

SECOND FOLLOW-UP REPORT:
A RECORD OF PRESIDENTIAL APPROVAL
TO TASK FORCE RECOMMENDATIONS FOR
Networking and Telecommunications, Fall 2008

Recommendations

- 1) Develop and publish an HCC approved IT hardware and software list in order to improve delivery of service and reduce support costs. Investigate the feasibility of including an OIT review for all procured hardware/software not included in applicable hardware/software standards college wide.

No progress-deferred to the 2009-2011 planning cycle.

- 2) In partnership with Academic Technology analyze OIT and College technical support resources to recommend a plan for more efficient and appropriate allocation of human, fiscal, and technological resources to academic and administrative technology support needs.

No progress-deferred to the 2009-2011 planning cycle.

- 3) In conjunction with Administrative Systems and ~~Institutional Research~~ the Department of Management Information Systems develop and recommend for adoption a formal Program Delivery Process. The process should ensure the following areas, at a minimum, are addressed as part of all information systems or network affecting projects or academic programs:

- i. Program definitions and objectives.
- ii. Document all areas impacted by the project.
- iii. OIT notification of all new hardware and software. This would not stop employees and staff from using new hardware and software but would ensure OIT awareness and support system and network integrity.
- iv. Document monitoring and control procedures for the new project.
- v. Document ownership, access, back up and retention requirements for data.
- vi. Document Disaster Recovery/Business Continuity requirements.
- vii. Establish metrics to evaluate system/network performance.
- viii. Data security.
- ix. Support roles, i.e. service level requirements, daily operation, access permission and ID's, procedure definition, etc.

A process has been developed and implemented in conjunction with ASAC.

- 4) Partner with Professional Development Services to develop and implement strategies to increase the level of communication between unit and college users.

No progress-deferred to the 2009-2011 planning cycle.

- 5) Create an IT policies/procedures committee to:
- i. Create, modify, recommend, and implement IT related polices/procedures
 - ii. Educate the HCC community of current IT policies/procedures.
 - iii. Conduct an annual review of all IT policies/procedures.
 - iv. Develop policies/procedure for new systems.

Committee has been established and policies are currently being reviewed.

- 6) Partner with Web Services to expand the OIT web site to assist customers in understanding the responsibilities of OIT and include a FAQ page(s) to assist the user community in obtaining information technology services.

The OIT website has been expanded and will continually be improved to include a comprehensive FAQ page.

- 7) Immediately address findings of the 2007 Operational Audit that have no budget impact and provide cost estimates for findings that do have budget impact to be considered for funding:

- i. Policies and procedures.** (Complete development, approval, and implementation of applicable IT polices/procedures.)
- ii. Security awareness and training.** (Approve and implement a security awareness and training program for all users of IT resources.)
- iii. Physical access controls.** (Transfer access control authority for the datacenter and communication closets to OIT management, restrict access to only those persons who have legitimate need, continue with plans to implement an electronic access system.)
- iv. Logical access controls** (Implement a biannual audit of all user account databases, strong passwords and industry password change frequency will be required for all capable systems, implement this security warning banner for all potential users for all systems that are capable.)
- v. Change management controls.** (Implement change management controls, automate if possible)
- vi. Service continuity controls** (Complete a comprehensive service continuity plan driven by a formal risk assessment and business impact analysis.)
- vii. Environmental controls** (Address environmental risk to data center and associated computing facilities.)
- viii. Risk analysis and security plan** (Conduct a formal risk analysis and business impact analysis to highlight actual exposure and drive the security/DR plan).
- ix. Incident response and monitoring controls** (Ensure appropriate security incident response and performance monitoring procedure are developed and implemented.)

See attached IT audit update.

- 8) Seek cabinet approval of the request in the 2007-2009 unit plans to add funding of helpdesk operations into departmental budget. Investigate costs for a hybrid model where the community could receive technology assistance after core hours from a 3rd party and add this initiative to the strategic planning cycle for 2007-2009 planning cycle.

No progress-deferred to the 2009-2011 planning cycle.

- 9) Through the IT policies/procedures committee develop and implement a College wide Service Level Agreement to be recommended to cabinet for enterprise approval.

No progress-deferred to the 2009-2011 planning cycle.

- 10) In partnership with Institutional Research seek modifications to the Faculty/Staff survey instrument that will allow a more direct evaluation of select networking operations (e.g. networking, server, desktop, help desk, telephone).

Paul Nagy sat on the unit review committees and is aware if the needed changes in the survey.

- 11) Develop a recommendation outlining organizational and fiscal impact for the establishment of a dedicated information security and audit arm for the College that would be dedicated to ensuring the availability, confidentiality, and integrity of electronic data and applicable regulatory and institutional policy compliance.

A Security and Integration Engineer position has been created. Further progress has been deferred to the 2009-2011 planning cycle.

- 12) Partner with Institutional Research, Management Information Systems, Student Services, Finance, Purchasing, Public Safety, Human Resources, and Legal to develop a data classification scheme/data ownership and implement a backup policy relevant to the scheme. The Network and Telecommunications unit is ultimately responsible for the protection of all electronic data at HCC. To provide this protection the unit needs direction regarding business operation, regulatory requirements and legal considerations from the data owners.

A contract has been signed with IBM to conduct a risk/data ownership assessment in Spring 2009.

- 13) Conduct a formal risk and business impact analysis to highlight actual exposure and drive the security/DR plan.

A contract has been signed with IBM to conduct a risk/data ownership assessment in Spring 2009.

14) Partner with the Office of Strategic Planning and Analysis to evaluate current enterprise technology initiative prioritization in order to develop and recommend a process that will lend itself to prioritization of technology initiatives as they relate to overall College objectives and strategic initiatives.

A contract has been signed with IBM to conduct a risk/data ownership assessment in Spring 2009.

HCC IT Audit Findings for 7/1/2006 – 6/30/2007

Finding No. 7: Policies and Procedures

Recommendation: The College should complete the development, approval, and implementation of the IT policies and procedures, including the aforementioned issues. In addition, the College should establish a process for developing new policies and procedures as the College implements new and progressive technologies.

20NOV2008 – The Acceptable Use Policy has completed the approval process and was approved. In addition nine other policies are currently going through the process and should be approved early in the 1st quarter 2009. The process for developing new policies and procedures has now been clarified. OIT policies are considered to be “Operational Procedures” that require the following approval process:

1. preliminary review by the President’s Cabinet
2. distribution to the HCC Community for review and comments
3. review and comments by the Technology Steering Committee
4. final review and recommendation for approval by the President’s Cabinet

Clarification of the status of OIT policies as Operational Procedures has facilitated the approval process and all planned policies will have completed the review process by the end of the 1st Quarter of 2009..

Finding No. 8: Security Awareness and Training

Recommendation: The College should approve and implement a security awareness and training program for all users of IT resources. The College should also determine an implementation schedule for the training program, particularly for individuals who occupy positions of special responsibility; require employees to provide written acknowledgement of security responsibilities beyond FERPA; and provide for monitoring and reviewing activities of individuals in positions of special responsibility.

20NOV2008 – The security awareness program is being implemented in two phases. Phase I includes a logon notification highlighting specific aspects of the Acceptable Use Policy (AUP) with an agreement to abide by the AUP being required prior to accessing the College network. This phase also includes the development of an on-line system for tracking acceptance of the security responsibilities for all Datatel Users. This same system will also be the basis for security awareness training beyond the first Phase of the project. By July 2009 the security awareness system have been developed with at minimum of two modules. This system will track users participation as well as tracking mini-test scores at the end of each module. Dates will be established for completion of a specific module and anyone who doesn’t complete the module successfully will have their network access temporarily deactivated. It will be reactivated on request with a caveat that the module must be completed within 48 hours or access to the network will be deactivated and their

supervisor notified. Two modules will be developed annually until a complete program is in place.

Finding No. 9: Physical Access Controls

Recommendation: The College should re-evaluate the policies and procedures for authorizing physical access to the Data Center and communication closets and should consider transferring the authority and responsibility for authorizing physical access to the Data Center and communication closets to OIT management. Additionally, OIT should review who has access to the Data Center and communication closets and appropriately restrict it to only those individuals who require access for the performance of their job duties. Further, as a part of its design of a comprehensive campus security system, the College should continue with its plans to implement an electronic access system that has the capability of assigning individual access codes and of logging each individual that enters the Data Center. Also, OIT should implement the use of a visitor's log for the Data Center.

20NOV2008 – Authorizing access to the datacenter by OIT – completed
Access control list review – completed
Datacenter access control system has been upgraded and now has no shared access ids - completed
A visitor's log is now in use in the Datacenter - completed

Finding No. 10: Logical Access Controls

Recommendation: The College should address the aforementioned issues by ensuring that proper access controls are in place to adequately protect all IT resources. The College should also enhance its procedures to ensure that user access privileges for terminated employees are removed in a timely manner; access privileges to data and programs are restricted to only those individuals who clearly need it in the performance of their job duties; password controls are strengthened; and approval for the implementation of security warning banner screens is obtained for all potential users.

11NOV2008 – Policy has been developed and is currently in the review process. Final approval of the policy should occur early in the 1st quarter of 2009. It covers:

- **initiation and termination of account procedures'**
- **guidelines for access associated with each category of employee**
- **password renewal required every 90 days**

The security warning banner is now in place and it currently highlights the AUP

Review of all security classes for Datatel Access is included in Phase II planning for R18. Security Class review should begin after the first of the year. The initial review of security classes will be completed by a Datatel consultant. The security class review with recommendations will be completed by December, 2009. This timeline may be too aggressive and the process may extend beyond the projected completion date.

Finding No. 11: Change Management Controls

Recommendation: The College should complete its implementation of an automated software product to control the change management process. Additionally, the College should ensure that user acceptance testing of program changes prior to the movement of programs into the production environment is incorporated into the change management process.

20NOV2008 – Completed – The Change Management process is now in place and working. Because of software development issues with the commercial change management software, a manual change control process is in now place.

Finding No. 12: Service Continuity Controls

Recommendation: The College should complete its efforts in developing, approving, testing, and implementing comprehensive service continuity controls, including, at a minimum, the IT disaster recovery plan and the continuity of operations plan.

20NOV2008 – Annual testing is in place for Payroll with additional modules to be included for the Spring 2009 testing based on the Risk Assessment information. Funding has been secured for Phase II of the Disaster Recovery project. The Risk Assessment project is expected to be completed by the end of the 1st Quarter of 2009.

Finding No. 13: Environmental Controls

Recommendation: Considering the aforementioned factors, along with the flooding risk from a hurricane, the College should address the risks to the computer facilities related to environmental controls, specifically water damage, and should consider adding water detection equipment to the Data Center.

Environmental monitoring is in place in the data center and it has been expanded to include water detection probes. The communications closet environmental monitoring and controls project will be requested for funding in FY 09-10.

Finding No. 14: Risk Analysis and Security Program Plan

Recommendation: The College should complete all of the key activities necessary, including performing adequate risk assessments and creating a comprehensive security program plan, to facilitate the development, approval, and implementation of an effective information security program.

11NOV2008 – Funding has been secured and we are currently in negotiations with IBM to perform the work. The risk assessment and data classification review and evaluation will be complete by the end of the 1st Quarter 2009. This assessment and classification process will guide the development and implementation of both the next phases of the Disaster Recovery/Business Continuity plan and the information security program. Phase II of the DR development program is currently in process

with expanded resources being included, based on the Risk Assessment results, by the end of the 2nd Quarter 2009.

Finding No. 15: Incident Response and Monitoring Controls

Recommendation: The College should ensure that appropriate security incident response and performance monitoring procedures have been properly developed and implemented.

20NOV2008 – The Incident Response Policy has been created and is moving through the approval process. It should be approved by the end of the 1st Quarter 2009.

Formal performance monitoring procedures have been implemented. Network bandwidth utilization and virus/spam statistics are reported in weekly and monthly increments. Additional monitoring components will be added based on prioritization results from the Risk Assessment Report. The final performance monitoring procedure document will be completed by the end the 1st Quarter 2009.