



John A. Carey
Inspector General

OFFICE OF INSPECTOR GENERAL PALM BEACH COUNTY

“Enhancing Public Trust in Government”

Audit Report 2015-A-0001 December 23, 2014 Redacted

*“Provide leadership in the promotion of accountability and
integrity of Government in Palm Beach County”*



**OFFICE OF INSPECTOR GENERAL
PALM BEACH COUNTY
AUDIT OF CHILDREN'S SERVICES COUNCIL
INFORMATION SYSTEMS MANAGEMENT
AUDIT REPORT: 2015-A-0001**

John A. Cary,
Inspector General

"Enhancing Public Trust in Government"

SUMMARY RESULTS AT A GLANCE

What We Did

We reviewed Children's Services Council (CSC) Information Management (IM) Security programs. Our overall objective was to determine if controls are in place to adequately safeguard CSC's information systems and ensure their continuous operation.

Our review included physical security, information management security, access security, segregation of duties and disaster recovery planning. We also reviewed CSC's Business Process Application Support and actions taken to mitigate medium and high risk areas identified in a prior IT systems review contracted by CSC. Our review covered the period October 1, 2012 through May 31, 2014.

What We Found

CSC's Information Management Security program is well managed and controlled. Both physical and access security are well documented with policy, procedures, and security standards for both site security and CSC data, including sensitive data such as protected health information (PHI). CSC Staff and outside contractors interfacing with CSC data systems are required to follow the CSC security requirements. Sufficient resources are in place to secure the IM

infrastructure. However, we noted that CSC has not had a system penetration test performed on their IM network. A penetration test would provide CSC with greater assurance that there are no significant unknown vulnerabilities in their security protocols.

Configuration management is effectively controlled through tracking of all requests to address computer issues and necessary hardware and/or software changes. However, although CSC staff follows a sound process for change control, there is no formal documentation of the change control processes.

With regard to segregation of duties, we found that because of the small staff size in the IM function, it would be difficult for CSC to establish traditional segregation of IM duties. However, there are sufficient mitigating controls in place to reduce the opportunities for unauthorized changes to the applications, data, or operating systems.

We found that CSC's contingency planning is well documented. CSC has contracted with a vendor to provide both routine back up for their data and applications and a disaster recovery "hot site" capability. However, CSC has not performed and documented a full test of its IM disaster recovery plan.

Additionally, although third parties are required to have disaster planning in place for CSC applications and data, third party support is not formally addressed in the CSC Emergency Management Guidelines.

We found that CSC's IM function effectively supports CSC's business applications and business processes. As part of its Strategic Plan CSC has designed its organizational goal planning to connect the IM support tasks with the overall organizational strategy. This resulted in identifying 89 specific tasks assigned to IM to adequately support CSC's mission. We found that under the leadership of the IM Director, the IM staff has completed 95.5% of these supporting tasks.

As part of our audit we also reviewed actions taken by CSC to address the results of an IT risk assessment performed by Computer Aid Inc. (CAI) in 2011. The CAI risk assessment resulted in 63 recommendations to address areas rated as low, medium and high risk. CSC has completed 55 (87%) of these recommendations and six (9%) are 75% to 90% completed. The two remaining

recommendations are addressed on page 10 and page 15 of this report.

What We Recommend

We made 4 recommendations to assist the CSC management in improving IM controls. CSC IM staff need to:

- Work with CSC management to contract for a third party penetration test,
- Formally document the change control process,
- Perform and document a full disaster recovery test, and
- Include third party support in its Emergency Management Guidelines.

In its response, CSC agreed with our recommendations and indicated it is taking or will take action to address each recommendation. CSC's response is included as Attachment 1.

BACKGROUND

Children's Services Council of Palm Beach County (CSC), an independent district established by voters in 1986, provides leadership, funding and research on behalf of children so they grow up healthy, safe, and strong. CSC's mission "is to enhance the lives of children and their families and enable them to attain their full potential by providing a unified context within which children's needs can be identified and resolved by all members of the community."



To achieve its mission, the CSC applies a system-of-care model that offers prevention and early intervention services to children and families. In 2013-2014 CSC's budget totaled \$110,707,741 of which \$80,112,448 funded programs that provide support for 38 community organizations.

To meet its information technology needs, CSC employs a staff of 10 employees who report to the Director of Information Management. These employees provide support for a diverse set of applications and data systems that serve the needs of both CSC staff and the many external provider agencies that assist CSC in carrying out its mission.

OBJECTIVES, SCOPE AND METHODOLOGY

Our overall objective was to determine if controls are in place and operating effectively to adequately safeguard CSC's information systems and ensure their efficient, effective and continuous operation. Our audit included but was not limited to reviewing policies, procedures and activities in the following areas:

1. General Controls:
 - a. Information Management Security,
 - b. Access Security Controls,
 - c. Configuration Management Processes,
 - d. Segregation of Information Management Duties, and
 - e. Contingency/Disaster Planning
2. Business Process Application Support
3. Actions taken to mitigate medium and high risk areas identified in CSC's Information Technology/Systems Review.

Our audit covered the period October 1, 2012 through May 31, 2014.

This audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

INFORMATION MANAGEMENT SECURITY**INFORMATION MANAGEMENT SECURITY IS BUILT AROUND THE HIPPA PROTECTED HEALTH INFORMATION (PHI) STANDARDS**

We reviewed information management security areas that addressed: Information Management staffing (job descriptions, reporting and assigned responsibilities); System infrastructure security; System resources inventories; Security policies (including security awareness, training, and compliance); Security as applied to third party vendors and users; and Security monitoring/reporting.

Staffing

The organizational structure for the Information Management (IM) staff is a “flat structure” with all staff members reporting directly to the IM Director. Job descriptions are well written with all necessary criteria for each job clearly documented. Documentation includes essential functions, knowledge, skills, software/equipment knowledge requirements, and minimum qualifications. There are nine job descriptions covering the ten staff positions in IM. To get a full understanding of their IM duties and responsibilities we interviewed all 10 staff members for this report.

Infrastructure and Resources

Control over the operating systems and the network are managed by the Network Engineer and the Network Database Administrator (System Team). This includes controls over the network architecture, firewall, virus/malware protection, server support and maintenance, operating system software (including patches and updates), and reporting. The System Team monitors and reports on the status of all operating systems and network systems including security incidents.

Policy and Compliance

Because of the nature of the Protected Health Information (PHI) collected and used by CSC and its member agencies, the CSC has adopted a series of security policies based on the Health Insurance Portability and Accountability Act (HIPPA) standards. This includes such policies as the “HIPPA Sanction Policy and Procedure,” “HIPPA Acceptable Use Policy,” and the “Technology/Social Media Usage Policy.” We reviewed the CSC HIPPA based policies and found that they adequately address the HIPPA standards.

In order to ensure staff follows the HIPPA based policies, the CSC has adopted a policy, the Workforce Education and Training Policy that requires all new employees of CSC to be trained as part of the employee orientation. In addition, all employees receive annual “update/refresher” training to stay current with the HIPPA requirements and regulations. Each employee is also required to sign a PHI non-disclosure “Confidentiality Agreement.”

The CSC HIPPA Risk Analysis and Ongoing Risk Management Policy and Procedure require a risk analysis “at least every two years”. This risk review included the four areas of CSC’s policy/procedures for HIPPA compliance in handling PHI. These four areas are designated as administrative, physical, technical, and organizational. We reviewed the risk analysis report dated January 2013 conducted by VMC, Inc. and found that CSC was rated “excellent” in the four designated HIPPA risk areas.

Third Parties

When dealing with third parties (parties), other agencies and vendors, the CSC requires a “Business Associate Agreement” (agreement) as part of the contractual relationship. This agreement requires these parties to comply with HIPPA requirements as they apply to PHI. (The parties agree not to misuse or disclose PHI data.) These parties must implement necessary administrative, physical and technical safeguards to protect the PHI data. The parties also agree to mitigate any harmful effects of disclosure violations and report any violations or breaches to CSC within 10 days of the incident. Violations of the agreement may result in the termination of the associated third party contract with CSC.

As part of this audit, we reviewed four vendor contracts identified in the applications inventory, two agency contracts, the email vendor contract, and the backup/recovery contract. All agency and vendor contracts reviewed included the required business associates agreement that mandates compliance with HIPPA privacy and security rules.

Monitoring

In accordance with the CSC HIPPA Accountability Audit Control Policy the PHI access information is to be logged, reported and reviewed monthly. A sample of this monthly report was provided to us by CSC. These monthly reports are sent to each program officer and require feedback to CSC in accordance with their contract. Access deviations are monitored by the CSC HIPPA Security Officer. When necessary, deactivation of the account is done by either the CSC program officer or a system administrator using an IssueTrak ticket to log the action.

ACCESS SECURITY CONTROLS

CSC HAS STRONG MANAGEMENT, PHYSICAL, LOGICAL, AND PASSWORD SECURITY

We reviewed access security to the CSC IM systems including: Physical access to CSC Offices, Computer Server Room, and Network Communication Equipment; Network access through the CSC; Communications Equipment and Firewall appliances; Logical (Password) access to various applications and databases (supported both internally and in some cases hosted by third parties) and Email archiving.

Physical Access



Network Communications

The network is protected by a network security firewall appliance. The system provides reporting of intrusion alerts that includes email to system administration staff. The system is protected from malware such as viruses, worms, trojans, spyware and adware by virus protection software. The software product is a client-server solution that protects laptops, desktops, Windows, Macs and servers. Status graphs and reports by the firewall appliance and virus protection software provided security status alerts to the system administration staff. The CSC maintains a public wireless network that is separate (isolated) from the secure production network used by employees and contracted third parties.

Logical Access

All logical (password) access to the CSC application programs (and databases) is provided through an IssueTrak request to the CSC Security Officer for processing. At the CSC the first point of contact for all IssueTrak requests is the Help Desk Coordinator, who also serves as the Security Officer. The roles and responsibilities of the Security Officer are detailed in the HIPPA Security Officer Responsibilities policy. The Help Desk Coordinator provides copies of all IssueTrak tickets to the IM Director for review.

As previously described, the security of the PHI data follows the CSC's HIPPA based standards. Strong password protection is standardized by the CSC's HIPPA User Identification and Authentication policy. This policy standard is based upon the Microsoft password best practices.

The CSC Security Officer and Privacy Officer are required to report, based on the HIPPA

Microsoft Password Standard, best practice

Password complexity policies are designed to deter brute force attacks by increasing the number of possible passwords.

When password complexity policy is enforced, new passwords must meet the following guidelines:

- The password does not contain the account name of the user.
- The password is **at least eight characters long**.
- The password contains characters from **three of the following four categories**:
 1. Uppercase letters (A through Z)
 2. Lowercase letters (a through z)
 3. Digits (0 through 9)
 4. Non-alphanumeric special characters; such as: exclamation point (!), dollar sign (\$), number sign (#), or percent (%).

You should use passwords that are as long and complex as

Security Incident Response Policy, any security incidents utilizing the CSC's Security Incident Report form. The policy states, "Following the identification of a security incident, the first priority must be to communicate the details of the incident to the IM Director to expeditiously log and begin resolving the issue."

Email Archiving

In order to protect and archive all email traffic the CSC utilizes a software package that filters incoming email for spam and archives all incoming email. Internal emails and emails sent from CSC are stored in on-site journals. All CSC email journals are archived in off-site storage. This email archive protects CSC against missing emails that could violate public record laws. Our sample contract review included the email vendor contract with CSC.

Audit Observation

While we did not identify any reportable deficiencies during our review of access security controls, we observed that CSC has not conducted penetration testing to determine if there are any unknown vulnerabilities in their network security. Such a test would provide CSC with an added level of assurance. In discussing this with the Director of Information Management, he indicated that CSC was budgeting for a penetration test in Fiscal Year 2015

Recommendation:

1.) CSC Management should contract with a third party information technology specialist to perform penetration testing to ensure network and logical access security cannot be compromised.

Management Response:

CSC acknowledges that a third party specialist should perform penetration testing and has entered into an agreement with Altius Information Technologies, Inc. to complete these tests by December 26, 2014.

CONFIGURATION MANAGEMENT

CSC HAS SOUND CONFIGURATION MANAGEMENT PROCESSES

Configuration Management processes reviewed included; new system development or procurement, help (service) desk support, change control, and maintenance of operating systems software.

New System Development

When CSC considers implementing a new system, a "project assessment" needs to be performed. Best practices in Information Management calls for the use of a system

development life cycle process (SDLC) assessment. The CSC utilizes their own hybrid form of this process documented as the “Information Management Project Lifecycle.”

The first steps in the CSC process include the submission of an IssueTrak ticket with attached supporting documentation for an Initial Project Assessment. These processes result in the development of a Project Charter which is in effect the “business case” for the project. The result of these first steps is a “Go or No Go Decision.” (See Attachment 2, “Initial Project Assessment.”)

Following these steps, if a “Go” decision is made the project moves to the Project Lifecycle steps. (See Attachment 3, “Project Lifecycle.”) The combination of the Project Assessment steps and Project Lifecycle steps provide the CSC IM staff with a sound structured process for decision making and plan execution.

Help Desk and Change Control Processes

The help desk is supported through the use of IssueTrak tickets for logging ‘incidents.’ The help desk is the single point of contact for the users of the CSC IM systems. Incidents can be minor such as forgetting your password. Repeated incidents of the same type can be classified as a “problem” and may require further investigation. Root cause analysis of a problem may identify the need for a “change” to a system/application. An incident being reclassified as a problem that results in a system change is not an uncommon practice in IM management. There are best practices for service support in information management such as the Information Technology Information Library (ITIL) which follows this standard practice.

CSC uses IssueTrak to provide service for reporting and tracking incidents, problem management, and change control. Each IssueTrak ticket is assigned to a responsible staff member, copied to the submitter and IM Department Director. Likewise, when any action is taken (logged) on an open ticket the requestor and IM Department are copied on the action taken up to and including the close out of the ticket when the incident is resolved.

CSC has a process for incident, problem and change control management. This involves a review of all IssueTrak tickets at weekly scheduled meeting of a “multifunctional group.” This group includes staff members from Information Management, Business Analytics, Evaluation, System Performance, and any impacted department. An IssueTrak spreadsheet that is used to track and report all issues until resolved (closed). The CSC’s SDLC like processes and the incident tracking system (IssueTrak) provide CSC with adequate control over new system development or problem resolution. We reviewed a sample of CSC “Issuetrak tickets” and a copy of the tracking spreadsheet that serves as an “audit trail” of the multifunctional group activities.

Operating System

Control over the operating systems and network are managed by the Network Engineer and the Network Database Administrator (systems team). The system team is responsible for installing operating system patches (bug/security fixes) and service pack releases (software updates/enhancements). Patches to systems are installed 30 days after release by the software vendor. The system team uses a conservative approach to installing service packs 3 to 6 months after release. With the system team managing the updates to operation systems (patches and service pack installs), CSC is able to maintain a current and safe environment for their users, applications, and PHI data.

Audit Observation

While we found that CSC follows a sound process for change control, we observed that the process is not formally documented in the CSC IM policies and procedures. Establishing written policies and procedures to document change control will formalize the process, ensure consistency and maintain continuity.

Recommendation:

2.) CSC Management should formally document the procedures that govern “change control” as currently supported by IssueTrak tickets, management review, system monitoring, and committee approval.

Management Response:

CSC recognizes that it does not have a formal narrative document with outlined procedures in place and has added this to its policy and procedure review in early 2015.

SEGREGATION OF IM DUTIES

LACK OF TRADITIONAL SEGREGATION OF DUTIES IS BEING MITIGATED BY OTHER CONTROLS

Segregation of IM duties is a way to provide technical controls over incompatible/conflicting functions performed by responsible Information Management support staff. Controls can be established with clear job descriptions that aid in identifying personnel who could be performing incompatible duties and functions, elimination of any delegated incompatible duties, and management determination that segregation of duties is functioning properly.

Segregation of duties helps reduce the risk of an unauthorized change which could provide the opportunity for fraud, undetected errors or system failures. Examples of segregation rules include activities such as:

- Programmers and developers not having access to production programs and data,
- Computer operations staff not having access to program source code,
- Change control functions established to exercise control over the movement of programs from the test environment into the production environment, and
- Change control committee confirmation that programming code being moved into production has been certified by affected management as being complete, accurate, and adequately tested.

However, segregation structures vary greatly according to the size of an organization. A small-sized organization may have difficulty in maintaining an ideal segregation of duties. In these cases it may not be economically feasible to hire the additional staff necessary to maintain adequate segregation of duties. Since CSC has a small staff of ten IM professionals to support its systems, traditional segregation of duties would be difficult.

In our review of CSC IM we noted that staff member responsibilities are clearly defined in their job descriptions; each application and database system has a staff member(s) delegated for support; all staff members report to the Director of Information Management; and all changes are reviewed/approved weekly by an interdepartmental committee.

Because of this small staff size, employees in IM have access to both the application development (testing) and the application production environment. With this necessary access to both environments an unauthorized change (outside of the IssueTrak system) could go undetected. However, the CSC IM systems team is now using a new software tool to monitor changes to the system environment. This tool allows for server and applications monitoring, alerts, and reporting.

With the current direct IM management oversight of all IssueTrak tickets, the existing weekly interdepartmental committee review/approvals of IssueTrak activities, and monitoring by the systems team, the opportunity for “unauthorized changes,” which is the primary purpose of segregation of IM duties, is adequately mitigated.

CONTINGENCY/DISASTER PLANNING

A SOUND CONTINGENCY PLAN IS IN PLACE

Contingency planning we reviewed included: back-up/restore of data, applications and system software with off-site storage, and retention; operational contingency planning including disaster recovery, business continuity, and business resumption; and physical site support equipment (including emergency power and fire protection systems).

Backup, Recovery, and Disaster Planning

CSC has a contract with Evault, Inc. for its data and applications backup as well as disaster recovery service. The Evault services provide a unique cloud based backup/restore and disaster recovery process that serves to meet the necessary requirements inherent in the proper management of computer based systems. The Evault contract was included in our sample contract review.

The first step in building both a file recovery and disaster site is to fully backup all the CSC servers that contain applications and data to the Evault “cloud” servers. After the initial upload, any application or data files that change are backed up daily by the Evault service. This process provides routine data recovery and full data/system backup operations following any disaster. In effect, this methodology provides CSC with “Hot Site” disaster recovery. With this now in place, CSC can run on the recovery site for 30 days without any additional charges. The contract provides annual testing of disaster recovery on the Evault “cloud” servers.

Power and Fire Suppression

Building power and fire suppression systems were reviewed. Normal power to the main computer (server) room and the locked network equipment closets (located on each floor) is provided by an uninterruptable power supply system (UPS). The UPS system receives its power from either the public utility (FPL) or the emergency generator. The Head of Facilities advised us that the generator (which also provides emergency lighting to the CSC building) is tested weekly.

The server room was originally protected from fire by a “wet pipe” system. As recommended in the CAI risk review document, the CSC replaced the wet pipe system with a clean and dry fire suppression agent used to protect areas with sensitive electrical equipment and valuable data.

Audit Observation

CSC's “Emergency Management Guidelines (2014-2015)” clearly identify the staff responsibilities and recovery guidelines that are assigned to the IM Director. Also, during our discussions with staff, we were informed that CSC has utilized file restoration and has performed some limited system recovery testing. However, CSC had not yet performed a full disaster recovery test using the Evault system.

Recommendation:

3.) On an annual basis, CSC Management should perform a full IM system disaster recovery test and fully document the test results.

Management Response:

CSC acknowledges that a full IM system disaster recovery test should be performed along with documented test results and has already started testing as of December 5, 2014. CSC is currently working with Evault to finalize the results and will have it documented by December 31, 2014.

BUSINESS PROCESS APPLICATION SUPPORT

THE IM STAFF HAS ADDRESSED ALL BUT ONE OF ITS STRATEGIC TASKS

Effectiveness of Business Process Application Support at CSC included:

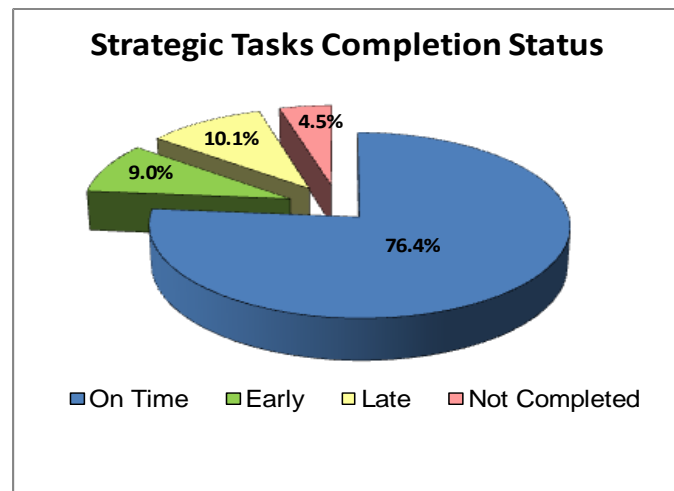
- IM planning that supports the Goals and Objectives of the CSC's Strategic Plan,
- IM control over inventory of current applications in use by the CSC and its customers,
- IM control over inventory of contractors/third parties or other governmental entities that process information, provide data, and/or operate systems for or on behalf of the CSC.

Goals and Objectives Supported by Recent Changes

We found that the CSC requires that Departmental Goals be linked to the Division Goals. Then, the linked Division Goals, the Organizational Strategies and desired Child Outcomes feed the Overall Organizational Goals. (See Attachment 4)

The CSC staff's tasks are detailed as assigned Individual Goals, Department or Division Goals. This structure aligns the individual IM staff tasks with the overall Organizational Strategies and Goals. This alignment helps ensure that IM's strategies and goals support the CSC Strategic Organizational Plan.

In the current CSC Strategic Plan there were 89 IM tasks to be completed by September 2014. Tasks we reviewed were from February 2011 through September 2014. Of the 89 strategic tasks, 68 were on time, 8 completed early, 9 completed late, and 4 not completed. The IM support staff has completed 95.5% of the scheduled tasks. Of the 4 tasks not completed, three were identified as between 75% to 90% complete and one was reported as not completed pending a vendor beta software release.



Application, Vendor and Data Inventories

The CSC IM business applications are assigned IM staff and/or contracted service providers. CSC IM maintains an inventory spreadsheet of all "Data Systems" (applications) which includes the application name, product or hosting vendor name, and the responsible IM staff member(s). Where there is a "Hosting Vendor" there will be a PHI privacy agreement with CSC. Also listed on this spreadsheet are the purpose, key data elements, and the systems reporting capability. A second inventory spreadsheet is maintained for "Data Source" information which includes; the agency providing the data, the responsible IM staff member(s), purpose, key data elements, and reporting method.

CAI INFORMATION SYSTEMS TECHNOLOGY RISK REVIEW STATUS

THE IM STAFF HAS ADDRESSED 96% OF THE 2011 CAI REPORT RECOMMENDATIONS

History

Under a previous IM organizational structure, the CSC contracted with Computer Aid, Inc. (CAI) to assess and report on the Business Information Systems (BIS) Department's risk status in terms of organization, skills, process, compliance, hardware and software.

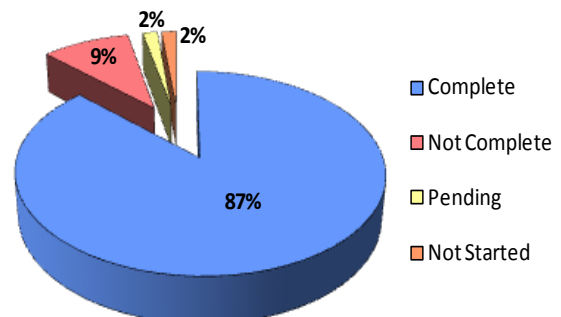
At the time the BIS group was organized into two teams, IS and IT, that reported to a BIS Director who was responsible for interfacing with CSC senior management and for coordinating the overall direction and focus of the BIS organization. The IS team's focus was the business software application portfolio. The IT team's focus was the internal server and networking hardware, the internal and external network connectivity, and the PC hardware and software support

Report Recommendations

The CAI report dated February 25, 2011 reviewed 12 major sections of CSC IT infrastructure: Hardware, Environments, Performance Monitoring, Disaster Recovery / Business Continuity, Process Management, Policy and Procedures, Externally Hosted Software, Service Level Management, Reporting/Metrics, Customer Interviews, Strategic Planning, and Cost of Operations. Within each section several areas were reviewed.

The report outlined 63 recommendations rated High (Significant), Medium, and Low (Minor). The CSC IM staff implemented 55 (87%) of the recommendations.

High, Medium, and Low Risk CAI Recommendations



Of the remaining 8 recommendations 6 are 75% to 90% completed. The two remaining, “documentation of externally hosted application disaster recovery” and “change control” are pending or not started, respectively. Change control is addressed on page 10 of our report.

Audit Observation

Although CSC's contracts for externally hosted applications include a provision for disaster recovery, we could not find a CSC IM disaster recovery policy for externally hosted applications in its disaster recovery plan. Documenting the policy for hosted applications would ensure that such applications are accounted for in testing or carrying out CSC's disaster recovery plan.

Recommendation:

4.) A disaster recovery policy for externally hosted computer applications needs to be developed and included in the CSC disaster recovery plan document.

Management Response:

CSC recognizes that it does not have a formal policy in place for externally hosted computer applications and has added this to its policy and procedure review in early 2015.

ACKNOWLEDGEMENT

The Inspector General's audit staff would like to extend our appreciation to the Children Services Council Information Management staff for their timely assistance and support in the completion of this audit.

This report is available on the OIG website at: <http://www.pbcgov.com/OIG>. Please address inquiries regarding this report to Dennis Schindel, Director of Audit, by email at inspector@pbcgov.org or by telephone at (561) 233-2350.

ATTACHMENT 1 – Management Response



2300 High Ridge Road
Boynton Beach, FL 33426
Tel: 561.740.7000
Fax: 561.835.1956

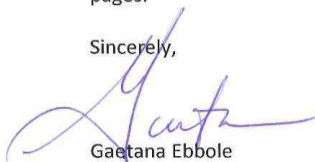
December 16, 2014

Dennis Schindel
Director of Audit
Office of Inspector General
P.O. Box 16568
West Palm Beach, FL 33416

Dear Mr. Schindel:

Please accept our thanks for completing our request for an external review of the Children's Services Council's Information Management Department, which concluded with your draft report issued on December 10, 2014. We are happy to see that your audit did not identify any deficiencies resulting in reportable findings. Your review and recommendations will aid the Children's Services Council in its efforts for continuous improvement within Information Management which directly impacts the entire organization. Our responses to the recommendations noted in your report are set forth in the attached pages.

Sincerely,



Gaetana Ebbola
Chief Executive Officer

www.cscpsc.org

ATTACHMENT 1 – Management Response (continued)**Response to Report on Children’s Services Council Information Systems Management****OIG Recommendation 1**

CSC Management should contract with a third party information technology specialist to perform penetration testing to ensure network and logical access security cannot be compromised.

Response to Recommendation 1

CSC acknowledges that a third party specialist should perform penetration testing to ensure our network security and access points have the proper restrictions in place. As stated in the report, we budgeted for an external penetration test last year and entered into contract with Altius Information Technologies, Inc. on November 17, 2014 to perform this project. Altius began testing on November 22, 2014 and has now completed the initial testing phase. We are scheduled to complete the external penetration test by December 26, 2014 and also plan to fully implement any recommendations that are brought to our attention by that date. Moving forward, CSC plans to perform an external penetration test every 2 years, or sooner if external firewall and security rules are modified that relate to externally facing services.

Summary Response

CSC acknowledges that a third party specialist should perform penetration testing and has entered into an agreement with Altius Information Technologies, Inc. to complete these tests by December 26, 2014.

OIG Recommendation 2

CSC Management should formally document the procedures that govern “change control” as currently supported by IssueTrak tickets, management review, system monitoring, and committee approval.

Response to Recommendation 2

CSC has fully documented the “change control” process in a Visio diagram titled “Application Enhancement Process” that has been used since October 2012. We recognize that we do not have a formal narrative document with outlined procedures in place and have added this to our review list as we implement our new policy and procedure review process in early 2015.

Summary Response

CSC recognizes that we do not have a formal narrative document with outlined procedures in place and have added this to our policy and procedure review in early 2015.

OIG Recommendation 3

On an annual basis, CSC Management should perform a full IM system disaster recovery test and fully document the test results.

Response to Recommendation 3

CSC acknowledges that a full IM system disaster recovery test should be performed along with documented test results and has additionally determined that this testing should be performed annually. As stated in the report, we entered into an agreement with Evault on March 24, 2014 to

ATTACHMENT 1 – Management Response (continued)

provide disaster recovery and remote disaster recovery services. This agreement provides us with an annual test along with documentation of the results and was scheduled to begin on December 5, 2014. Our network engineer is working with Evault to finalize the results and will have it documented by December 31, 2014. Moving forward, CSC will be scheduling annual disaster recovery tests that will occur every December.

Summary Response

CSC acknowledges that a full IM system disaster recovery test should be performed along with documented test results and has already started testing as of December 5, 2014. We are currently working with Evault to finalize the results and will have it documented by December 31, 2014.

OIG Recommendation 4

A disaster recovery policy for externally hosted computer applications needs to be developed and included in the CSC disaster recovery plan document.

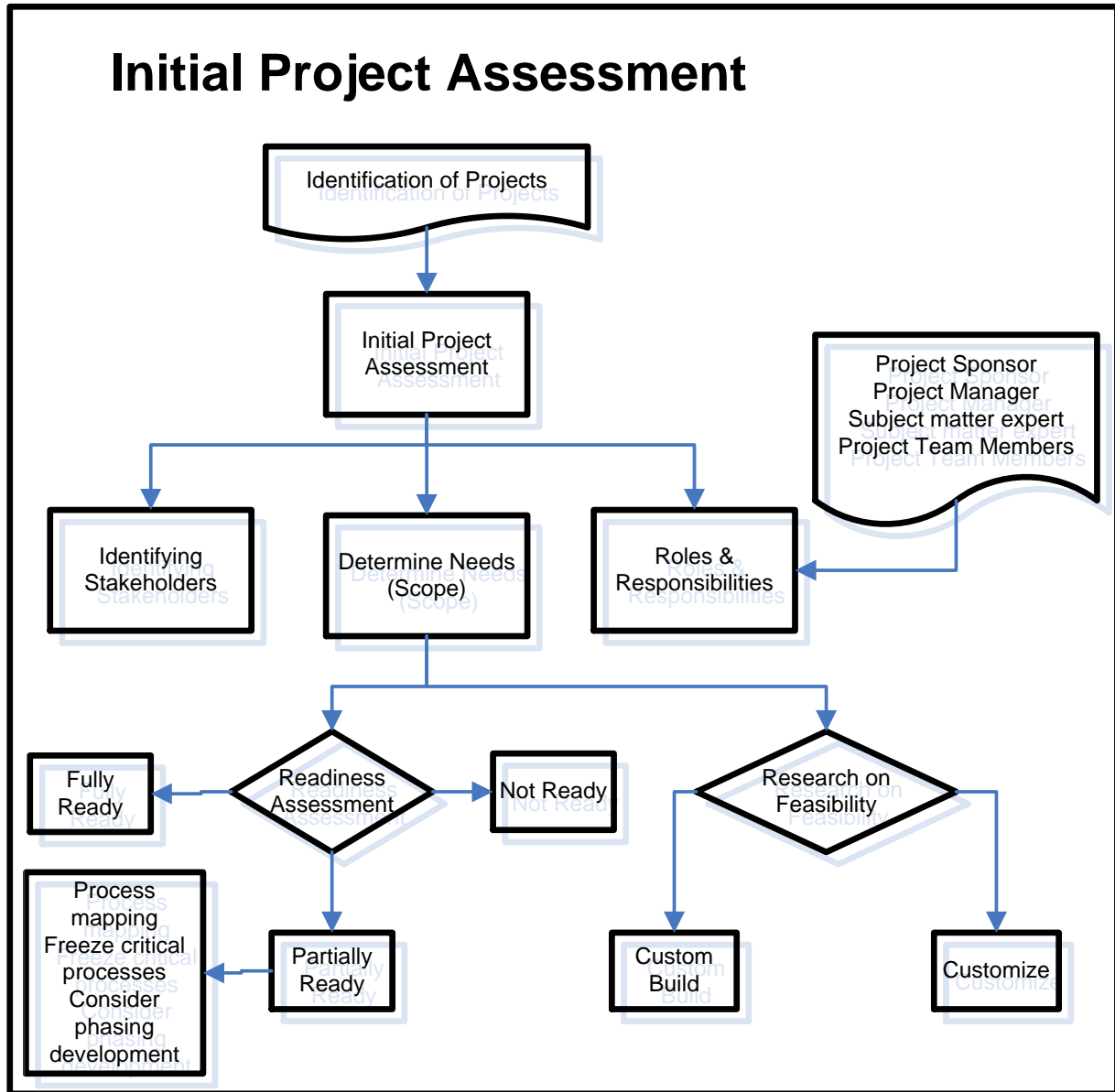
Response to Recommendation 4

Although CSC does not have a formal policy, we require all externally hosted computer applications to include a disaster recovery component in line with our internally hosted applications with Evault. We have added this policy to our review list as we implement our new policy and procedure review process in early 2015.

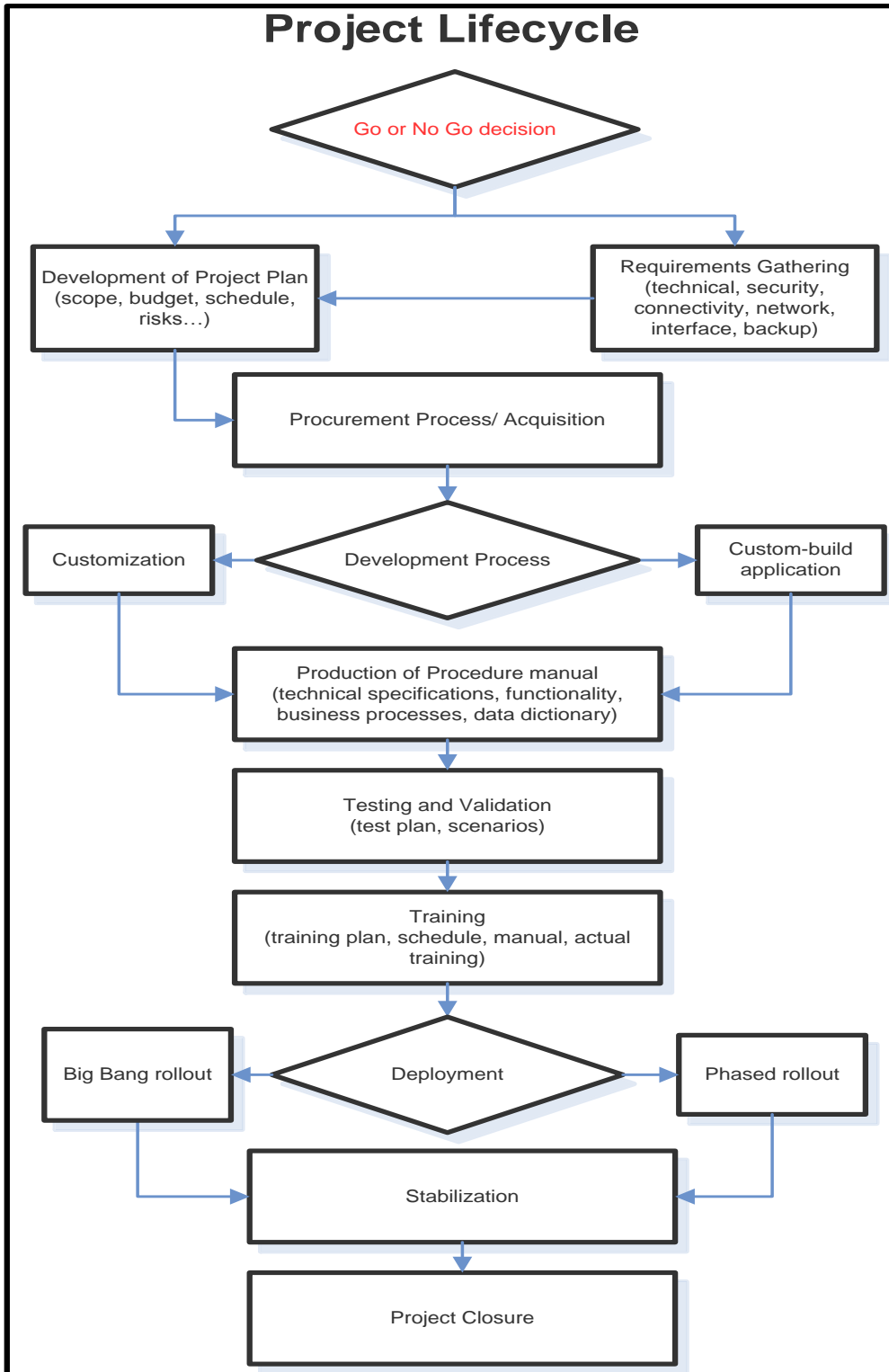
Summary Response

CSC recognizes that we do not have a formal policy in place for externally hosted computer applications and have added this to our policy and procedure review in early 2015.

ATTACHMENT 2-Initial Project Assessment



ATTACHMENT 3– Project Lifecycle



ATTACHMENT 4 – CSC Goals Connection Diagram

