Chabot-Las Positas Community College District
Information System Memo

June 30, 2007

Reference:	**T500**
Prepared by:	Jeannine Methe
Date:	6/28/07
Reviewed by:	

Instructions: This memo is designed to assist in obtaining an understanding of the general computer and computer application controls for an in-house system or computer service organization. To assist the auditor in answering the questions below, the auditor may have the Agency complete the questionnaires at GCX-9o and GCX 9p included in the GCX-9 Governmental Control Procedures Form – Financial Statements section from PPC. At the end of this memo is a list of documents the auditor should request from the Agency.

1. Describe the staffing levels maintained in the IT department (change titles as needed):

Title	Names/Number of Staff
Director – Chief Technology Officer	J. Methe/1
Systems Analysts – Programmer/Analysts (4 job levels)	E. Stricklen, D. Suhr, D. Troche, S. Followill, K. Judson, C. Gould/6
Operators – 1 Supervisor + 2 Operators	T. Hirstein, K. Barto, I. Polvorsa/3
Network Administrators – Help Desk Admin + includes Network Technicians noted below	K. Tollefsen/1
Program Analysts – Admin Analysts (2 job levels)	P. Brown/1
Network Technicians – NW Specialists (Level 2) Includes Network Administrator duties based on specific network/server responsibilities	M. Smythe, J. McHugh/2
Desktop Technicians – NW Specialist (Level 1)	R. Starling/1
Network Manager/Systems and Services	Ken Agustin/1
Programmer/Analysts II	To be hired in July & August 2007/2
Administrative Analyst II	To be hired in August 2007/1

2. Describe the extent to which the computer is used in significant audit areas by completing the following:

a. List the significant computer applications run on the system, identify the source of the software used, and indicate whether the institution has access to the source code.

Application	Source of Software Used (Check One)				Does Agency have access to source code? (Yes/No)
	Service Provider	Internally Developed	Vendor (Unmodified)	Vendor (Customized Or Modified)	
Food Service	NONE				
Warrants			SCT Banner	SCT Banner	Yes
Fixed Assets			SCT Banner	SCT Banner	Yes
General Ledger			SCT Banner	SCT Banner	Yes
Attendance			SARS & STARS at College for Student	No	Yes

			Attendance		
Programs/Grants			SCT Banner	SCT Banner	Yes
Student Body			SCT Banner	SCT Banner	Yes
Payroll			SCT Banner	SCT Banner	Yes
Component Units	DOES NOT APPLY				
Budgeting			SCT Banner	SCT Banner	Yes
Building Projects			SCT Banner	SCT Banner	Yes
NOTE: CLPCCD uses SCT Banner baseline as well as customizations that are mainly reports or special processes created as a supplement to the original Banner System.					
Room Scheduling			CollegeNet	No	No
Luminus (Portal)			SCT Banner (now Sungard)	SCT Banner (now Sungard)	No
Web Intelligence & Crystal Ad-hoc Query/Reporting			Business Objects	No	No

b. If a service center is used for computer processing in significant audit areas, give the name of that service center.

Not Applicable – District Data Center is housed at the Chabot campus in Building #300.

c. If an in-house computer system is used for significant audit areas, briefly describe the computer hardware and any vendor software packages used.

- **Hardware (brand name and model of main processor, number and type of terminals, etc.):**

  Hardware is IBM p671A – estimated 400 administrative users access the Banner System via Banner forms, ODBC, & SQL*Net connections.

- **Vendor software packages (indicate the vendor, brand name, and any significant customized features or modifications made):**

  Software is Sungard SCT Banner version 7.3. Core product is 95% unchanged. Customizations to the baseline product are made in separate files (not the originals). Separate bolt-ons are used for third party products or in-house developed sub-systems that interface with Banner. Other primary vendors for common District software include GroupWise for email, Novell, Microsoft for desktops.

d. Who maintains software inventory and licensing?

District Information Technology (ITS) staff under the management of the District CTO.

e. **Are vendor maintenance contracts in place? What level? If not, is maintenance and support provided by another organization?**

Yes, vendor maintenance contracts are purchased annually for all production hardware and software. All production hardware and software for mission critical systems is covered 24 x 7. All non-critical hardware and software is covered on an 8 to 5 next day service.

f. Describe extent of use of online terminals and computer networks.

There is only 1 directly connected terminal for the IBM. All other access is done via TCP/IP connections, ODBC, or encrypted SQL*Net connections. On-line computer access is used for administrative applications, e-collaboration, internet services, and email in addition to the Banner System on the IBM.

3. Obtain third-party reviews (SAS #70 letter) for the applicable service organization and describe scope of results. Review SAS 88 for applicable procedures to perform.

Not applicable.

4. Inquire as to whether a third party administrator is used for health or workers' compensation, self-insurance funds. Document your findings. Obtain a copy of the third party administrators' SAS #70 report and review for exceptions, etc. Document your findings below.

Not applicable.

If the Agency is using a central processing facility, the remaining questions should be completed by speaking with personnel from that facility. If a separate review of the processing facility has already been completed, reference that document where applicable. For Agencies that do use a central processing facility, all questions should be completed by speaking with the appropriate Agency personnel.

5. Tour IT data center of computing facility and note the following:

a. Environmental controls

	Yes	No	Comments
Sprinklers (wet or dry?)		No	Use Inergen Gas (Halon Gas) Fire Suppression System
Fire Extinguisher (check tag to ensure it has been recently inspected)	Yes		Fire extinguisher last inspected March 2007. System provides complete zonal protection for all areas of data center.
Raised floor	Yes		Is sunken floor with raised tile.
Temperature controls (air conditioner, etc)	Yes		Air conditioner

b. Security

	Yes	No	Comments
Keylock door (What type of lock is used?)	Yes		Keylock is standard Schlage System.
Alarm	Yes		Sonitrol alarm system and fire alarm system in place. Have building access alarm, building fire alarm, computer area alarm & computer area fire alarm.
Facilities access	Yes		Restricted access to District ITS and Security personnel only who possess a key.
Library controls	Yes		Data and library access is restricted to the District ITS personnel based on job function and duties.
Terminal access controls	Yes		Only 1 console access is allowed to the IBM in the computer room. For other applications, authentication to the servers is performed.
Authorization controls	Yes		The root user is only able to login at the main console for the IBM in the computer room. Restricted access to District ITS responsible staff. For other applications, user/directory policies are provided via authentication to the servers.

c. Is data center properly protected from outside intrusion? (Yes/No – Explain)

Yes, the data center is protected by locked doors and Sonitrol alarm and restricted to District ITS personnel.

6. Describe other areas of security:

	Yes	No	Comments
How does user request access? What procedure should be followed?	Yes		Users must submit to ITS a Computer Access Request form signed by the responsible manager. If the request crosses functions like access to Finance data, then that Finance manager must also sign the request. ITS then creates the appropriate accounts and the user is assigned to the proper groups/roles. Users must set up passwords for each of the systems for which access is granted. District ITS provides Password Guidelines to users for periodic changing of their passwords and suggestions for types of

			secure passwords.
Passwords – Minimum number of characters? Special characters? Expiration interval?	Yes		Passwords vary in length and special characters based on the system you are accessing. Network passwords are 5 character minimum with no special characters; no minimum size for email passwords with no special characters; IBM passwords are 6-8 characters and must include some special character; Banner passwords can be any length and not case sensitive. No expiration interval is automatically controlled, but change of passwords on a regular basis is procedurally done by users as needed and encouraged to be done on a routine basis. Users can change their passwords directly for all systems they access.
Workstation – Hours of access, time-out interval?		No	
Describe procedure for deleting terminated employees.	Yes		Computer Revoke Request form is submitted to ITS by responsible manager. Emergency requests can be processed through phone request by employee's direct manager or management above with follow up of Revoke Request form.
What is the process of reviewing access profiles? Are authorization requests documented and kept on file?	Yes		Computer Access & Revoke Request forms are filed for documentation. Managers are responsible to review access profiles for employees as job duties change and then notify ITS of any required changes. Reports for Banner user accounts are run periodically for management review.
Who has the ability to add users to the system?	Yes		Network and email users are added by the ITS Network/Help Desk staff; Banner users are added by

			the ITS Application staff using the Banner security features by user module.

7. Network and System Security

	Yes	No	Comments
Do you use a firewall? (If so, document vendor and version)	Yes		PIX 515 E at each location
If using a firewall, has the configuration been reviewed? What is the process to change the configuration if necessary?	Yes		Network administrator is contacted by authorized technicians to request necessary changes. Recent purchase of redundant firewalls under Bond Measure B enables a fail over configuration.
Is the network monitored for intrusion attempts (intrusion detection?)? (If so, document vendor and version)	Yes		Network Intelligence Envision product. Logs of all connections and activity are stored on special logging servers and all server usage is monitored and logged on a daily basis. Outside Internet access to internal servers is controlled, monitored, and logged using firewalls.
Who receives intrusion alerts? Are IDS logs reviewed periodically?	Yes		Network administrator reviews logs daily and notifies appropriate management and takes correction action as needed.
Are system configurations reviewed on a regular basis?	Yes		New equipment purchased under Bond provided opportunity to review the full configuration and make modifications as required. This equipment facilitates the review of configurations on a regular basis. New Cisco switches and routers have been installed at all locations to provide improved performance, stability, advanced software capabilities, and new security features.

8. Describe backup functions:

a. Location of onsite backup –

District System Backup tapes are stored on site at Chabot in Building #200 in a fireproof safe which is separate from the building that houses the servers.

b. How are requests prioritized?

District System Backups are performed on an automatic nightly and weekly schedule. Special backups are scheduled if required for major project implementations.

c. What is the offsite rotation schedule?

Full weekly backup tapes done on Friday are stored offsite at the alternate Computer Room locations – District Data Center housed at Chabot uses the District server room at the District building as its offsite location. Offsite tapes are rotated back to the central Data Center once new weekly tapes are generated.

d. Describe backup procedures.

All data on District servers are backed up to tapes using industry best practice procedures. Backup procedures are run on a daily basis Monday through Thursday and then a full weekly backup is created on Friday or Saturday dependent on the server. The tapes are rotated in a daily/weekly/monthly/yearly algorithm with a selection of tapes stored in a fireproof vault in a separate location from the servers.

e. Has the backup been tested?

Yes, backups for all systems are tested.

f. Data recovery

Yes, data recovery provisions are available for all backups.

g. Personnel backup

Backups are performed by the District Operations staff for the Banner System. Backups are performed by the Network Specialists for the other District systems such as GroupWise email, Web, etc. There are backup personnel designated to replace the primary staff if they are not available.

h. Supplies backup

Supplies for backup tapes are provided by the District ITS department. As part of Bond Measure B, hardware redundancy is being installed for all common District services and a new tape backup equipment has been purchased to consolidate server backups where appropriate. The new hardware and software tape backup solution is scheduled for operation in October 2007.

9. Describe programming controls:

a. How are program modification requests initiated?

Program modification or enhancement requests that affect the Banner System are submitted and approved through the Banner User Groups (one committee for each Banner module) and the Banner Chairs (committee of all committee chairs for the individual Banner user groups). These program requests are tracked through the automatic Banner User Task List System for status and priorities. Banner major projects that are over 2 months

effort go through an additional review process through the Chancellor's Cabinet for approval and priorities. These major projects are reviewed and planned for a 3-year period with adjustments made as necessary.

b. How are requests prioritized?

Requests are prioritized through the Banner User Groups, Banner User Chairs Committee, and for the major projects additionally through the Chancellor's Cabinet.

c. Who approves the request?

Requests are approved through the appropriate groups depending on the magnitude and impact across groups of the change – Banner User Groups (group impact only), Banner User Chairs (cross groups impact), Chancellor's Cabinet (major projects that are in line with the District's goals).

d. What are the program documentation standards?

Program documentation is performed within the programs or specific scripts that are written by the analysts. A composite list of program modifications to baseline is maintained to be used for review during Banner upgrades. Documentation is also created for Operations to run the process. For new sub-systems created to supplement Banner, user documentation of functionality is also created for distribution.

e. Do the programmers work in test libraries? – Yes. Programmers work in a test environment that is identical to the production environment.

District ITS has several test environments for programmers to test in for new modifications, user testing and training, and upgrade of Banner releases or patches. These test environments are refreshed as needed (minimum weekly unless frozen in time for iterative testing) to synchronize with the production environment for complete system testing before modifications are released to production.

f. How are programs tested?

Programs and when needed the entire processes are run by the programmers within one of the test environments to check the accuracy of the change and validate the affect the program modification or addition has on the Banner System. Also, users are brought in to re-test the modification and validate the accuracy from their group and the impact on other groups. Approval is received from user groups on results of change before released to production.

g. Who moves the program from the test library to the production library?

For Banner release upgrades, the Database Administrator controls all movement of programs from the test to production libraries through an automated process that is completed after full testing and approval has been completed. For routine Banner corrections, the programmers work with the DBA to set up test environments and migrate the changes to production once testing is completed.

10. Describe End User Computing controls:

	Yes	No	Comments

Has a software standard been adopted?	Yes		Windows is standard operating system for desktops and MS Office suite is standard for word processor and spreadsheet and Norton Anti-virus is standard.
Is the standard acquired through a site license?	Yes		Microsoft Campus Agreement through the State Chancellor's Office; Norton is site license.
Is a software license inventory maintained?	Yes		Maintained by District ITS and College Computer Support staffs.
Are machines virus checked?	Yes		Standard is Norton Anti-Virus controlled through the servers
Are users given software manuals?	Yes		Software manuals are made available on-line
Are users provided training?	Yes		On-going training is provided to users by District ITS and College Computer Support staffs. Vendor training may be provided for specific products.
What permissions do users have on their system? Can the install/uninstall software? Disable services?	Yes		In general, Administrative users have no permission rights so the software installs are totally controlled by the IT staffs, with a few exceptions where approval has been granted by management. For faculty, permission rights are granted on an as needed basis.

11. Describe the agency's Strategic Plan

a. Has a strategic plan been prepared and implemented?

Yes, District ITS activities are already in process as part of Bond Measure B using our Information Technology Master Plan (ITMP) and updates are made when appropriate based on technology advances. The District has already established new District standards for Cabling, Network Infrastructure, Desktops, Servers, and Printers. Banner Project Priorities are established for a 3-year period for major implementations with approval at the Banner Chairs Committee and Chancellor's Cabinet. The Banner Project Priorities for 2005-2008 have been approved by the Cabinet and additions are made for new critical tasks as appropriate. The District Strategic Plan Draft was completed in May 2007 to identify new automation projects and process improvements for all the District Services to the Colleges. A list of the projects in the District Strategic Plan that require ITS support was compiled to compare the requirements to the Banner Project Priority List and highlight new automation initiatives.

b. When was it adopted?

The Banner Project Priorities for 2005-2008 have been approved and was adopted April 2005. The IT Master Plan has been adopted in conjunction with the College Facilities Master Plan, which was approved in June 2005. Additional sections are being added as new technology initiatives are reviewed at a more detail level. The Draft District Strategic Plan was distributed in May 2007 to the District and Colleges to review and provide any additional feedback with the Final plan adoption targeted for Fall 2007.

c. What period does it cover?

The Banner Project Priorities cover through 2008. The IT Master Plan covers the first 5 years of the Bond Measure B with updates required as new technology evolves. The Draft District Strategic Plan, for the specific ITS projects enumerated, covers up to 2 years for the initial service improvements recommended.

d. Who is involved with the planning process?

Chief Technology Officer for the District, Chancellor's Cabinet, College VPs and Directors, District ITS staff, Deans of Technology at the Colleges, College Computer Support staffs.

e. How are accomplishments measured against the plan?

For Banner Projects, Banner User Chairs Committee reviews project progress and status on a monthly basis, Chancellor Cabinet reviews are done periodically based on project progress, and annual Board of Trustees presentations are done on project accomplishments and future planned projects. For Network infrastructure related to Bond Measure B, the activities are monitored through the College Facilities Committees, College Technology Committees, and District Technology Committees with periodic updates to the Chancellor's Bond Steering Committee and the Board of Trustees.

12. Describe the agency's Disaster Recovery

	Yes	No	Comments
Sufficient power protection is provided?	Yes		There is a UPS system for the critical applications today but the time is limited; however, now that funding is available with Bond Measure B, a larger scale UPS and also a generator will be installed to support the District Data Center operations in conjunction with the move to the new IT Building at LPC. At that time, UPS and generators will be installed at both the new central Data Center at LPC and the other remote data centers.
Has a disaster recover plan been developed?	Yes		The Disaster Recovery Plan was developed several years ago and periodic updates are done when appropriate; a new updated plan is scheduled to be completed in conjunction with the Bond Measure B campus improvements and Data Center relocation from Chabot to LPC planned over the next 2 years.
When was it adopted?	Yes		The Disaster Recovery Plan

			was adopted in 1996.
Has it been tested?	Yes		Testing was limited due to available manpower resources. Also, users want minimal service interruption so testing time is limited.
Was the test documented?		No	No formal documentation of the full test cycle is available.
Does the plan cover all aspects of the system?		No	The current Disaster Recovery Plan will be updated under Bond Measure B to address all the new systems in place already as well as those systems being installed over the next 1-2 years, including the new planned Data Center at LPC.

13. Describe the Organization Controls and Personnel Practices:

	Yes	No	Comments
Is IT precluded from correcting user-originated errors?	Yes		Users are responsible to correct the user errors themselves and they are able to do so for most problems. When data problems arise that the users cannot do through the normal system functions or that involve large volume, the programmers will create special scripts to do the correction, but these changes are handled like normal user requests that require testing and approval before implementation. Data corrections such as these require approval at the appropriate management level dependent on the impact.
Is there a separation of programming from systems analysis?	Yes		District ITS has different levels of programmer analyst positions and network systems specialist positions and the position level determines the duties for programming vs.

			systems analysis.
Is there a separation of library function from operations and programmer/systems functions?	Yes		Data access and library access is restricted to the District ITS personnel based on job function. The categories of access include: systems analysts who support IBM, database administrators for Banner System, programmer/analysts, and operations personnel.
Is there a separation of programming, systems analysis, and operations functions?	Yes		Operations job responsibilities are segregated from programmer analyst job responsibilities in accordance with the defined position duties.
Is the data processing control function separate from user and operations functions?	Yes		Data processing controls are restricted to authorized District ITS personnel. Different system access levels are established for programmer/systems analyst, network specialists, operations, and users.
Who provides oversight for the IT department?	Yes		District ITS is under the management of the Chief Technology Officer (CTO) for the District who reports directly to the Chancellor. College Computer Support staff (dotted line to the CTO) are under the direct management of the Dean of Technology for that college and/or the VP Business Services for that college.
New personnel are given hiring tests prior to employment?	Yes		Appropriate technical testing is conducted during the formal interview process.
Background checks are made of applicants for employment?	Yes		Reference checks are performed prior to hire.
IT department employees covered by fidelity bonds?		No	
Are IT department employees provided continuing professional education?	Yes		Professional education is provided on a topic basis either through Web classes, formal vendor product training off-site or on-site,

			and on the job training.
Are there periodic evaluations of IT staff?	Yes		Annual evaluations are done for the ITS staff.
Are the duties of IT staff rotated during times of vacation, illness, etc.?	Yes		ITS staff has been cross-trained to handle other staff members' duties and serve as backup when they are not available.

14. Describe Standard Operating Procedures:

	Yes	**No**	**Comments**
User departments initiate and originate items for processing?	Yes		Selected users have the ability to run portions or all of Banner processes or reports that have been automatically setup by the District ITS staff. However, large scale Banner processes and most routine weekly/monthly processes are still run by the District Operations staff.
Preparation of data is outside IT department?	Yes		Users are responsible for the data preparation for their respective areas to be performed prior to the run of the Banner processes dependent on that data.
Authorization to originate master-file changes is outside IT?	Yes		Users approve any change of Banner data for their respective areas and perform those changes themselves. If the data is large volume or cannot be corrected within the standard Banner controls, the user management requests assistance from the District ITS staff and the controls for testing and approving the modifications are handled just like other projects.
Access to systems and program documentation is restricted?	Yes		Program code is restricted to the District ITS programmer/analysts. Banner system documentation for functional users is

			available on-line but restricted to authorized Banner users only.
Operating activities are defined?	Yes		District ITS Operations staff duties are defined and documented.
Workload is scheduled and up-to-date?	Yes		District Operations staff are active participants in the planning of Banner processes to run per the required schedules. The Operations Supervisor reviews and schedules these processes in coordination with the programmer/analysts and appropriate user groups.
Access to computer facilities and data files is restricted?	Yes		Computer facilities are restricted to the District ITS staff. Access to data files are restricted and vary by job function for programmer analysts, operations, network specialists, and users.

Chabot-Las Positas Community College District
Document Request
Information Technology Audit
June 30, 2005

The following documents should be requested from the IT manager every year:

1. Security Policy
2. User Request Form
3. Business Continuity/Disaster Recovery Plan
4. New Hire Checklist
5. Termination Checklist
6. Backup Procedures
7. Program Change Request Form
8. Default System Configurations
9. Firewall Configuration
10. List of System Administrators and their access
11. Network Architecture Diagram
12. Strategic Plan