

Other Observations and Recommendations on Internal Control and Financial Operations

	<p>processes and strategies to be supported by IT; perform risk/investment analysis of proposed high dollar/high risk/mission critical IT projects; measure IT value; review IT sourcing, security and architectural policies. The steering committee also monitors and evaluates ongoing projects for risk/value/cost; identifies shared service opportunities across business units and evaluates and approves IT architecture. Such a committee does not exist in the District.</p> <p>b. An IT Architecture Committee, comprised of the Chief Information Officer (CIO) and direct reports. The role of the Architectural Committee is to create and enforce standards for IT across the enterprise and assess exceptions to the rules.</p> <p>c. Business Process Teams, comprised of business and IT personnel these teams oversee IT initiatives dealing with specific business areas. Such teams have been developed for some of the business areas at the District. For instance larger agencies at the District have established program offices, which operate on the behalf of the functional business areas, prioritize IT services, and interface with OCTO and central business functions. Examples include OTR's Information Systems Administration, Department of Human Services' Income Maintenance Administration, and Office of Pay and Retirement Services' Enterprise Office.</p>
<p><b>Management's Response</b></p>	<p>Management does not concur.</p> <p>For four and half years, OCTO has maintained a single Project Management Office who responsibility is to provide review, approval, tracking and monitoring all major District of Columbia government IT capital projects.</p> <p>IT Steering Committee – OCTO has such a function established. OCTO's certified agency CIO program is in place to provide this function. OCTO is in the process of certifying a CIO for each major city agency. One of the purposes of this program is to have the agency CIOs serve in the capacity of an IT Steering Committee. The effort to fully staff the agency CIOs is well underway and should be completed by the end of the calendar year.</p> <p>Architecture Committee – OCTO has established an in-house Architecture group, staffed by experienced IT architects. The OCTO Architecture group serves as the citywide Architectural Committee. Currently the group is being expanded.</p> <p>Business Process Teams – For five years, OCTO has maintained an in-house Business Process group, staffed by experienced business process experts. The OCTO business process group provides their services to the District agencies on a priority basis.</p>

## Other Observations and Recommendations on Internal Control and Financial Operations

<b>Process</b>	Information Technology General Controls
<b>Title</b>	Office of Chief Technology security policies
<b>Observation</b>	Critical OCTO security policies and procedures have not been approved for formal implementation and enforcement. A formal proactive system of IT Security governance for administering policies and procedures has not been established. As a result, drafted policies and procedures are stagnant in the approval cycle.
<b>Recommendation</b>	OCTO should create a proactive mechanism involving all security stakeholders to promptly review, provide comments and approve policies. This could be in a form of a security committee to ensure effective and efficient approval and implementation of policies and procedures.
<b>Management's Response</b>	Management concurs with the findings.  OCTO is developing a policy for development, approval, and distribution process in FY 2005.

<b>Process</b>	Information Technology Controls around the Local Area Network (LAN) and Wide Area Network (WAN)
<b>Title</b>	Anti-virus protection
<b>Observation</b>	No anti-virus screening is in place for inbound network traffic. Anti-virus programs deployed by OCTO are host- and workstation- based; there is no anti-virus protection or filtering done at the gateway to the DC LAN/WAN.
<b>Recommendation</b>	OCTO should deploy an anti-virus application at the gateway (firewall) level to prevent inbound traffic carrying viruses, malicious code or Trojans from entering the DC LAN/WAN.
<b>Management's Response</b>	Management concurs with the findings.

<b>Process</b>	Debt Management Process
<b>Title</b>	Deboise, Brown & Company (DBC) Application Controls

Other Observations and Recommendations on Internal Control and Financial Operations

<b>Observation</b>	<p>DBC application controls need improvement. Specifically:</p> <ul style="list-style-type: none"> <li>a) Users with access to the DBC Application have read/write permissions in excess of their job requirements. Management has not implemented a Security policy that ensures access privileges granted to system users are based on the principal of least privilege or need-to-know.</li> <li>b) There are no documented policies and procedures around system security and processing of user Access Requests (informal system access request policies are currently in place).</li> </ul>
<b>Recommendation</b>	<p>We recommend that:</p> <ul style="list-style-type: none"> <li>a) Management should ensure permissions granted to users in the DBC application reflect those needed to perform their job.</li> <li>b) Management should adopt formal written policies and procedures around system security and processing of user access requests. The user access request procedures should ensure evidence of documented approval of access request by the system owner.</li> </ul>
<b>Management's Response</b>	<p>Following are management responses to each of the above observations:</p> <ul style="list-style-type: none"> <li>a) Management concurs with the findings. They will reduce the number of people with access from 4 to 3.</li> <li>b) Management concurs with the findings.</li> </ul>

<b>Process</b>	Fixed Assets
<b>Title</b>	Periodic Physical Inventory
<b>Observation</b>	<p>The District has policies in place that require a physical inventory of fixed assets to be performed on an annual basis. However, it was noted during the audit that the District has not performed a physical inventory since 2002.</p>
<b>Recommendation</b>	<p>We recommend that the District perform a physical inventory of its fixed assets in accordance with its stipulated policy, but in no case no less often that every two years.</p>
<b>Management's Response</b>	<p>The District's Fixed Assets Policy and Procedure Manual will be updated to reflect the true frequency of physical inventory, which is every two years. Management asserts that the most recent physical inventory occurred in FY 2002. While budget constraints prevented the District from performing a</p>

Other Observations and Recommendations on Internal Control and Financial Operations

	physical inventory during FY 2004, it has been scheduled to take place in FY 2005 and every other year thereafter.
--	--

<b>Process</b>	Information Technology controls
<b>Title</b>	Student Information System (SIS +) general and application controls
<b>Observation</b>	<p>We noted the following observations:</p> <ol style="list-style-type: none"> <li>1. University of the District of Columbia's (UDC) SIS+ programmers perform the functions of data security administrator and have full responsibility for programming application changes, testing changes, and implementing changes. [Note that financial data is not interfaced automatically to R*STARS. Financial data is manually re-entered into R*STARS.]</li> <li>2. Lack of information systems plans, lack of documented systems related policies and procedures, and lack of agency level information technology steering committees.</li> </ol>
<b>Recommendation</b>	UDC management should consider the risks arising from these observations and develop an action plan for responding/mitigating these risks. The UDC CIO should ensure timely implementation of the corrective measures documented in the action plan.
<b>Management's Response</b>	<p>Management concurs with the findings.</p> <p>Regarding separation of duties - the Office of Information Technology has already implemented procedures which provide separation of duties. We need to better document the procedures. A proposed UDC information technology governance committee has been developed, with university representatives and committee mission. The proposal has been reviewed with the University Executive V.P. of Operations, and the University Provost. They are in support of the proposal. This committee will be convened by February 1, 2005, and led by the University CIO. From this committee, a plan for development of needed plans, policies and procedures will be developed and approved.</p>

Other Observations and Recommendations on Internal Control and Financial Operations

<b>Process</b>	Washington Convention Center Authority (WCCA) General information technology controls
<b>Title</b>	Service Continuity
<b>Observation</b>	<p>WCCA management has not developed or implemented the following:</p> <ul style="list-style-type: none"> <li>• Offsite backup storage facility for backup tapes</li> <li>• A comprehensive Disaster Recovery Plan (DRP) to include new servers such as the FMS II.</li> <li>• Appropriate environmental controls in the server room.</li> </ul>
<b>Recommendation</b>	<p>We recommend that WCCA management formalize the Business continuity process for critical financial resources, as well as develop a comprehensive Disaster Recovery Plan (DRP) including the FMS II. In addition, an offsite backup storage facility should be established for recovery of operations in the event of disaster or loss of data. Appropriate environmental controls including: fire extinguishers, redundant air coolers to provide a dedicated second source of cooling, and signs prohibiting drinking or eating in the server room should be implemented.</p>
<b>Management's Response</b>	<p>Management concurs.</p> <p>The recommendations above have been reviewed and addressed within the Technology Management Division (TMD) of WCCA. The process to contract with an offsite storage facility has begun. The Disaster Recovery Plan has been updated and the appropriate environmental controls to the server room have been implemented.</p>