDLC)*

**Legend:**

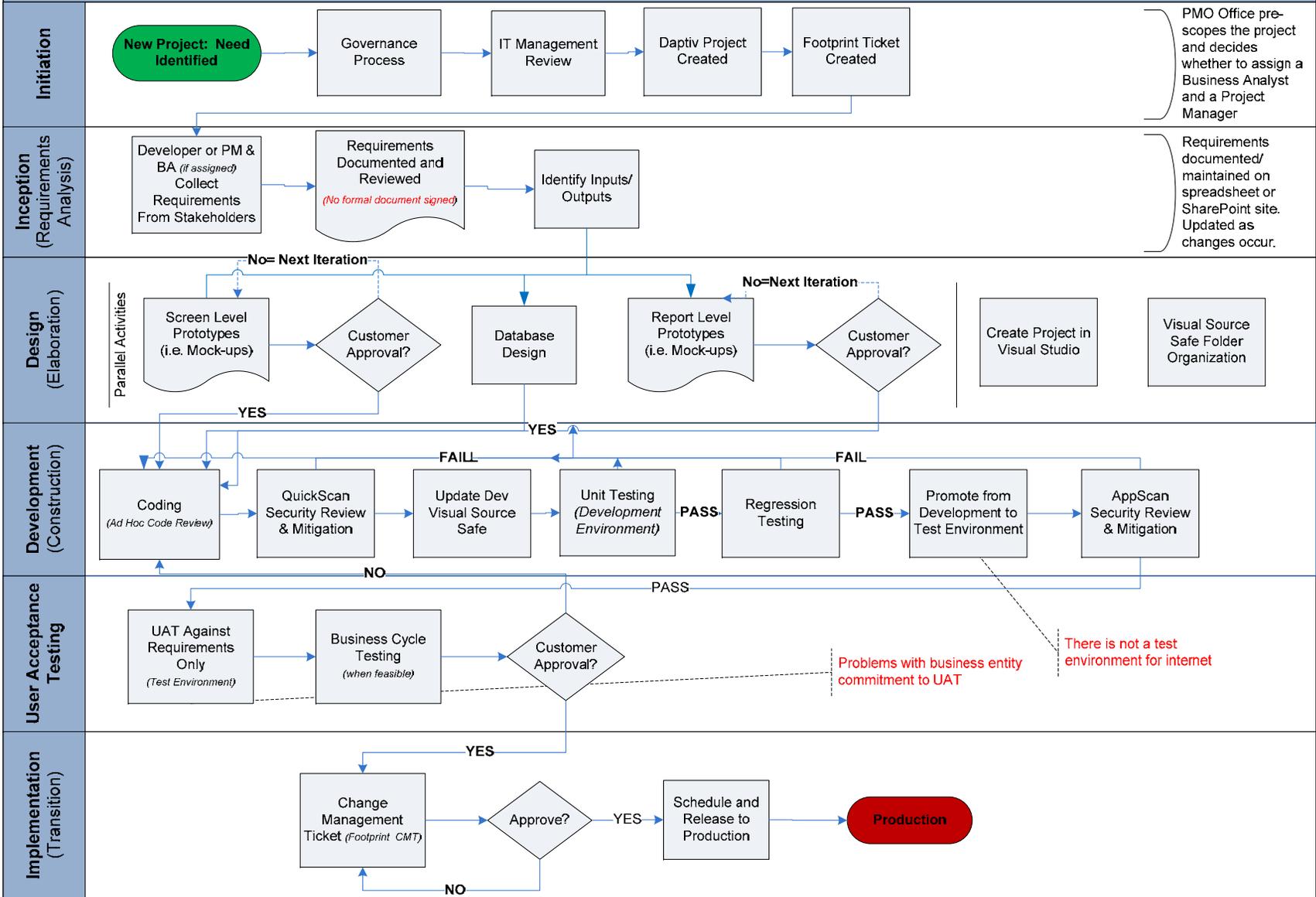
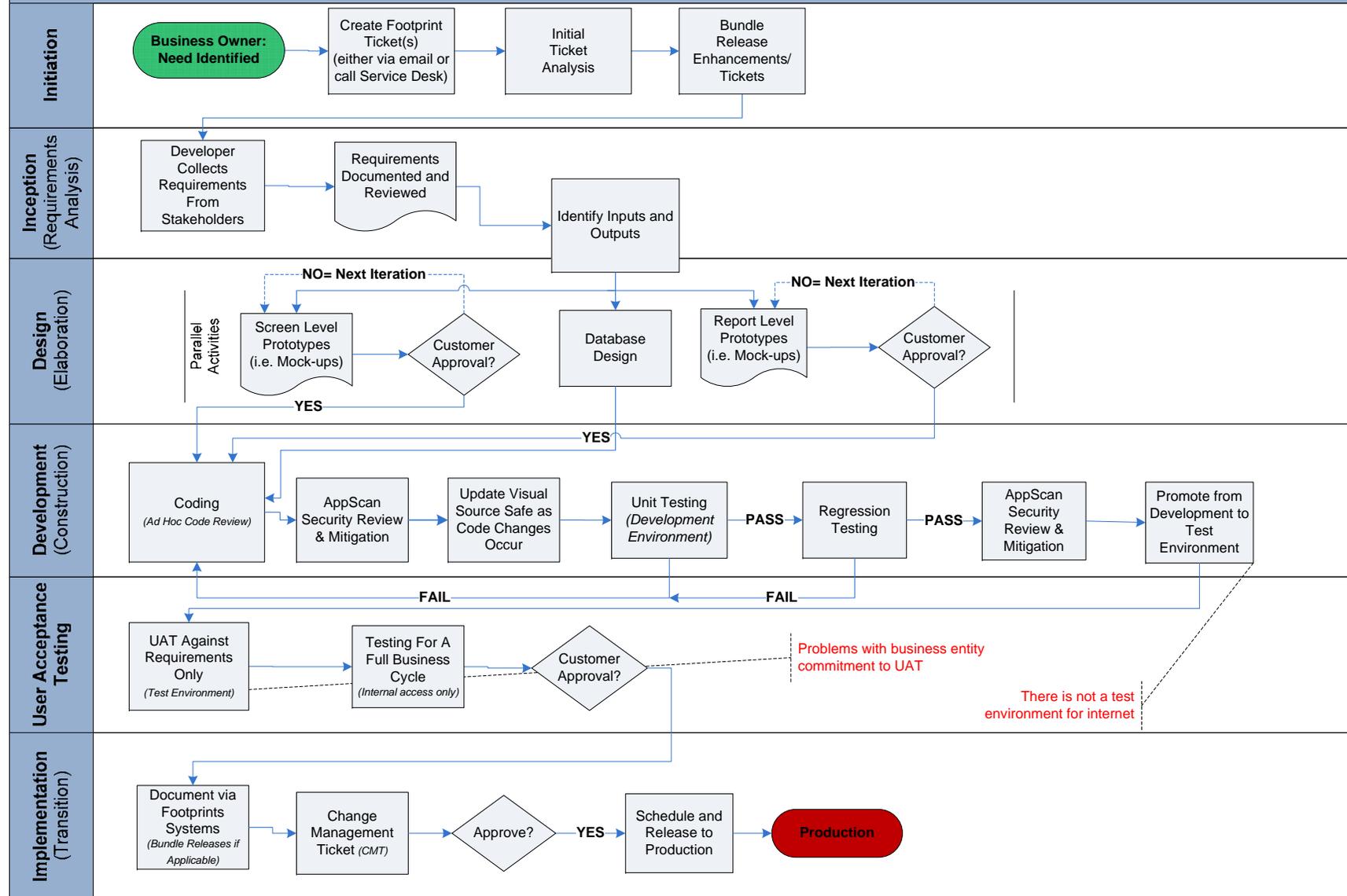


EXHIBIT A (CONTINUED)

Enterprise Applications Systems (EAS): System Enhancement Process  
 As of January 18, 2011  
 Project # A-1011DOH-021, *Systems Development Life Cycle (SDLC)*

Legend:



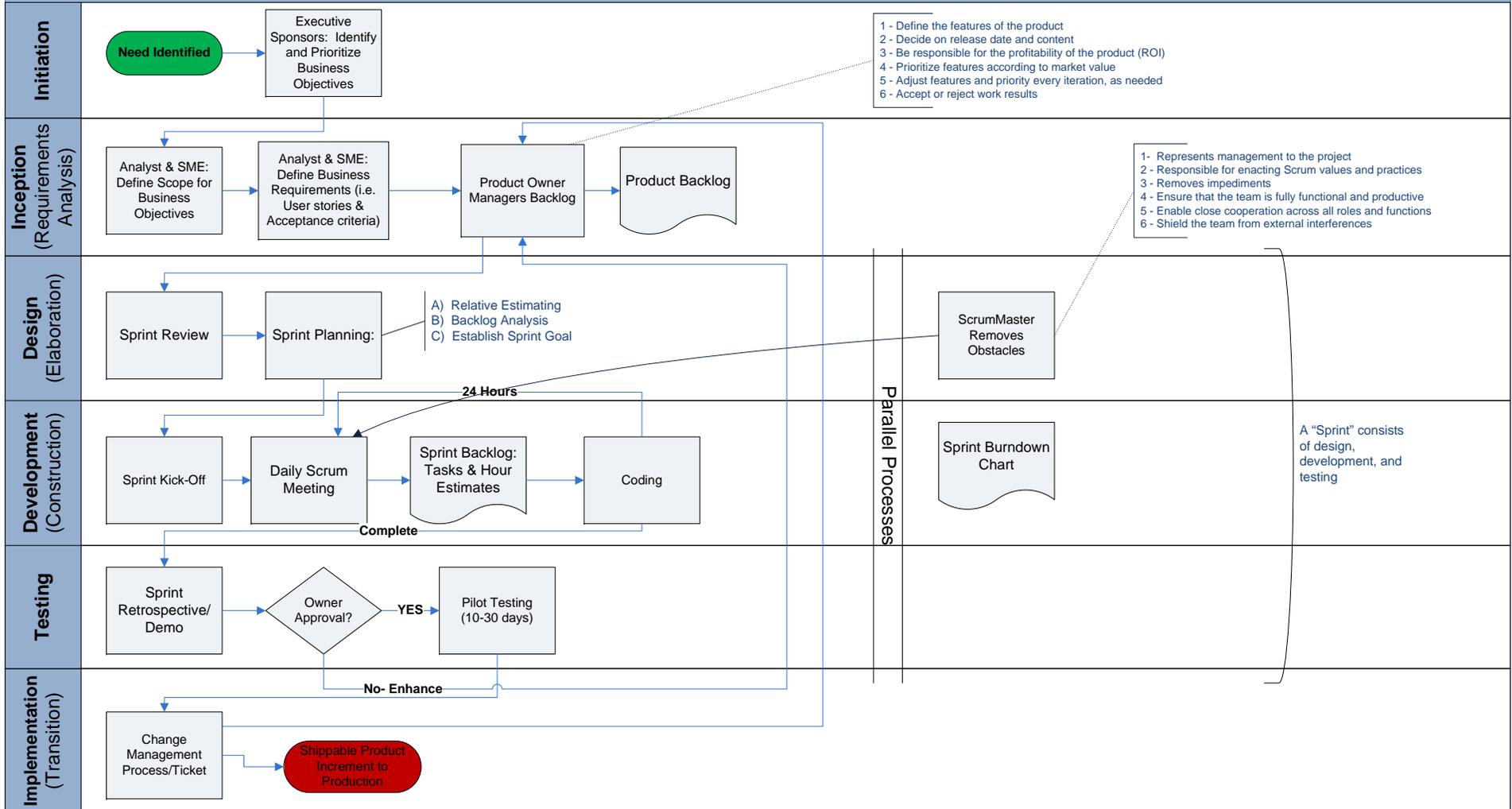
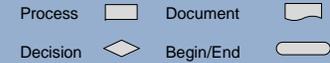
**EXHIBIT A (CONTINUED)**

**Health Management Systems (HMS): System Development Process**

As of January 18, 2011

Project # A-1011DOH-021, *Systems Development Life Cycle (SDLC)*

**Legend:**



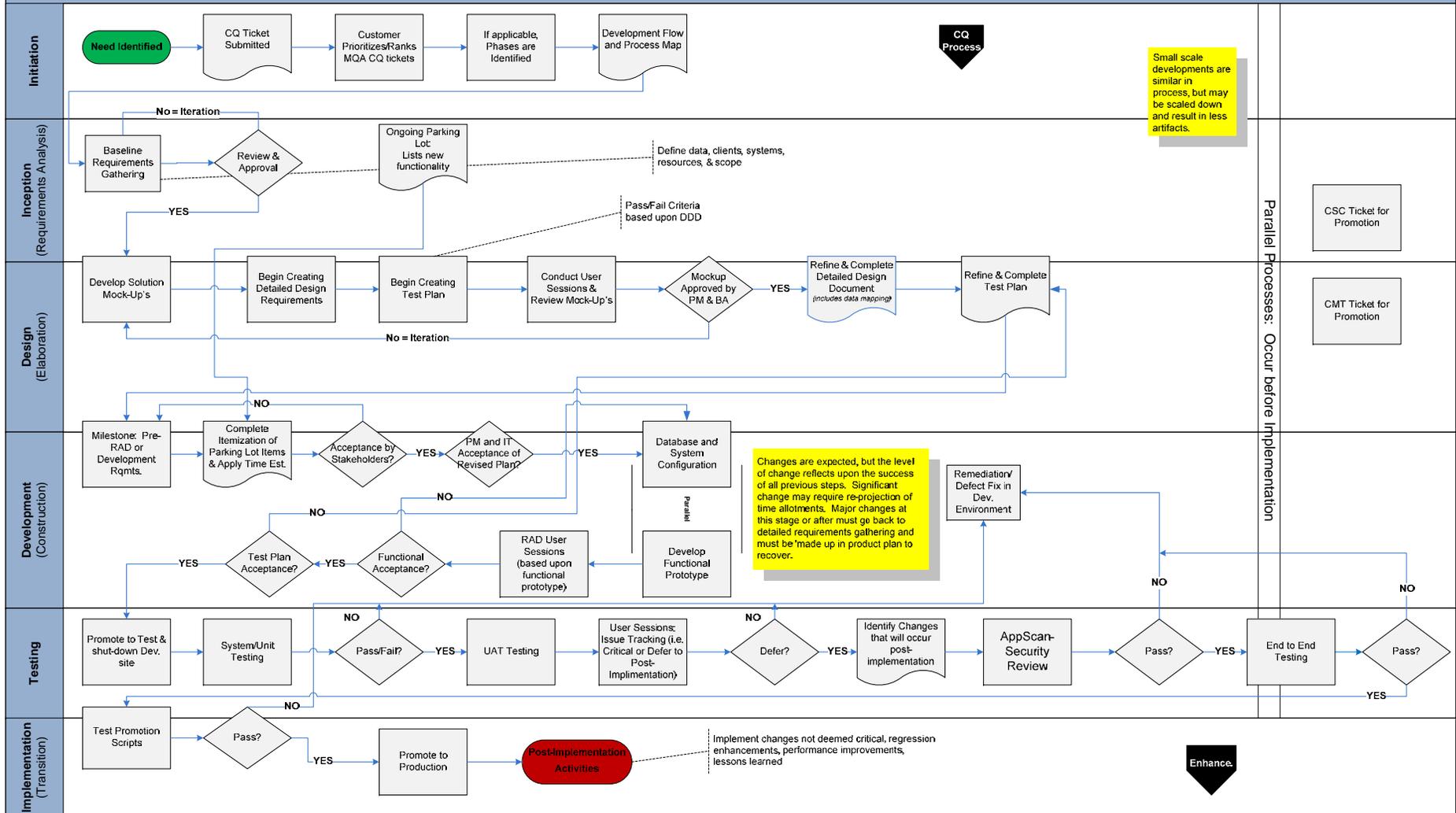
**EXHIBIT A (CONTINUED)**

**Medical Quality Assurance (MQA): Large Scale Development Process**

As of January 14, 2011

Project # A-1011DOH-021, Systems Development Life Cycle (SDLC)

<b>Legend:</b>		<b>Acronomy:</b>	
Process	Document	CQ- ClearQuest	RAD- Rapid Application Development
Decision	Begin/End	PM- Project Manager	CSC- Customer Service Center
		BA- Business Analyst	



# Medical Quality Assurance (MQA): ClearQuest & CSC Ticket Process Flow

As of January 14, 2011

Project # A-1011DOH-021, *Systems Development Life Cycle (SDLC)*

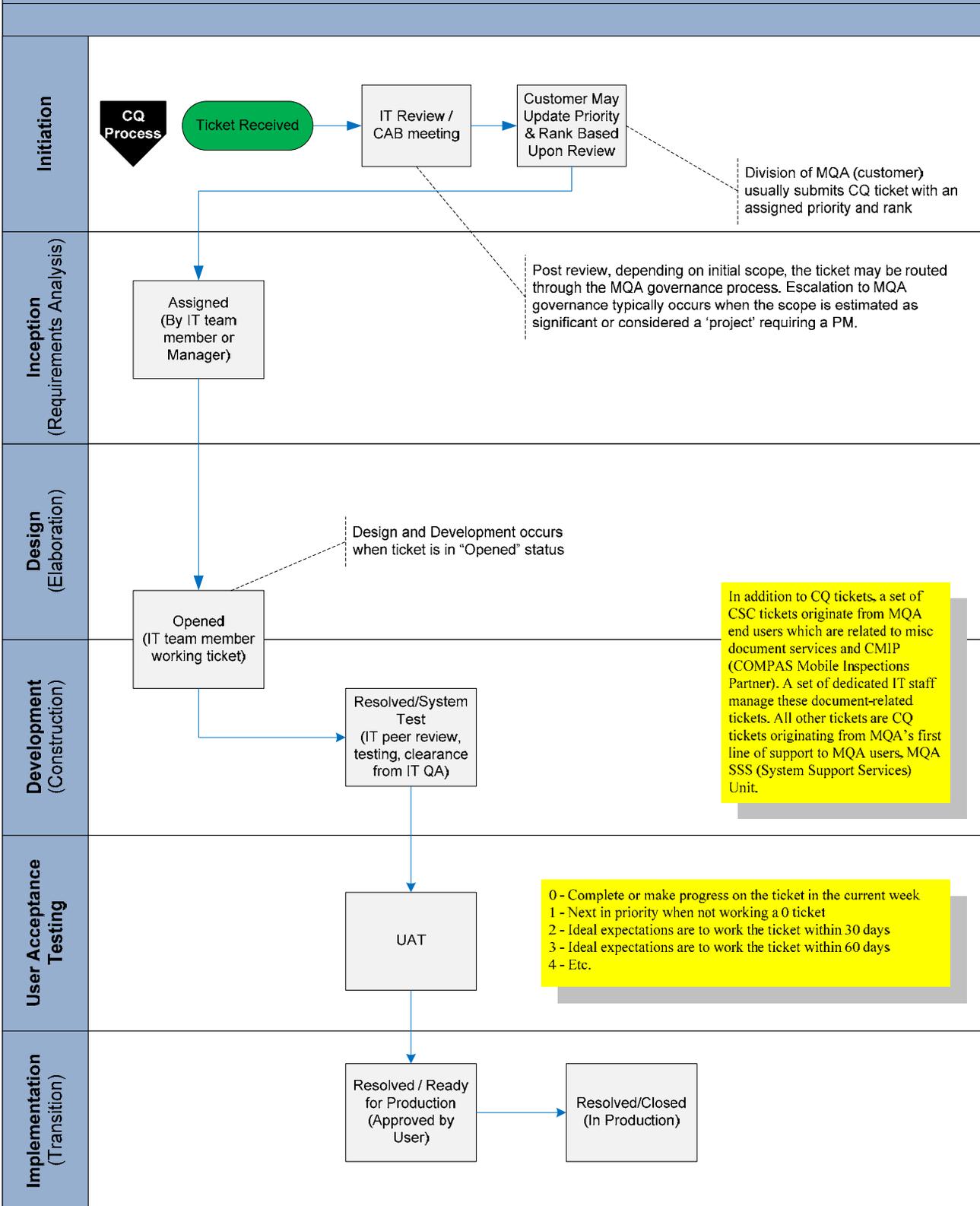


EXHIBIT A (CONTINUED)

# Medical Quality Assurance (MQA): Enhancement to existing system

As of January 14, 2011

Project # A-1011DOH-021, *Systems Development Life Cycle (SDLC)*

**Legend:**

- Process 
- Document 
- Decision 
- Begin/End 

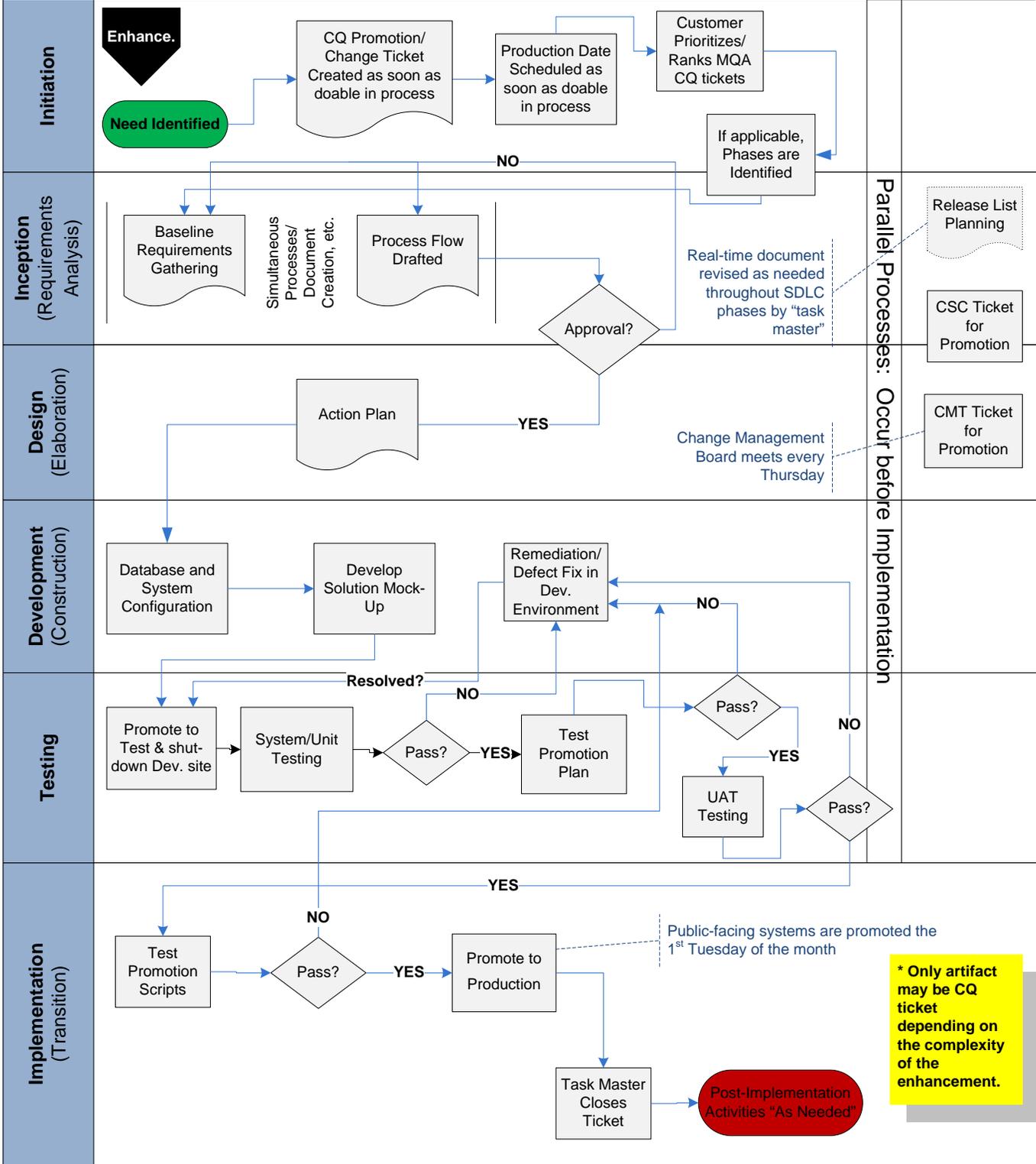


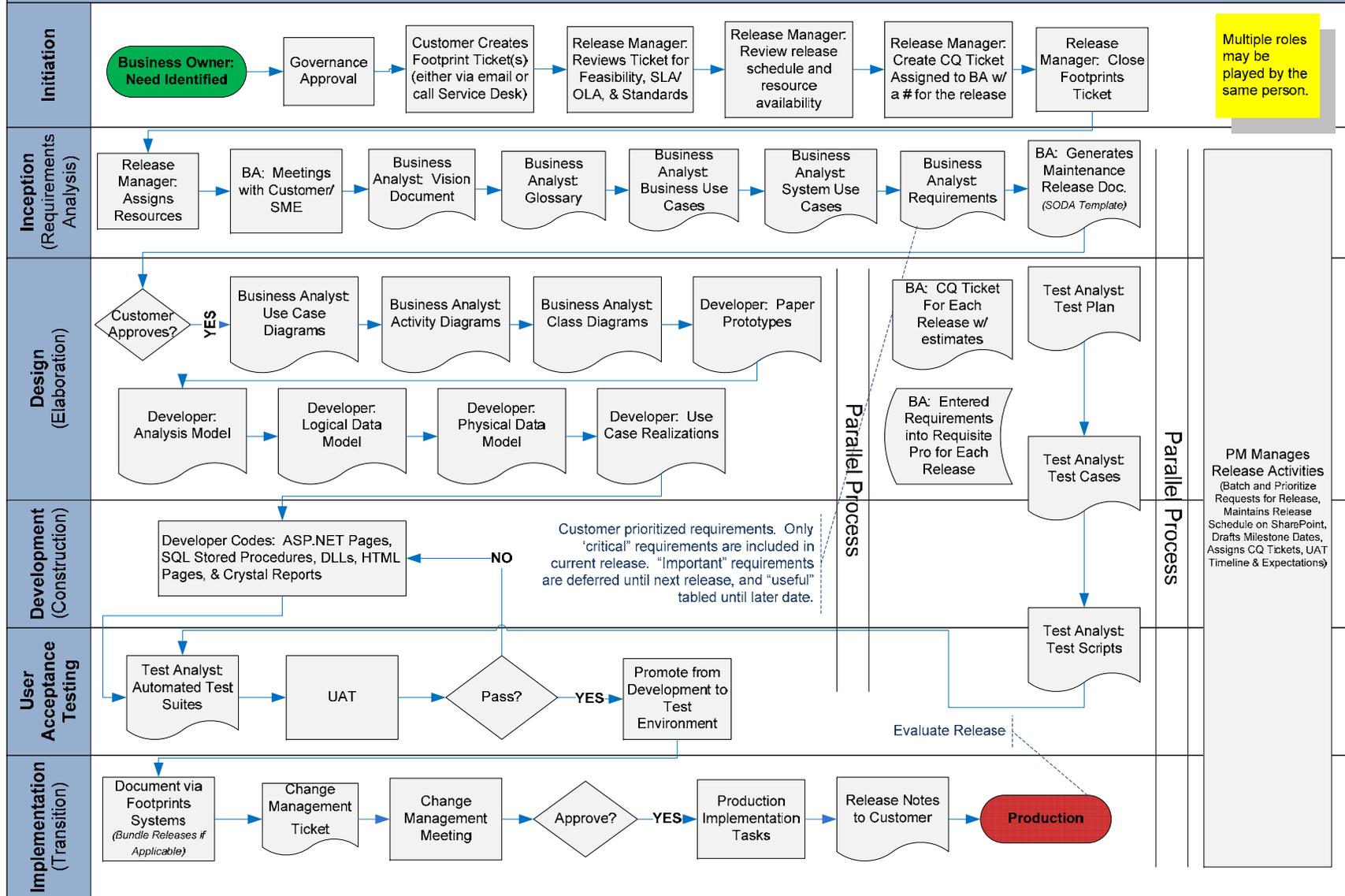
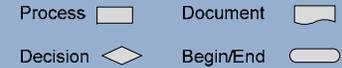
EXHIBIT A (CONTINUED)

Enterprise Software Engineering Team: New System Development and Major Enhancement Process

As of March 7, 2011

Project # A-1011DOH-021, *Systems Development Life Cycle (SDLC)*

Legend:



**EXHIBIT A (CONTINUED)**

**Enterprise Software Engineering Team: System Maintenance Process**

As of March 7, 2011

Project # A-1011DOH-021, *Systems Development Life Cycle (SDLC)*

**Legend:**

