Confidential Business Information

Prepared By: SunGard Higher Education
4 Country View Road
Malvern, Pennsylvania 19355
United States of America

Table of Contents

Executive Summary

Bakersfield College

Cerro Coso Community College

Porterville College

KCCD KERN COMMUNITY COLLEGE DISTRICT

Charge

The Kern Community College District (KCCD) undertook an initiative to improve its ability to deliver reliable and cost-effective information technology based services and will accomplish this using a phased approach. The first phase is to document the current state of IT and its ability to support KCCD's instructional and college business operations and to develop strategies and action plans that will serve as a basis for subsequent phases of this initiative. KCCD contracted with SunGard Higher Education to fulfill this charge.

Process

SunGard Higher Education used a hybrid amalgamation of several services in its delivery of this scope of services to the KCCD. This includes select, key components from our IT Organizational Assessment, IT Planning Review, and IT Infrastructure Readiness services. This combination of services offered KCCD an optimized examination of:

- The expectations and plans of its IT stakeholders. This phase of the assessment documented the strategic and business requirements (current and future) of the colleges and district entities
- The ability of current IT infrastructure and staff to deliver future services. This will provide a benchmark of current IT operations and ability to support instructional and college business operations
- The resulting gap analysis which intends to resolve any macro-level differences between supply and demand. This empowers the assessment to develop and document strategies and action plans that will serve as a basis for subsequent phases

SunGard Higher Education used a comprehensive methodology in its consulting process for an IT assessment. At the start of the process there is an advance review of available documentation so that the consulting team is well prepared prior to any client interviews. There is also a detailed planning session with the client's project sponsor to prepare for interviews of key and leading IT stakeholders, IT management and staff.

This methodology includes iterative reviews of initial findings and recommendations with the client's project sponsor. This includes a mix of executive debriefings, presentations, and reviews of the interim report. This methodology also includes a powerful combination of information gathering techniques including a wide variety of interviews (124 in total), a survey of a sampling of faculty, staff and management (195 response out of a sample of 500), and a detailed review of existing documentation (81 in total).

Celebration of Strengths

Individuals, organizations, and certainly assessments tend to focus on existing weaknesses and threats. There is seldom time to consider opportunities and most existing strengths are typically taken for granted. It is important for individuals and organizations to take key moments to celebrate

accomplishments and to reflect upon the strengths that they possess.

During the process of this IT assessment, a number of strengths were discovered within the colleges and district that should be celebrated. These strengths represent the best practices of IT that should be shared within the district and in fact to other institutions when possible. From a strategic standpoint, these strengths should be used to address weaknesses, opportunities, and threats. At the very least, these strengths can form a tactical underpinning to address the next steps resulting from this assessment.

It is to the district and college's credit that these strengths address areas of student computing, instructional technology, and college support services to students in addition to IT infrastructure and processes.

- The Bakersfield College open computing lab makes good use of several technologies that enable proactive management of an environment with diverse and significant demands. The computers are protected by Deep Freeze which prevents students from making permanent changes to the standard images and settings. There is also routinely scheduled re-imaging and software patch updates to these computers. These technologies minimize the amount of reactive events that would require the attention of Bakersfield IT staff.

- The CAD lab at Bakersfield College uses an effective combination of software site licensing and relationships with industry users to maintain a current environment for students to learn this technology from faculty. This "Ready-Fire-Aim" process for maintaining technical currency is an absolute requirement in higher education as compared to private sector. Students must complete courses and degrees with the most modern skill sets that will be required by their potential employers.

- The open computing labs, combined with the LRC's, at both Bakersfield College and Cerro Coso College have proved themselves to be such enticing magnets for student learning that Porterville College is presently constructing a similar environment. The combination of a social environment along with the use of technology and learning resources creates an enticing and memorable student experience. This has been copied from higher education by many commercial bookstores and coffee shops. This will remain a substantial strength of the traditional brick-and-mortar institutions as students increasingly consider the use of online and distance education. A similar comparison has now been drawn in the private sector between the social aspects of movie theaters and shopping malls as compared to home movie viewing and online shopping respectively.

- Some disciplines are easier than others to deliver through alternative media used in distance education. Despite this challenge, several students noted outstanding faculty delivery of classes in the areas of chemistry, astronomy and nursing. The certification process to prepare faculty to deliver effective teaching and learning through these nontraditional mediums is obviously effective. Such a certification

process is actually rare in its use at many other institutions that offer distance education programs.

- The online distance education program at Cerro Coso College created a standard in its day that was used to as a model within the State of California. The use of interactive television in the delivery of a nursing program at Bakersfield College and Porterville College would be of keen interest to every nursing program trying to reach out to more students. Many institutions use this medium but a smaller number of them have done so effectively.

- The Bookstore services at Cerro Coso College for online students are a best practice as a key support service in a distance education model. Many institutions which provide online distance education have been struggling to expand or modify their traditional models of student support to address this new paradigm shift. The areas of focus include counseling, library, bookstore and other traditional services available in the "brick-and-mortar" environment.

- The Bookstore at Cerro Coso College has become a miniature Amazon.com in its operation to support online distance education students. Interviews with students indicated a surprise at the speed of delivery services from this area. This best practice should be shared through white papers and presentations at conferences as an expansion of the institution's best practice established years ago in the online distance education area.

- The use of the Banner Steering Committee and subset functional steering committees is viewed as a successful governance structure over the implementation of this ERP. Particularly in the area of the student system, it is acknowledged that the involvement of appropriate people and the adequate discussion of key issues were well attended to. The combination of communication and deliberation on decisions prove to be a model of effectiveness for the process of implementation of this new technology.

- The data center in the district office, which houses key servers and infrastructure for much of the district and colleges IT systems, is well designed and thought through. The appropriate subsystems, which help to secure and maintain this environment, are all in place. Such an environment is tantamount to the provision of stable, reliable and secure IT systems and services.

Critical Gaps

Many areas of IT infrastructure and IT organizational issues are examined in the detailed report. Three specific areas were seen as the critical gaps as they must be addressed for the district and colleges to improve its collective IT ability to "help itself". They include IT governance, professional development, and IT staffing levels.

Critical Gap and Roadmap: IT Governance
KCCD has a mixed IT organizational structure, with governance and planning for college and district IT occurring at multiple levels across the college and district. This model results in a structure that is not as coordinated or streamlined as it might be, and may limit some options for future growth and benefit.

An IT governance structure will allow key stakeholders to contribute to the problem definition, identification of alternative solutions, and recommendations for implementation. An effective IT governance structure has key members of district or college management as leaders who take the accountability for the decisions based upon the deliberations of the IT governance structure.

The highest-level IT governance holds all subset committees responsible for their charters. This level is called the IT Governance Committee and it functions to monitor, control, and facilitate where necessary the balance of the IT governance structure. The IT Governance Committee should report to the chief executive or senior executive body.

Executive sponsorship from the Chancellor or Executive Council will be critical to the success or failure of the IT Governance Committee and sub-committees. To ensure its successful construction and ability to stand on its own the role of the executive sponsor is, but not limited to the following:

- Provide leadership to the IT Governance Committee
- Ensure the committee focuses on a timely completion of its key tasks
- Ensure an appropriate separation of governance activities and management responsibilities
- Monitor the contribution of committee members and ensure that they are appropriately and actively involved in discussions and decision making
- Provide external mentoring, coaching or facilitation to the committee as needed
- Take a lead role in adjusting the composition and structure of the Committee
- Discharge the subcommittees when their role is no longer required or of further use to the institution

Critical Gap and Roadmap: Professional Development
Throughout KCCD many staff talked about the need for “heavy-duty” professional development specific to technology and Banner. Many indicated that they had not received any professional development training – specific to IT or otherwise – in many years. Most felt professional development was defined as a week-long session held in a geographically different location than the college or district.

When institutions fail to provide ongoing training and professional development for staff, finding competent people to promote or to hire internally for advanced positions becomes increasingly challenging. Additionally, growing gaps between existing skill levels of employees, and the skills actually required to properly and effectively perform the job for which they were hired begin to appear. This type of environment almost inevitably presents challenges that typically include lower staff morale, decreased work productivity, and increased errors.

There is a need to create a professional development plan for each IT employee based on needed areas of knowledge and skills related to their job function and level. These needs are established by referencing relevant strategic goals, competency lists, job descriptions, job analysis, task analysis, as well as the institutions mission. There are twelve different roadmaps detailed within the report; however, the key is to remove the time and location boundaries of assumed training. That is, the use of blended training media used for KCCD's students should be "turned inward" and applied to delivery new IT content training to staff.

Critical Gap and Roadmap: IT Staffing Levels

The continued need for new technology will press the existing IT staffing levels given the limitations of budget. This is exacerbated by the limited amount of professional development training to keep maintain and improve IT staff skills.

The college and district IT departments believe they are inadequately staffed to support the technology needs of the institution. Performance metrics are not captured that would justify and / or validate the perceived need for additional staff.

Specific to the support of existing IT infrastructure and services, it is obvious that the quantities and qualities of IT staff at Cerro Coso College are inadequate to support its existing environment. It is not as obvious a deficiency in the other colleges and district office. The permanent IT staff and management at Cerro Coso should be recruited and put into place to effectively support the existing desktop, open lab, distance education, and network technologies.

The only inefficiency noted in the current staffing model is the redundancy of staffing for the multiple help desks throughout the district. The staffing, operations, equipment and facilities should be consolidated among the current varieties of help desks within the district.

Specific to the support of new IT infrastructure and services, there is no obvious "bench" of the appropriate expertise to address the rapids of technology changes that continue to grow from year-to-year. Additional staffing and management skill sets are required for emerging technologies. Where possible, efficiencies should be sought in the temporary use of contractors, consultants, part-time staff, etc. In the rare case where the volume of work necessitates the hiring of full-time staff or management, these new positions should be placed at the district level and serve all colleges. The passage of time and escalating use requirements might eventually require each college to have such a position

added for dedicated local support.

SWOT Workshop

The facilitation of a Strengths, Weaknesses, Opportunities and Threats (SWOT) Analysis, conducted by a SunGard Higher Education consultant, was held with key members of KCCD faculty, staff and management. The general purpose of the meeting was to begin discussions on the need for developing a strategic plan for information technology at KCCD. Each of the key stakeholders within the institution shared their opinions on strategic planning elements of significant consideration to the institution.

The work session developed a key step in the IT strategic planning process, which is to analyze the strengths, weaknesses, opportunities, and threats -- the SWOT analysis. Its primary purpose is to ensure that an institution is positioned to take maximum advantage of the capabilities of information technology to achieve their organizational objectives. Additionally, it provides a starting point to establish (or validate) a clear long-term direction for all technology projects and expenditures.

The SWOT Workshop was conducted at the Bakersfield College Fireside Room on Thursday, March 8, 2007 from 9:00 a.m. to 12:45 p.m. There was a high degree of engagement which rendered a significant number of suggestions to include in the SWOT. 20 KCCD faculty and staff participated in the SWOT Workshop.

During the session, participants were allowed to “vote” on the most significant of each areas of the SWOT. By selecting a subset of the high vote issues, several subset “themes” were derived and represented in cruciform charts. From these cruciform charts, a SWOT analysis was conducted which offered some strategies to be pursued. The first cruciform chart sifted significant issues that are specific to IT infrastructure and rendered the following suggested strategy:

- Increase the accessibility of IT for teaching and learning by students and faculty

Relevant qualitative, long-term goals underpinning this strategy may include:

- Expand network availability to laptops brought into colleges by students
- Support the expanded use of teaching and learning using popular student devices such as iPOD’s
- Expand the use of portable computing devices to faculty
- Introduce wireless access in key areas for students and faculty
- Promote the district and colleges with a presence on new social networks including MySpace and YouTube

The next cruciform chart sifted significant issues that are specific to data usage and training and rendered the following suggested strategy:

- Empower staff with self-service data and expanded IT training

Relevant qualitative, long-term goals underpinning this strategy may include:

- Expand the use of self-service data access through portal technologies, web access and data warehouse tools
- Expand the use of data-driven planning
- Introduce "anytime – anywhere" training for all staff on current and emerging IT topics
- Expand the use of enrollment management tools to increase student enrollment

The third and final cruciform chart sifted significant issues that are specific to IT staff and management processes and rendered the following suggested strategy:

- Evolve the quantities and skills sets of IT staff and management to improve and appropriately expand services to all stakeholders supporting the mission of the colleges and district.

Relevant qualitative, long-term goals underpinning this strategy may include:

- Introduce training for IT management and staff on emerging issues such as security, mobile technologies, wireless, etc.
- Track consistent and complete metrics on equipment and users to derive a formula for allocating the appropriate types and number of IT staff within the district and college.
- Introduce new staff positions where volume of work necessitates the addition of dramatically different skill sets.

User Satisfaction Survey

During March 2007 a survey was conducted to assess service levels and user satisfaction with college and district IT departments. Full-time faculty, adjunct faculty, classified / confidential staff and management were randomly selected to participate in the survey.

The purpose of the survey was to:

- Measure the satisfaction and importance of college and district IT / IS services at baseline
- Inquire which additional or improved services would be most valuable
- Give users a voice to influence college and district IT / IS service priorities and potential initiatives

The online survey was distributed to approximately 500 randomly chosen users of college and district IT / IS services. College and district IT / IS staff were excluded from participating.

There was an interesting mix of responses to the satisfaction with several IT services. Among the highest scores was Internet services. The lowest average response was training which corresponds with many of the findings during the assessment phase.

Spam proved to be the most significant concern among IT issues. The use of a variety of portable computing devices was significant.

There was a large selection of help desks that are referred to when assistance is required. While most scored reasonable satisfaction rates their frequency of use appears to be low. The resolution rate for problems showed some significant duration.

By far the most interesting outcome was on the topic of IT security. Half of all respondents use a common password for different logon applications; however, the majority of users change these passwords infrequently. Enough users share passwords or write them down for to pose a significant risk. Finally, there is significant storage of confidential or sensitive information to portable devices.

Next Steps

It is important to begin to focus on the immediate next steps that should be taken at the conclusion of the assessment. After a reasonable review and discussion on findings and recommendations, it is imperative to select from the suggested top priorities and began with an action plan.

As an added value, there is a rich selection of tools that can be used to navigate the roadmaps – or recommendations – that have been made in this report. These navigational tools represent best practices that can be immediately considered and tailored for use within KCCD. It is usually easier to critique and modify an existing best practice to address the unique needs of an institution than to create something new from scratch. Obviously, the degree of required tailoring will vary for each navigational tool.

The obvious difficulties are the lack of available and appropriate resources to implement many of these recommendations. The majority of existing staff are preoccupied with current operations or projects. In many cases the required talents or backgrounds necessary to implement these recommendations may be missing within KCCD. As such, KCCD should consider the temporary use of facilitators, contractors or consultants to act as the catalysts for change. Any use of such temporary staff should offer ideal mentoring, coaching, professional development, or cross-training of existing staff during their engagements. After such temporary staff have completed their engagements and cross-training then the existing KCCD staff will be able to continue to manage, operate and maintain any changes that have been put into place.

Throughout the implementation of the IT assessment next steps, and particularly at the beginning, it is important that KCCD use the proposed IT governance structure to monitor and control this implementation project. The governance structure should assign the required resources and then hold them accountable for successful completion of the next steps. This drive for stronger governance and requisite accountability will be key to the empowerment of KCCD's user community in improving the deployment and use of IT.

A large part of the value of an assessment report must be measured on the positive impact it makes on its subject area in the future. The consensus and understanding of the issues that must be addressed have been placed in their prioritized order within a proposed Short-Term Improvement Program (STIP) named the "KCCD IT Assessment Implementation Program". It is recommended that KCCD consider and adopt a selection of the high priority activities identified within the program immediately to begin making progress.

Overview

Bakersfield College

SunGard Higher Education will use a hybrid amalgamation of several services in its delivery of this scope of services to the Kern Community College District (KCCD). This includes select, key components from our IT Organizational Assessment, IT Planning Review, and IT Infrastructure Readiness services. This combination of services will offer Kern an optimized examination of:

- The expectations and plans of its IT stakeholders. This phase of the assessment documents the strategic and business requirements (current and future) of the colleges and district entities.
- The ability of current IT infrastructure and staff to deliver future services. This will provide a benchmark of current IT operations and ability to support instructional and college business operations.
- The resulting gap analysis which intends to resolve any macro-level differences between supply and demand. This empowers the assessment to develop and document strategies and action plans that will serve as a basis for subsequent phases.

Methodology & Approach

SunGard IT Assessment uses various techniques for data collection to draw its conclusions and make recommendations. The service is provided in three phases:

- Phase I – Gather and Analyze Information on Client Environment
- Phase II – On-Site Reviews
- Phase III – Final Report

Phase I – Gather and Analyze Information on Client Environment
A review of all relevant procedures, processes and documentation within the allocated duration was conducted. Observations and recommendations are documented. A range of documentation was requested for review including:

Help Desk
- Software Inventory (include version level) - Service Level Agreement(s) - Problem Management Reports - Call Statistics (ACD monthly activity reports) - Standard Operating Policies and Procedures - Help Desk Tools (problem and call management) - Staff Training Plans (personal, technical and professional) - Client Satisfaction Surveys - Promotional Materials - Help Desk Problem Ticketing / Telephone Software License and Support Contracts - 3rd Party Vendor Contracts

Network
- Network Infrastructure diagram(s) - Network Equipment Inventory List - Network Statistics (if available) - Security Policy
Systems & Databases
- Server Inventory (or new equipment list) for any Banner related servers - List of administrative applications, languages and databases - Database sizes and statistics, if available - Details of planned technical training
Data Center
- Operations documentation - Backup and recovery documentation - Disaster Recovery Plan - Computer Room floor plan
IT Organization
- IT Governance Organizational Chart - IT Strategic Plan - IT Annual Work Plan - IT Organization Chart - IT Departmental Contact List (titles, phone numbers and email addresses) - IT Job Descriptions (applications, systems, database, network, helpdesk, data center, desktop support) - IT Staff Training Plans (personal, technical and professional) - IT Performance Goals and Objectives (sampling) - IT Recent Performance Evaluations (sampling) - IT Strategic Plan - IT Annual Work Plan - IT Budget - List of all meetings IT staff attend
Institutional
- College / Campus / Building Maps - Institutional Facts (including number of students, faculty, staff) & Growth Plans - Institutional Strategic Plan - Business Continuity Plan

The following items were provided prior and/or during the site visit:

KERN COMMUNITY COLLEGE DISTRICT (KCCD)	
DOCUMENT	**LOCATION**
Quick Facts about KCCD	http://www.kccd.edu/Quick%20Facts/Default.aspx
Frequently Asked Questions	http://www.kccd.edu/FAQ.aspx

KERN COMMUNITY COLLEGE DISTRICT (KCCD)	
DOCUMENT	**LOCATION**
Strategic Plan (approved 9/06)	http://www.kccd.edu/Chancellor/Strategic%20Planning/Strategic%20Plan/Default.aspx
Learning Services Center Service Quality Survey (Fall 2002)	http://www.pc.cc.ca.us/research/Files/survey%20reports/LSC%20Service%20Quality%20Survey%20Report.pdf
Strategic Planning Survey (09/04)	http://www.pc.cc.ca.us/research/Files/survey%20reports/KCCD%20Strategic%20Planning%20Survey%20Report.pdf
District Office IT/LSC Organizational Chart	http://sp.kccd.edu/ita/General/District%20IT%20ORG%20CHART%20-%20July%202006.pdf
IT Staff Directory	http://www.kccd.edu/Information%20Technology/Default.aspx
IT Job Descriptions	http://sp.kccd.edu/ita/Job%20Descriptions/Forms/AllItems.htm
District IT Enterprise Backup Guide (Data Center Tab)	http://sp.kccd.edu/ita/Data%20Center/Forms/AllItems.htm
District IT Banner Backup Schedule note	http://sp.kccd.edu/drsec/Systems%20BackupVeritas/banner%20Backup%20info.htm
IT Security Policy (Policies Tab)	http://sp.kccd.edu/ita/Policies/(Unadopted)%20Board%20Policy%20-%20Information%20Technology%20Security%20Policy%20---%20DRAFT%20Ver%204.doc
District Office Master System List (Draft; Systems Team Tab)	http://sp.kccd.edu/ita/Policies/(Unadopted)%20Board%20Policy%20-%20Information%20Technology%20Security%20Policy%20---%20DRAFT%20Ver%204.doc
District IT Plan (Outdated; General Tab)	http://sp.kccd.edu/ita/General/District%20IT%20Plan.pdf
BT Infonet Disaster Recovery Security Presentation (04/05; General Tab)	http://sp.kccd.edu/ita/General/Infonet%20KCCD_DR_SEC_Presentation.pdf
BT Infonet Security and Disaster Recovery Gap Analysis (01/05; General Tab)	http://sp.kccd.edu/ita/General/Infonet%20Security%20and%20DR%20GAP%20Analysis%20Report%20-%20Jan2005V3.doc
Banner Management Framework (General Tab)	http://sp.kccd.edu/ita/General/KCCD%20Banner%20Management%20Framework.jpg
Banner Steering Charge Overview	http://sp.kccd.edu/ita/General/KCCD%20Banner%20Steering%20Charge%20Overview.doc
Organizational and Operational Effectiveness Study (03/01 by KH; General Tab)	http://sp.kccd.edu/ita/General/KH%20Final%20Rpt%203-15-2001.pdf

KERN COMMUNITY COLLEGE DISTRICT (KCCD)	
DOCUMENT	**LOCATION**
Director of IT Goals 2006 – 2007 (General Tab)	http://sp.kccd.edu/ita/General/LSC%20Dir%20of%20IT%20Goals%20for%202006-07.doc
District Office Help Desk Phone Tree (Network Tab)	http://sp.kccd.edu/ita/Network/District%20Office%20Help%20Desk%20PhoneTree.pdf
WAN Physical (Network Tab)	http://sp.kccd.edu/ita/Network/KCCD_WAN_physical.pdf
IT Vision and Mission Statements	http://www.kccd.edu/Information%20Technology/VisionAndMission.aspx
HelpMaster Software (DO & BC Help Desk Problem Management Software)	http://www.prd-software.com.au/prd/help-deak-products/enterprise/features.asp
District Wide CMS Evaluation Task Force	http://sp.kccd.edu/ita/General/CC%27s%20Distance%20Education%20Summary%20Report%202005-2006.doc
KCCD VideoTech Use Survey May 2006	http://sp.kccd.edu/ita/General/KCCD%20VideoTech%20Use%20Survey%20May06.pdf
Microwave Network Support Contract	http://sp.kccd.edu/ita/General/Forms/AllItems.htm
Using Technology for District-Wide Meetings – DP President & Notes	http://sp.kccd.edu/ita/General/Using%20Technology%20for%20District-wide%20Meetings%20-%20DP%20Pres%20and%20Notes.ppt#270,13,Current Interactive TV Support Model
District-Wide Distance Education Task Force Recommendation (01/2006)	Hard copy provided by Eddie Alvarado
Sample Help Desk reports	Hard copy provided by Rosemary Lopes
HelpMaster Pro License details	Hard copy provided by Rosemary Lopes
Help Desk procedural guide	Hard copy provided by Rosemary Lopes
IT Job Procedure Manual (Help Desk)	Hard copy provided by Rosemary Lopes
Sample Help Desk ticket entry	Hard copy provided by Rosemary Lopes
KCCD News Brief (11/2006)	Hard copy
Banner Access Request & Training Validation	Hard copy

BAKERSFIELD COLLEGE (BC)	
DOCUMENT	**LOCATION**
Quick Facts about BC	http://www.bc.cc.ca.us/about/
Strategic Plan (2006 – 2007 Educational Master Plan)	https://www.bc.cc.ca.us/irp/Institutional_Effectiveness/Ed_Master_Plan/Ed_MasterPlan_Index.asp
Accreditation Study (10/06)	http://www2.bc.cc.ca.us/accreditation/20-wholestudy.pdf
Student Satisfaction Survey (04/00)	http://www.bakersfieldcollege.edu/irp/Surveys/S00%20Student%20Survey%20Summary%20Results.pdf
IS Staff Directory	http://www2.bc.cc.ca.us/is/ourteam.asp
Faculty & Staff Satisfaction Survey (04/99)	http://www.bakersfieldcollege.edu/irp/Surveys/S99%20Staff%20Survey%20Summary%20Results.pdf
Media Services Staff Directory	http://www2.bc.cc.ca.us/mediaservices/
IT Systems & Database Listing (Systems Team Tab)	http://sp.kccd.edu/ita/Policies/(Unadopted)%20Board%20Policy%20-%20Information%20Technology%20Security%20Policy%20---%20DRAFT%20Ver%204.doc
IS 2006 – 2007 Budget (General Tab)	http://sp.kccd.edu/ita/General/BC%20IT%202006-2007%20Budget.doc
Software Inventory (General Tab)	http://sp.kccd.edu/ita/General/BC%20Software%20Inventory.xls
Computer Use Procedures	http://www2.bc.cc.ca.us/is/BCCompUse.pdf
Web Policy, Procedures and Style Guides	http://www2.bc.cc.ca.us/is/Bakersfield_College_Web_Policy_Final_Version.pdf
Department News	http://www2.bc.cc.ca.us/is/default.asp
Altiris Vision Tutorial	http://www2.bc.cc.ca.us/is/tutorials.asp?cat=Altiris%20Vision
Outlook Tutorial	http://www2.bc.cc.ca.us/is/help/OUTLOOKWEB_V4.pdf
IT Goals (Accomplishments)	http://www2.bc.cc.ca.us/is/goals.asp
Computer Labs	http://www2.bc.cc.ca.us/is/ComputerLabs/
Non-IT Staff Training Opportunities	http://www.bakersfieldcollege.edu/staff_development/
Campus / Building Maps	http://www.bakersfieldcollege.edu/about/maps/map.pdf
The Source Magazine (11/2006)	Hard copy
2006 Summer/Fall Class Schedule	Hard copy
Spring 2007 Class Schedule	Hard copy
Distance Learning packet	Hard copy provided by Kathleen Loomis-Tubbesing
Fall 2006 Enrollment (Interactive Courses)	Hard copy provided by Kathleen Loomis-Tubbesing
Redesign of BC website (under development)	http://new.bakersfieldcollege.edu
Sample Help Desk reports	Hard copy provided by Judy Ahl

CERRO COSO COLLEGE (CC)	
DOCUMENT	**LOCATION**
Quick Facts about CC	http://www.cerrocoso.edu/about/index.htm
Home Page (President's Page; Mission/Philosophy; District; College Goals; Why You Should Attend CCCC; Board Report 08/06)	http://www.cerrocoso.edu/about/welcome.htm
Accreditation Study 2006	http://www.cerrocoso.edu/accreditation/2006/reports/2006%20Acreditation%20Self%20Study.pdf
IT Staff Directory	http://www.cerrocoso.edu/it/staff.htm
IT Home Page	http://www.cerrocoso.edu/it/Default.htm
Help Desk Priorities Flowchart	http://www.cerrocoso.edu/it/Default.htm
Computer Use Policy	http://www.cerrocoso.edu/it/Default.htm
Website Policies & Guidelines	http://www.cerrocoso.edu/it/Default.htm
"How To" (includes Outlook/Exchange Training Manual; FAQ on various topics)	http://www.cerrocoso.edu/it/howto.htm
IssueTrak (Help Desk Problem Management Software)	http://www.issuetrak.com/features.htm
Distance Education Summary Report, Cerro Coso Community College, Academic Year 2005-2006	http://sp.kccd.edu/ita/General/CC%27s%20Distance%20Education%20Summary%20Report%202005-2006.doc
The Coyote Howler (11/2006)	Hard copy
Spring 2007 Schedule of Classes	Hard copy

PORTERVILLE COLLEGE (PC)	
DOCUMENT	**LOCATION**
Quick Facts about PC	http://www.portervillecollege.edu/president/index.html
Strategic Plan (2002 – 2009 Educational Master Plan)	http://www.pc.cc.ca.us/research/Files/Planning%20Documents/Educational%20Master%20Plan.pdf
Accreditation Study (10/06)	http://www2.bc.cc.ca.us/accreditation/20-wholestudy.pdf
IT Staff Directory	http://www.portervillecollege.edu/Staff_Directory/index.html
Library Netbook Quick Start Guide	Hard copy
Library Subscription Databases (site listing with URL's ID's and UserName & Passwords)	Hard copy
Update Newsletter (08/2006 & 11/2006	Hard copy

Phase II – On-Site Interviews
This phase was performed at the Kern Community College District office as well as Bakersfield College, Cerro Coso Community College and Porterville College. During this phase SunGard interviewed personnel to review and focus on the following:

- The expectations and plans of its IT stakeholders, documenting the strategic and business requirements (current and future) of the colleges and district entities.
- The ability of the current IT infrastructure and staff to deliver future services, providing a benchmark of current IT operations and ability to support instructional and college business operations.
- The resulting gap between supply and demand. This empowers the assessment to develop and document strategies and action plans that will serve as a basis for subsequent phases.

During the engagement at KCCD the following staff was involved in this assessment:

BAKERSFIELD COLLEGE (BC)	
NAME	**DEPARTMENT / OFFICE / DIVISION**
Adie Geiser	Supportive Services
Angela Alvarado	EOP&S
Angela Guadian	Title V
Ash West	Student
Dr. Bill Andrews	President
Bill Moseley	Computer Studies
Bob Shimmin	Information Services
Brian Larson	Student
Bryan Smith	Information Services
Candice Carmona	Human Resources
Carol Barling	Information Technology (Training)
CeCe Westerfield	Information Services
Chris Leithiser	Information Services
Cindi Swoboda	Distance Learning
Cindy Collier	Allied Health
Dr. J. Dan O'Connor	Math, Science and Engineering
David Barnett	Information Services
Dean Serabian	Information Services

BAKERSFIELD COLLEGE (BC)	
NAME	**DEPARTMENT / OFFICE / DIVISION**
Dennis Jorgenson	Industrial Technology
Don Turney	EOP&S
Earl Parsons	Student
Ed Knudson	Student Learning
Gayle Richardson	Business Administration
James Boughton Jr.	Student
Jim McGee	Information Services
Joan Wegner	Financial Aid
John Griffith	Business Services
John Jaramillo	Educational Administration
Joyce Kirst	Supportive Services
Judy Ahl	Information Services
Kathleen Loomis-Tubbesing	Distance Learning
Kathy Howarth	Human Resources
Kristin Rabe	Media Services
Kirk Russell	Library
Micah Card	Student
Dr. Mildred Lovato	Student Services
Monty Snyder	Information Services
Nick Strobel	Physical Science
Patricia Ross	Student Learning
Patrick Ferree	Information Services
Phil Mesel	Computer Studies
Osmond Param	Student
Rachel Vickrey	Mathematics
Sue Granger-Dickson	Learning Support Services
Sue Vaughn	Enrollment Services
Zenaida Tutop	Human Resources / Payroll

CERRO COSO COLLEGE (CC)	
NAME	**DEPARTMENT / OFFICE / DIVISION**
Candace Cornett	Financial Aid
Chris Harper	Information Technology
Corey Marvin	Information Technology

CERRO COSO COLLEGE (CC)	
NAME	**DEPARTMENT / OFFICE / DIVISION**
Cori Ratliff	Information Technology
Dan Johnson	Information Technology
David Cornell	Admissions & Records / Veteran's Affairs
Debby Kilburn	Computer Science
Dennis VanderWerff	Learning Resource Center
Gale Lebsock	Business Services
Heather Ostash	Counseling
Dr. Jane Harmon	Student Learning
Janet Wilson	Library
Jill Board	Student Services
John Daly	Maintenance & Operations
Karen O'Connor	Business Office Technology / Computer Science
Kiana Wyatt	CC Online
Lori Olivera	CC Online
Dr. Mary Retterer	President
Matt Hightower	CC Online
Mike Barrett	Information Technology
Natalie Dorrell	Bookstore
Pam Coward	Human Resources
Resa Hess	Human Resources
Robotic Class (Kilburn)	Students

PORTERVILLE COLLEGE (PC)	
NAME	**DEPARTMENT / OFFICE / DIVISION**
Antonia Ecung	Academic Center
Chris Craig	Technology Services
Diane Allen	Academic Center
Donna Berry	Business Services
Gary Wallace	Auxiliary Services, Maintenance & Operations
James Carson	Academic Center
Janet Hawkins	Human Resources
Jennie Brission	Human Resources
Dr. Kathy Bennett	Learning / Technology Services
Lorie Barker	Library / Media Center

PORTERVILLE COLLEGE (PC)	
NAME	**DEPARTMENT / OFFICE / DIVISION**
Lydia Smith	Academic Center
Randy Morgan	Information Services
Richard Goode	Science / Mathematics
Rickelle Syradahl	Science / Mathematics
Dr. Rosa Carlson	President
Sarah Phinney	Library / Media Center
Steve Schultz	Academic Center
Terry Harter	Library / Media Center
Vern Butler	Technology Services
Virginia Gurrola	Financial Aid / Admissions & Records

DISTRICT OFFICE (DO)	
NAME	**DEPARTMENT / OFFICE / DIVISION**
Brian Tully	Information Technology
Carl Bowman	Information Technology
Charley Chiang	Information Technology
Christina Ipe	Information Technology
Dana Tusaw	Information Technology
David Palinsky	Information Technology
Eddie Alvarado	Information Technology
Dr. Greg Chamberlain	Educational Services
John Collins	Consultant
Judy Marty	Human Resources
Karen Pryor	Information Technology
Kenneth Robinson	Human Resources
Kim Crews	Facilities
Marc Beam	Institutional Research
Marco Galvez	Information Technology
Mary Jones	Human Resources
Michael Regpala	Information Technology
Mike Arnold	Information Technology
Pam Whitley	Human Resources
Patti Evans	Information Technology
Raj Doshi	Information Technology
Randy Patterson	Facilities

DISTRICT OFFICE (DO)	
NAME	**DEPARTMENT / OFFICE / DIVISION**
Ron Wilson	Information Technology
Rosemary Lopes	Information Technology
Sally Errea	Educational Services
Sandra Serrano	Chancellor
Sean James	Internal Audit
Stephen Kegley	Information Technology
Suyun Ding	Information Technology
Todd Coston	Information Technology
Tom Burke	Finance
Trudy Geissel	Human Resources
Victor Collins	Human Resources
Wayne Clement	Information Technology

Phase III – Final Report

This phase focuses on combining the information gathered and analyzed in Phases I and II to develop the IT Assessment report. The report documents findings and provides a roadmap for enhancements and improvements. A site visit is scheduled for Tuesday, March 27, 2007at KCCD to discuss the findings and recommendations of the report.

Exclusions

The following areas were not the focus of this assessment and include:

- Functional or technical considerations of the Banner system
- Capacity planning for servers
- Detailed network infrastructure analysis
- Detailed cost analysis

Celebration of Strengths

Bakersfield College

Individuals, organizations, and certainly assessments tend to focus on existing weaknesses and threats. There is seldom time to consider opportunities and most existing strengths are typically taken for granted. It is important for individuals and organizations to take key moments to celebrate accomplishments and to reflect upon the strengths that they possess.

During the process of this IT assessment, a number of strengths were discovered within the colleges and district that should be celebrated. These strengths represent the best practices of IT that should be shared within the district and with to other institutions when possible. From a strategic standpoint, these strengths should be used to address weaknesses, opportunities, and threats. At the very least, these strengths can form a tactical underpinning to address the next steps resulting from this assessment.

It is to the district and college's credit that these strengths address areas of student computing, instructional technology, and college support services to students in addition to IT infrastructure and processes.

Student Computing Labs

The Bakersfield College open computing lab makes good use of several technologies that enable proactive management of an environment with diverse and significant demands. The computers are protected by Deep Freeze which prevents students from making permanent changes to the standard images and settings. There is also routinely scheduled re-imaging and software patch updates to these computers. These technologies minimize the amount of reactive events that would require the attention of Bakersfield IT staff.

The CAD lab at Bakersfield College uses an effective combination of software site licensing and relationships with industry users to maintain a current environment for students to learn this technology from faculty. This "Ready-Fire-Aim" process for maintaining technical currency is an absolute requirement in higher education as compared to private sector. Students must complete courses and degrees with the most modern skill sets that will be required by their potential employers.

The open computing labs, combined with the LRC's, at both Bakersfield College and Cerro Coso College have proved themselves to be such enticing magnets for student learning that Porterville College is presently constructing a similar environment. The combination of a social environment along with the use of technology and learning resources creates an enticing and memorable student experience. This has been copied from higher education by many commercial bookstores and coffee shops. This will remain a substantial strength of the traditional brick-and-mortar institutions as students increasingly consider the use of online and distance education. A similar comparison has now been drawn in the private sector between the social aspects of movie theaters and shopping malls as compared to home movie viewing and online shopping respectively.

Instructional Technology Use By Faculty
Some disciplines are easier than others to deliver through alternative media used in distance education. Despite this challenge, several students noted outstanding faculty delivery of classes in the areas of chemistry, astronomy and nursing. The certification process to prepare faculty to deliver effective teaching and learning through these nontraditional mediums is obviously effective. Such a certification process is actually rare in its use at many other institutions that offer distance education programs.

The online distance education program at Cerro Coso College created a standard in its day that was used to as a model within the State of California. The use of interactive television in the delivery of a nursing program at Bakersfield College and Porterville College would be of keen interest to every nursing program trying to reach out to more students. Many institutions use this medium but a smaller number of them have done so effectively.

College Support Services to Students
The Bookstore services at Cerro Coso College for online students are a best practice as a key support service in a distance education model. Many institutions which provide online distance education have been struggling to expand or modify their traditional models of student support to address this new paradigm shift. The areas of focus include counseling, library, bookstore and other traditional services available in the “brick-and-mortar” environment.

The Bookstore at Cerro Coso College has become a miniature Amazon.com in its operation to support online distance education students. Interviews with students indicated a surprise at the speed of delivery services from this area. This best practice should be shared through white papers and presentations at conferences as an expansion of the institution’s best practice established years ago in the online distance education area.

IT Infrastructure and Processes
The use of the Banner Steering Committee and subset functional steering committees is viewed as a successful governance structure over the implementation of this ERP. Particularly in the area of the student system, it is acknowledged that the involvement of appropriate people and the adequate discussion of key issues were well attended to. The combination of communication and deliberation on decisions prove to be a model of effectiveness for the process of implementation of this new technology.

The data center in the district office, which houses key servers and infrastructure for much of the district and colleges IT systems, is well designed and thought through. The appropriate subsystems, which help to secure and maintain this environment, are all in place. Such an environment is tantamount to the provision of stable, reliable and secure IT systems and services.

IT Governance

Open Lab

- **SHORT STAFFED**
- **HISTORICALLY LIMITED / SHRINKING BUDGETS**
- **GREATER DEMAND FOR SERVICES**
- **INCREASINGLY COMPLEX INFRASTRUCTURES**
- **GROWING REGULATORY COMPLIANCE AND LEGISLATED BURDENS**

It is no secret that these have become standard operating conditions in many IT departments. While enterprise infrastructure, resource management and IT resource infrastructure and portfolio management solutions can help to mitigate these burdens, they do not facilitate visibility into the interdependencies of resources across business processes, policies, regulatory compliance and legislated mandates. As a result, business units understanding cross-functional risks, their impacts, and the ways these risks can be managed is difficult, if not impossible.

With a governance approach, IT departments can offer business units within an institution a collaborative environment for key users of IT services including networks, applications, transactions, and the use of data. With a robust, adaptive and collaborative governance approach, IT can link all of these assets to specific policies and processes, delivering a contextual framework for determining how the IT infrastructure can be exploited to enable more effective governance through improved management of regulatory and legislative compliance / mandates, technology and other business risks.

a. Finding(s)

KCCD has a mixed IT organizational structure, with governance and planning for college and district IT occurring at multiple levels across the college and district. This model results in a structure that is not as coordinated or streamlined as it might be, and may limit some options for future growth and benefit.

The current governance structure operates in a feudal / silo environment (where each college/business unit independently builds systems and sets priorities) rather than one that is more of an adaptive / collaborative mindset, where achieving a common purpose is the overriding goal, thereby eliminating the "I" mentality. The existing structure has the potential to set up rewards for competition, as opposed to collaboration, which may result in patterns that benefit individual areas rather than the entire institution.

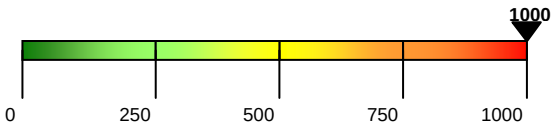
Possible Impact

KCCD's current IT organizational mix has limited its ability to develop institution-wide IT priorities and strategic plans and to effectively align and implement consistent and effective IT support services on emerging technologies.

The lack of formal IT governance limits key stakeholder participation in driving all of the priority IT needs of the institution. IT projects can experience abrupt starts and stops as they operate in small silos. The lack

of formal IT governance creates confusion about IT roles and responsibilities and the demarcations of authority. This can result in a lack of accountability for both the delivery and management of IT services and support at the college and department level. Additionally, overlaps and gaps in IT services, applications, support and equipment are inevitable and significantly increase institutional costs (e.g., seven help desks, at least two incident / problem management applications, business units independently pursing applications, etc.).

Suggested Priority for Resolution



Roadmap

For many years now, publicly funded institutions have seen a steady decline in many different revenue sources including state and federal government. Some have argued that these cuts have reduced the quality of education. The issue is that real solutions to the problems confronting most institutions require organizational and governance changes.

An IT governance structure will allow key stakeholders to contribute to the problem definition, identification of alternative solutions, and recommendations for implementation. An effective IT governance structure has key members of district or college management as leaders who take the accountability for the decisions based upon the deliberations of the IT governance structure.

The highest-level IT governance holds all subset committees responsible for their charters. This level is called the IT Governance Committee and it functions to monitor, control, and facilitate where necessary the balance of the IT governance structure. The IT Governance Committee should report to the chief executive or senior executive body.

Executive sponsorship from the Chancellor or Executive Council will be critical to the success or failure of the IT Governance Committee and sub-committees. To ensure its successful construction and ability to stand on its own the role of the executive sponsor is, but not limited to the following:

- Provide leadership to the IT Governance Committee
- Ensure the committee focuses on a timely completion of its key tasks
- Ensure an appropriate separation of governance activities and management responsibilities
- Monitor the contribution of committee members and ensure that they are appropriately and actively involved in discussions and decision making

- Provide external mentoring, coaching or facilitation to the committee as needed
- Take a lead role in adjusting the composition and structure of the Committee
- Discharge the subcommittees when their role is no longer required or of further use to the institution

The charter for the primary IT Governance Committee should be detailed as follows. Other subset governance committees should follow a similar charter.

1) Hold the chair of the committee accountable for assuring that the actions of the committee are effective, efficient and appropriate to its charter.

2) Communicate progress and issues in all appropriate directions within the institution.

3) Facilitation, coaching or mentoring is sought out when assistance is needed owed to required direction, impasses, or the need for additional expertise.

4) Establish and invoke an adaptive / collaborative IT governance structure to clearly delineate roles and responsibilities and to coordinate institutional IT decisions and policies, providing for appropriate conflict resolution.

5) Establish formal sub-committee work groups. **SEE FIGURE 1 – RECOMMENDED KCCD IT GOVERNANCE COMMITTEE STRUCTURE.** Key characteristics of work groups include but are not limited to:

   - Staffing support
     - Facilitate meetings at a strategic level
     - Ensure tactical actions are implemented by all responsible bodies
     - Own and be accountable for implementing a communication strategy
     - Track and respond to issues raised by the community stakeholders
     - Provide analysis of issues (as requested)

   - Meet at regular intervals
     - Calendar of meeting dates is publicized
     - Agendas for meetings are publicized in advance

   - Annual review of the scope, membership and charter
     - Ensure outcomes meet KCCD expectations
     - Identify opportunities for improving IT governance

- Make modifications to IT governance as appropriate

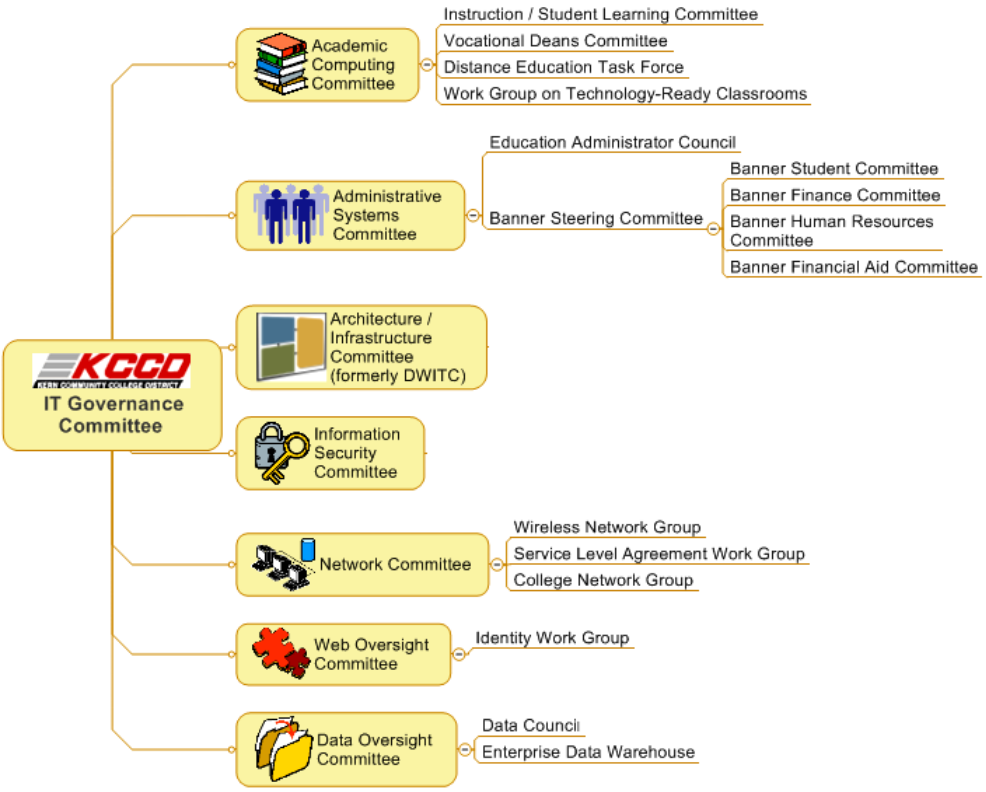


Figure 1 – Recommended KCCD IT Governance Committee structure

6) Appoint members to the Academic Computing Committee that have a global orientation. Representation includes but is not limited to:

   - KCCD Academic Champion
   - Representative Faculty (one per college)
   - Representative from the Administrative Computing Committee
   - Librarian

7) Appoint members to the Administrative Systems Advisory Committee. Representation includes but is not limited to:

   - Representative Administrative Staff from the colleges and district
   - Representative from the Academic Computing Committee

8) Appoint members to the IT Governance Committee that have an institutional orientation and capacity to think strategically and define tactically. Representation includes but is not limited to:

- College President who serves as Chair
- Executive VP from DO
- College Support Services
- Library
- Faculty (involved in instructional or distance learning technology)

Where possible on this committee and all others, student subcommittees should be formed for specific input when possible and necessary.

9) Additional members participate in the IT Governance Committee as ex officio. Representation includes but is not limited to:

- Director of IT
- College IT Managers
- Academic Computing Champion
- Faculty members from the Academic Computing Committee (appointed by the Academic Computing Committee)
- Business Officer from the Administrative Computing Committee (appointed by the Administrative Computing Committee)
- Architecture / Technology Committee representative
- Information Security Committee representative
- Network Committee representative
- Web Oversight Committee representative
- Data Oversight Committee representative

10) Develop charge / scope of the KCCD IT Governance committee as well as all sub-committees. Consider the following committee charges that would include but is not limited to:

SAMPLE IT GOVERNANCE CHARTER

- Direct and oversee activities of all KCCD IT Governance structure committees
- Review and approve recommendations for policies, standards, and guidelines and communicate these to the user community
- Review, approve and submit requests for budget / funding
- Encourage and facilitate communication amongst all committees
- Ensure communication between all committees and the user community
- Foster clear communication channels for end users to share input

- Appoint Chairs of all sub-set governance committees; review and advise on committee membership to ensure broad KCCD participation
- Provide a coordinated vision for IT to facilitate planning
- Ensure faculty participates in decision making
- Operate efficiently and in a manner that is responsive for the changing needs of the institution
- Establish priorities for institutional activities
- Actively build trust within the KCCD community
- Develop appropriate funding mechanisms to ensure cost sharing is equitable
- Ensure central funds are allocated to priority projects, systems and services
- Review, consider, prioritize and approve /disapprove IT projects

SAMPLE ACADEMIC COMPUTING COMMITTEE CHARTER

- Oversee the maintenance and development of technical resources in direct support of teaching and learning – e.g., Moodle, Athos, classroom technology / room design, distance learning and emerging technologies
- Review and approve updates to existing systems, standards, polices and procedures – e.g., development and delivery of distance education courses
- Serve as an advisor to the Architecture / Infrastructure Committee
- Recommend long-term strategies on distance learning programs, usage and training, hardware and software, as well as fiscal and staff support for technology

SAMPLE ADMINISTRATIVE SYSTEMS COMMITTEE CHARTER

- Develop a business architecture and a master plan for administrative systems – e.g., Banner – and a mechanism to keep the plan current with the involvement of appropriate stakeholders
- Prioritize / sequence needs for the immediate future and updating these needs annually for use in preparing funding requests as part of the budget process

- Establish standards-based architecture for enterprise-wide administrative systems and updating annually
- Recommend long-term strategies on distance learning programs, usage and training, hardware and software, as well as fiscal and staff support for technology

SAMPLE ARCHITECTURE / INFRASTRUCTURE COMMITTEE CHARTER

- Develop and publish standards of interoperation for administrative systems, including database standards, data interchange standards, authentication and authorization protocols
- Perform analysis of administrative systems interrelationships and dependencies
- Identify, define and collect metadata for administrative systems
- Specify architecture / infrastructure for and oversee the implementation of projects – e.g., Identity Management
- Review proposed implementation plans for information systems which have institution wide impact
- Oversee the maintenance and development of desktop computing environment including annual hardware and software replacement standards, policies and procedures.

SAMPLE INFORMATION SECURITY COMMITTEE CHARTER

- Oversee computing security including review, revision and enforcement of the network security and appropriate use policies
- Oversee the desktop computer security in consultation with the Architecture / Infrastructure Committee
- Develop institution wide incident response plan
- Develop and implement institution IT risk plan
- Develop security training and education program for user community

SAMPLE NETWORK COMMITTEE CHARTER

- Review and recommend additions or improvements to the data, wireless, and video communications network
- Recommend standards, policies and guidelines for data and wireless networks

- Establish guidelines for network Service Level Agreement(s)
- Recommend strategic direction – e.g., plan for future growth in the number of users and locations needing to be connected to the network and anticipate changes in technology
- Determine how best to incorporate technology changes / improvements into the KCCD network
- Advise on network security, including security awareness, plans, operations and training

SAMPLE WEB OVERSIGHT COMMITTEE CHARTER

- Review web content including but not limited to coordinating cross-college / district content
- Establish and evaluate models for broad cross-college / district reorganization
- Recommend standards, policies and guidelines for cross-college / district web content
- Improve web services to students, faculty and staff
- Maintain and update web site content
- Serve as an advisor for academic computing projects – e.g., Moodle, Athos, etc.
- Review and incorporate future re-design of web site to accommodate people with disabilities. Refer to Web Accessibility Initiative (WAI) for guidelines

SAMPLE DATA OVERSIGHT COMMITTEE CHARTER

- Develop standards for the storage, retention, and disposal of the institutions data
- Work with data owners, managers and users to continually improve data flow
- Develop and monitor control policies for data
- Provide oversight, prioritization, policy, tools and training to support the institution in managing and protecting its data assets
- Identify, analyze and make recommendations on key functional and technical components of strategy for managing the institutions' data – e.g., data access, privacy, security and use, data sharing, data integration, data warehousing, information architecture, data

quality, data standards and metadata management

- Support select data-driven initiatives, such as Operational Data Store (ODS) / Enterprise Data Warehouse (EDW)
- Recommend the purchase of technology, and the design, funding and prioritization of data-driven initiatives
- Serve as an advisor to the Academic Computing and Information Security Committees
- **REFER TO THE DATA STEWARDSHIP SECTION FOR ADDITIONAL INFORMATION.**

11) Develop a communication strategy to facilitate two-way communication, involving stakeholders in the IT planning and decision making process. **REFER TO THE IT COMMUNICATION PLAN / STRATEGY SECTION FOR ADDITIONAL INFORMATION.**

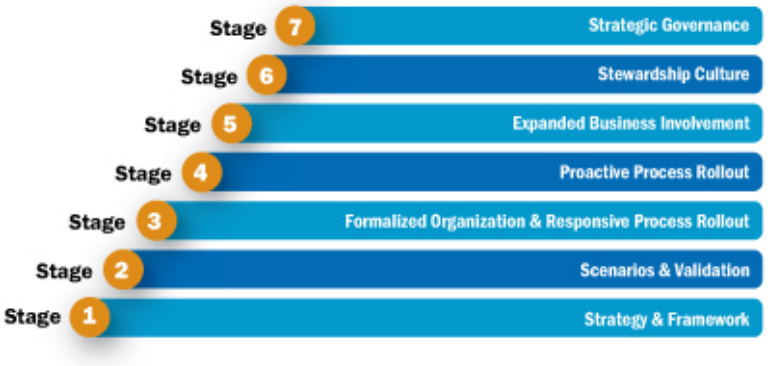
Data Stewardship

Data governance refers to the overall management of the availability, accessibility, quality, consistency, auditability and security of the data employed in an institution. A sound data governance program includes a governing body or council, a defined set of procedures, and a plan to execute those procedures.

Enterprise data governance is a relatively new concept. Many institutions have not yet established the appropriate policies and procedures for data governance, and therefore have not been able to achieve holistic data quality. Technology plays a key role in the data governance process. Its integration into the process, along with assignment of data ownership, can help to ensure that data quality is achieved.

A well defined data governance program defines the growth cycle and associated benefits that can be attained by institutions as they embrace the principles, policies, procedures and standards. The seven layers of maturity, as defined by Martha Dember, include:

FIGURE 1: The Data Governance Maturity Model



REFER TO THE GLOSSARY SECTION FOR A DEFINITION OF EACH STAGE.

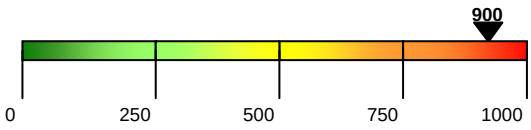
a. Finding(s)

Data integrity was cited as one of the top areas for improvement by the SWOT participants. The establishment and deployment of roles, responsibilities, policies and procedures concerning the acquisition, maintenance, dissemination and disposition of data are not currently in place.

Possible Impact

Data that is inaccurate, out of date and inconsistent is pervasive and costly to an institution. Students, faculty, staff, and suppliers are negatively impacted through poor service, billing errors and inconvenience. Data quality problems are exacerbated in large institutional databases where information is collected from multiple data sources.

Suggested Priority for Resolution



Roadmap

It must be emphasized that a data governance program is not an application that can be purchased, installed, and implemented with a specified end date, but a process that, overtime affects the culture and the way the institution conducts business.

1) Define the owners or custodians of the data assets for the institution.

2) Define processes on how the data is to be stored, archived, backed up, and protected / protected from mishaps, theft, or attack.

3) Develop a policy that specifies who is accountable for various portions or aspects of the data, including its accuracy, accessibility, consistency, completeness and updating. Additionally, consider developing policies such as:

   - Adherence of data to business rules
   - Enforcing authenticity
   - Access rights to data
   - Complying with laws and regulations
   - Protecting data assets
   - Data standards – e.g., specifications and rules for the definition, creation and usage of data within the institution

4) Develop a set of standards and procedures on how the data is to be used by authorized personnel.

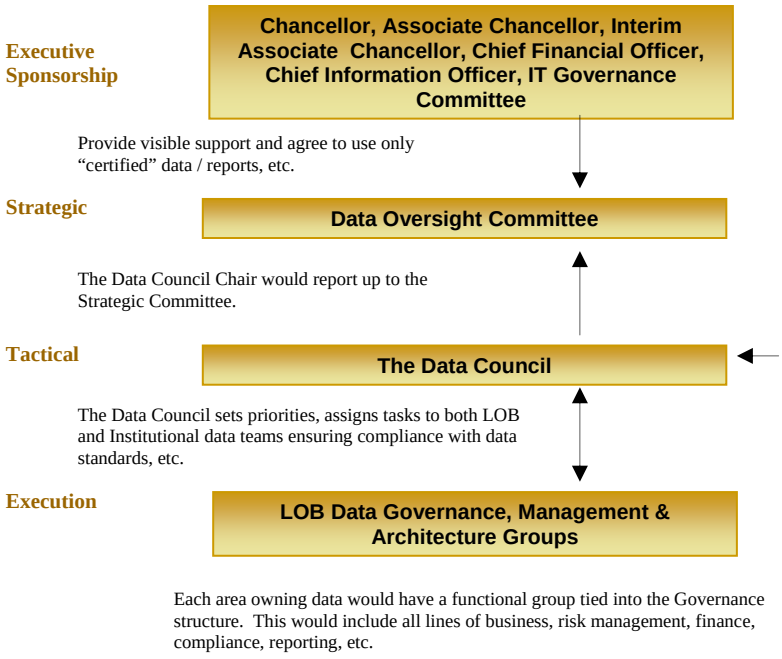
5) Put in place a set of controls and audit procedures to ensure ongoing compliance with government regulations.

6) Implement a data governance program. **REFER TO THE DIAGRAM ABOVE - THE DATA GOVERNANCE MATURITY MODEL.**

7) Establish a Data Oversight Committee that is empowered by executive management, funded, accountable and "closed loop" – e.g., data quality issues are resolved at the source, not just cleansed via the process.

   Since the concept of enterprise data governance is new to many institutions and since key components of data management are not well established, questions abound regarding the structure and responsibilities of the data governance.

   The following diagram is one example of a Data Oversight Committee structure.



Source: B-Eye

8) Segregate activities and responsibilities into three layers – strategic, tactical and execution. For example:

Level	Key Responsibilities
Strategic	• Ratify / modify data management principles • Ensure on-going funding is available • Identify opportunities and issues • Understand costs and benefits • Define priorities • Monitor progress
Tactical	• Execute to priorities of the strategy • Ensure the availability of processes and infrastructure • Focus on coordinating tactical delivery • Leverage existing implementation efforts or initiate separate projects • Manage and report opportunities and issues • Analyze costs – e.g., monitor, track and report on progress against goals and objectives

Level	Key Responsibilities
Execution	• Implement projects as defined by tactical component • Educate developers, end-users, etc. on data standards and the importance of data quality • Audit (sampling and monitoring) of data quality to ensure compliance against standards for both internal and external data • Participate in system-related projects to ensure standards (data model, metadata, etc.) are incorporated in development / enhancement

9) Provide data owners and data stewards with the knowledge, training, tools, forums and processes to be effective in their roles.

Processes of Management

Porterville College

The management of a technology organization requires the effect use of a variety of processes of management such as knowledge, skills, tools, techniques and systems to define, visualize, measure, control, report and improve processes. Processes of management allow an IT department to provide seamless operations and effective implementations to its user's community.

Areas addressed in this section include:

- Change Management
- Project Management
- IT Communication Plan / Strategy
- Policies & Procedures
- Professional Development
- IT Support & Services
  - Incident & Problem Management
  - Performance Metrics
  - Service Level Agreements
  - IT Staff Levels
  - Support Infrastructure
  - Grant Funding
- Cost of IT Operations
- Business Requirements & Critical Processes
- Asset Management
- Asset Replacement Program
- Desktop Software Environment

Change Management

Change management is the process of developing a planned approach to change and coordinating the implementation of all changes (any planned alteration or addition to the operating environment including application software (Banner) systems software, hardware, etc.) into the production environment in a logical and orderly fashion. Change management objectives include but are not limited to the following:

- Minimize the adverse impact of necessary changes on system integrity, security and service level agreements
- Allow the coordination and planning of changes in order to provide a stable production environment
- Maximize the collective efforts of all people involved in the change

Change management can be either reactive, in which case management is responding to changes in the macro environment (external environment), or proactive, in which case management is initiating the change in order to achieve a

desired goal (internal environment). Change management can be conducted on a continuous basis, on a regular schedule, or when deemed necessary on a program-by-program basis.

To be effective, change management should be multi-disciplinary, touching all aspects of the organization, ensuring all changes to configuration items and / or application systems are carried out in a planned and authorized manner. This includes ensuring that there is a business reason behind each change, identifying the specific configuration item and IT services affected by the change, planning the change, testing the change, and having a back out plan should the change result in an unexpected state of the configuration item.

Sarbanes Oxley (SOX), section 404, is also having an impact on change management. SOX's requires any processes that could have an effect on an organization's bottom line be auditable. For IT managers, this means ad-hoc or informal change management procedures are no longer enough. What this means is who did what, to what systems and / or applications, where and when needs to be tracked and documented.

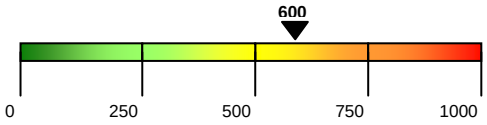
a. Finding(s)

KCCD does not have or follow a comprehensive change management methodology. Records of all changes requested, each level of approval, and functional unit test plans and proof of execution are not tracked.

Possible Impact

The risks of poorly implemented and executed changes range from minor inconveniences to disasters that could cost millions of dollars and directly affect short-term profitability. Often failures are a result of unexpected conflicts in seemingly harmless upgrades, such as installing an operating system or application patch. An unauthorized change to firewall settings can result in serious vulnerabilities that not only threaten institutional data and disrupt revenue-generating services, but can also imperil compliance with regulatory compliance (e.g., HIPAA, Gramm-Leach-Bliley, SOX, etc.).

Suggested Priority for Resolution



Roadmap

1) Define, establish, and implement an IT enterprise-wide formal change management methodology.

2) Develop and implement a standard operating policy and procedure to ensure effective and efficient Change Management / Control measures are utilized within IT. **REFER TO THE ROADMAP NAVIGATIONAL TOOLKIT SECTION – SITE PROPRIETARY IT POLICY & PROCEDURES GUIDE – CHANGE MANAGEMENT FOR AN EXAMPLE.**

3) Develop a Systems / Network Change Request Form and instructions for completing the form. **REFER TO THE ROADMAP NAVIGATIONAL TOOLKIT SECTION – CHANGE REQUEST FORM FOR A SYSTEMS / NETWORK TEMPLATE.**

4) Develop a Software Change Request Form and instructions for completing the form. Suggested categories include, but are not limited to the following:

   - Configuration Item: Software or Documentation
   - Change Type: New Requirement, Requirement Change, Design Change, Other
   - Reason: Legal, Business, Performance Tuning, Defect
   - Change Category: Emergency, Major, Minor or Routine
   - Description
   - Technical Evaluation: Type of software affected, Modules / Screens / Tables / Files affected, Document affected
   - Time Estimates: Analysis / Design, Coding / Testing, Acceptance
   - Impact Analysis
   - Approvals

5) Investigate automating the change management process through the incident / problem management system.

6) Document all changes, whether these changes consist of fixes, enhancements, or major revisions to the operating environment including application software (Banner), systems software, hardware, etc.

7) Define, establish, and implement a communication and notification structure that will support change visibility across all functional work units and the user community. **REFER TO THE IT COMMUNICATION PLAN / STRATEGY SECTION FOR ADDITIONAL INFORMATION.**

8) Hold regular meetings to discuss changes within the environment. Attendees include but are not limited to:

   Bakersfield College
   - Director of Information Services
   - Network Manager
   - IS Technical Coordinator
   - Network Technician
   - Other areas as needed

Cerro Coso Community College
- Dean / Director of Information Technology
- Network Manager
- Other areas as needed

Portersville College
- Dean / Director of Information Technology
- Network Manager
- Other areas as needed

District IT
- Director of Information Technology
- Assistant Director of Information Technology
- Telecommunications Manager
- Systems Manager
- Network Manager
- Security Manager
- Database Administrator Team Leader
- Systems Analyst / Programmer Team Leader
- Help Desk Technician
- Other areas as needed

9) Develop and utilize a *monthly* report for IT Executive Management and / or IT Governance summarizing changes in the environment. Topical areas include:
   - Change category (major, minor, low, emergency)
   - Change requests per status (entered, in review, assigned, completed, rejected)
   - Time spent on tasks
   - Lost time
   - Reason for Change (performance, solve problem, new function, maintenance)

10) Retain change logs / records for a minimum of one year.

Project Management

Information Technology departments within higher education have been rapidly realizing the need for a Project Management Office (PMO). The establishment of a PMO would centralize the tracking of all new and existing IT projects for infrastructure or applications. The PMO is often used as the coordinator of any change management processes. Tasks for the PMO include, but are not limited to, the following:

- Project monitoring and control
- Resource scheduling
- Escalation of issues or jeopardies
- Tracking projects against annual work plan
- Development of budget
- Communication status with the user community
- Establishing project scheduling standards – e.g., MS Project
- Developing project definitions for management's consideration including the outline or risks, mitigation and organization

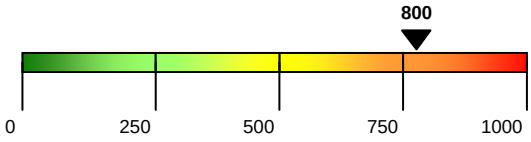
a. Finding(s)

KCCD does not have a methodology or project manager who is coordinating and / or responsible for overseeing both college and district IT projects.

Possible Impact

The lack of a coordinated project management function does not render an accurate forecast of staff needs or accurate timing and forecasting of project completion. Additionally, the lack of a consistent project management methodology can confuse users or at least offer an inconsistent communication standard to the user community.

Suggested Priority for Resolution



Roadmap

1) Consider assigning an individual the part-time function of project management coordinator.

2) Select and use industry best standards as project management templates.

3) Coordinate the establishment of a project management office with the change management function.

4) Identify and provide required training on project management methodologies.

5) Develop and utilize a *monthly* report for IT Executive Management and/or IT Governance summarizing changes to projects. **REFER TO THE ROADMAP NAVIGATIONAL TOOLKIT SECTION – IT ANNUAL WORK PLAN FOR AN EXAMPLE.**

Topical areas include, but are not limited to the following:

- Name of Project
- Brief Description of Project
- Project Start Date
- Project End Date
- Status
- Percent Complete
- Planned Hours
- Actual Hours
- Project Lead

6) Interview user community / stakeholders for all requested projects. **REFER TO THE ROADMAP NAVIGATIONAL TOOLKIT SECTION – IT PROJECT REQUEST FORM FOR AN EXAMPLE.**

7) Ensure all projects are fully investigated, scoped and defined.

8) Solicit input, if needed, from the IT to complete the project request form and scorecard.

9) Weigh and rank each project. **REFER TO THE ROADMAP NAVIGATIONAL TOOLKIT SECTION – IT PROJECT SCORECARD FOR AN EXAMPLE.**

   Categories include, but are not limited to the following:

   - Alignment
   - Posture
   - Planning
   - Implementation Timeframe
   - Risk
   - Funds
   - Investment Costs
   - Capability Gap
   - FTE Requirements

10) Ensure requestor and associated administrator(s) have reviewed the completed project request form and scorecard.

11) Ensure requestor and associated administrator(s) concur that the documents represent the details of the request and the justification for its submission to the IT Governance Committee.

12) Present project requirements and scorecard to the IT Governance committee for review, consideration, prioritization and approval / disapproval.

13) Continue to post project updates to the college and / or district IT web site.

IT Communication Plan / Strategy

IT communication planning is figuring out how to communicate important key messages to key IT stakeholders of the institution in the most effective way possible.

Elements of communication planning include:

- Initiative – e.g., changes in technical environment, decision results, projects, technology demonstrations, success stories
- Objective – e.g., prepare community for changes to the environment, advertise positive/negative results
- Channel – e.g., electronic media (email, intranet, internet), teleconference, print media (memo, bulletin boards, newsletters), face-to-face
- Audience – e.g., students, faculty, staff
- Timing – e.g., as needed, daily, weekly, monthly, quarterly
- Responsibility – e.g., Director of IS / IT, departmental areas

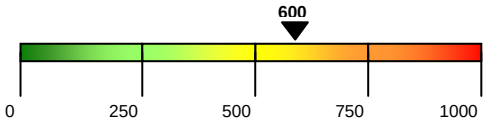
a. Finding(s)

KCCD lacks an IT communication plan that is focused on managing end user expectations for IT services, support and infrastructure and informing the user community of new IT initiatives that are underway. Additionally, horizontal communication channels that facilitate peer-to-peer communication both within and across central and distributed departments are also missing.

Possible Impact

Without effective communication, managing end user expectations for IT services, support and infrastructure becomes difficult or nearly impossible thereby promoting conflict and misunderstandings.

Suggested Priority for Resolution



Roadmap

1) Create and implement an IT communication strategy that builds awareness, support and acceptance of IT within the KCCD community. For example:

Initiative	Objective	Channel	Audience	Timing	Responsibility
Planned Service Interruptions	Make customers aware of downtimes	▪ Web Site ▪ eMail	All All	▪ Post schedule monthly ▪ Day before and day of interruption	Help Desk
Technology misuse	To minimize theft of portable devices	▪ Web site ▪ Article in newsletter	All	▪ September ▪ October	Information Security
Changes in technological environment	Prepare customers for changes in the environment	▪ Web site ▪ eMail ▪ Department visits	All	▪ Post project plan weekly ▪ Two days before change	Project Management Office
Image Review	Review all marketing materials; Check quality	▪ N/A	N/A	▪ Quarterly: March, June, September, December	Information Technology
Technology demonstrations	Setup demonstrations to showcase new technology & uses	▪ Seminar ▪ Brown-bag lunch	All	▪ Bi-annual ▪ Quarterly: March, June, September, December	College IT Departments

2) Develop a mechanism for two-way communication that facilitates stakeholder input and peer-to-peer IT support staff communication within and across departments, colleges and district office. For example:

   - Develop and maintain an IT Governance web site that allows end users to:
     - Obtain information about IT policies, proposed actions, meeting agendas and minutes, IT issues, best practices, case studies, focus group meetings, etc.
     - Obtain hyperlinks to appropriate subcommittees to submit feedback
     - Provide feedback on IT support policies and services – e.g., if end users feel service level agreements have not been met

3) Close the communication loop with end users who submit feedback by acknowledging that their feedback has been received and how it will be processed from IT Governance members and from IT support.

4) Create consolidated communication mechanisms to coordinate messages from college and district IT services and support – e.g., communicate changes to the environment.

5) Link college and district IT websites to the IT Governance website. College and district IT websites should contain the same type of information including but is not limited to:

- *e*Mail and phone links to their department
- Answers to commonly asked IT questions
- Accepts problem tickets from end users
- Allows end users to track their IT issues while they are being resolved
- Links to IT purchasing
- IT training opportunities
- End user and support staff responsibilities in each tier of support as defined by the service level agreement(s)
- IT support performance data relative to service level agreement(s)
- Channel for giving feedback on the quality of their IT support
- Executive Corner
- What's "new" section

6) Consider re-designing web site to accommodate people with disabilities. Refer to Web Accessibility Initiative (WAI) for guidelines.

7) Continue to hold monthly meetings with college and district IT support and staff for ongoing professional development and to share common IT issues. Such meetings would be a forum for collaborating on common IT support issues throughout KCCD and for sharing best practices across the institution.

8) Mine the problem management system (IssueTrak or HelpMaster Pro) for trends, commonly reported problems, overall number of calls, etc.

9) Report problem management statistics, performance against service level agreement(s), end user satisfaction surveys, operating costs and areas of strengths and weaknesses to the IT Governance body to assist the group with the prioritization of IT issues and with policy making for the institution.

Policies & Procedures

A key element of an effective IT program is establishing and implementing appropriate policies, procedures and technical standards to govern over an institution's computing environment. This guidance is key in providing boundaries and controls in the way user's access and manage data within the institution. Establishing and documenting policies is important because they are the primary mechanism by which management communicates its views and requirements; these policies also serve as the basis for adopting specific procedures and technical controls.

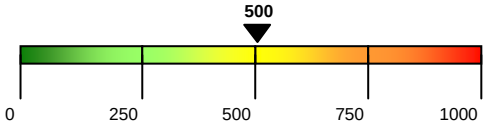
a. Finding(s)

Very little documentation, historical logs, and / or standard operating policies and procedures are maintained and / or updated by college and district IT.

Possible Impact

The lack of comprehensive IT policies, guidelines and procedures eliminates an institutions ability to establish measurable controls and requirements to achieve KCCD objectives. Executive management must set clear, precise policy statements for all aspects of IT. Middle management must have broad guidelines for each policy which offer interpretive boundaries and control for enacting these policies. Detailed procedures for employees to follow are vital to enabling key policies and guidelines to be carried out consistently. Where these procedures are lacking, varieties of interpretation can comprise the intended result.

Suggested Priority for Resolution



Roadmap

Well written policies are difficult and time consuming to create from scratch. Policies that work well and address the unique needs of an institution take time to digest. The optimum, quick start to this process is to either gather or procure best practices available for specific policies within similar higher education institutions. The modification of best practices, which can be tailored to KCCD specific needs, can become a faster development path. If there are limited resources to search for best practices then an external resource, with specific expertise in this area, may be best used for a short period of time.

1) Develop a comprehensive set of IT policies and procedures that establish accountability and responsibility, define expectations for work processes and products, serve as a training tool and ensure correct and consistent service from college and district IT departments. The categories below are listed in priority of importance based upon KCCD's environment. Policies for each of the categories include, but are not limit to, the following:

   - Help Desk
     - Function and Responsibilities
     - Support Level Descriptions
     - Priority Level Classifications
     - Priority 1 & Notification
     - Reporting Requirements

- Problem Tickets
- Problem Escalation
- Response Time Requirements
- Level 1 Response
- Telephone Techniques

- Change Management
  - Change Control Procedures
  - Technical Review
  - Audit Trail

- Asset Classification and Control
  - Accountability for Assets
  - Information Classification
  - Distribution of Sensitive Data

- Access Control
  - Business Requirement for Access Control
  - User Access Management
  - User Responsibilities
  - User Password Management
  - Access Rights and Permissions
  - Modem Access and Use
  - Network Access Control
  - Operating System Access Control
  - Applications Access Control
  - Monitoring Systems Access and Use
  - Mobile Computing

- Project Management
  - Roles and Responsibilities (project manager, team members, executive management, etc.)
  - Project monitoring and control
  - Resource scheduling
  - Escalation of issues or jeopardies
  - Tracking projects against annual work plan
  - Budget development
  - Communication
  - Project scheduling standards

- Communications and Operations Management
  - Operation Procedures and Responsibilities

- Segregation of Duties
- System Planning and Acceptance
- Protection Against Malicious Software
- Information Backup
- Media Handling and Security
- Exchanges of Information and Software
- Data Retention

- Physical and Environmental
  - Access to Secured Locations
  - Equipment Security
  - Fire/Water/Humidity Protection
  - Hardware Power On/Off and Restart
  - Application Start Up and Shut Down
  - Systems Start Up and Shut Down
  - General Controls

- Operating System
  - Installation
  - System Configuration
  - Startup Options
  - Memory Configuration
  - Disk Management
  - Troubleshooting

- Network Infrastructure
  - System Access Control
  - End User Passwords
  - Password System Set-up
  - Logon / Logoff Process
  - System Privileges
  - Establishment of Access Paths
  - Computer Viruses, Worms and Trojan Horses
  - Data and Program Backup
  - Encryption
  - Portable Computers
  - Remote Printing
  - Privacy
  - Handling Network Security Information
  - Physical Security of Computers and Communications

2) Enact and implement policies and procedures.

3) Update and review written procedures regularly, particularly when processes, hardware, software or configurations change.

4) Disseminate policies using various media including the college / district IT Intranet web site, new hire orientations, executive presentations, status reports, department visits, IT Governance, etc.

5) Keep KCCD end user community apprised of changes being made on standard operating policies and procedures specific to escalation procedures, priority levels, etc.

Professional Development

Professional Development is the acquisition of the knowledge, skills and competencies that allow people to keep current with changing technology and practices in their profession. In a very broad sense, professional development may include formal types of vocational training and post-secondary education. Informal programs such as on-the-job training can also be part of professional development, helping staff to develop both process and task skills.

Consistent, quality professional development and learning opportunities represent an investment that helps employees prosper and develop their careers, while simultaneously providing institutions with a highly skilled workforce and a competitive advantage in the market. Benefits of a strong professional development approach include, but are not limited to:

- Improved quality of work
- Increased productivity
- Greater flexibility and responsiveness to change
- Higher staff retention rate
- Improved morale

a. Finding(s)

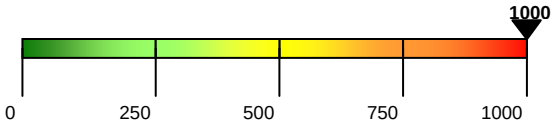
Throughout KCCD many staff talked about the need for “heavy-duty” professional development specific to technology and Banner. Many indicated that they had not received any professional development training – specific to IT or otherwise – in many years. Most felt professional development was defined as a week-long session held in a geographically different location than the college or district.

Possible Impact

When institutions fail to provide ongoing training and professional development for staff, finding competent people to promote or to hire internally for advanced positions becomes increasingly challenging. Additionally, growing gaps between existing skill levels of employees, and the skills actually required to properly and effectively perform the job for which they were hired begin to appear. This type of environment almost

inevitably presents challenges that typically include lower staff morale, decreased work productivity, and increased errors.

Suggested Priority for Resolution



Roadmap

The work effort and / or time required to develop a comprehensive, professional development plan for each employee within the institution will vary greatly and depends upon factors such as, but not limited to, the following:

- Are physical, capital, people and time resources available to gather details about individuals, identify the skills / knowledge required for each job, and conduct a gap analysis
- Have skills and competencies required for each job been determined
- Have skill target levels and importance levels for each job been determined
- What data collection methods (e.g., interviews, surveys, questionnaires, focus groups, observations, existing data, etc.) will be used to survey the population on skill levels and training needs
- Is an inventory of current skills available

1) Create a professional development plan for each employee based on needed areas of knowledge and skills related to their job function and level. These needs are established by referencing relevant strategic goals, competency lists, job descriptions, job analysis, task analysis, as well as the institutions mission. **REFER TO THE ROADMAP NAVIGATIONAL TOOLKIT SECTION – HELP DESK PROFESSIONAL DEVELOPMENT PLAN, MS ACCESS DATABASE SELF ASSESSMENT, AND A BANNER STUDENT ROLE BASED ASSESSMENT FOR AN EXAMPLE OF PLANS, TEMPLATES AND MAPPING.**

2) Identify a training program for all new product releases / upgrades – e.g., Banner, software applications, etc.

3) Work with the Human Resources department to identify an appropriate professional and personal skills training program.

4) Consider undertaking a staffing skills audit / assessment.

5) Explore and continue to offer various blended training media including but not limited to:

- Documentation
- Role Playing
- Learning Lunches
- Apprenticeships
- Conferences
- Seminars / Webinars
- Web casts / Pod casts
- *e*Learning
- Virtual instruction
- *e*Mail
- Live chat
- Knowledge base
- Online tutorials
- Books
- Job aids
- Video / Video teleconferencing
- Forums
- Newsletters / Magazines / Trade Journals
- User Groups
- *i*TV
- Telepresence (videoconferencing)
- Train-the-trainer
- Coaching / Mentoring
- Colleagues / Peers

6) Ensure professional development for staff is included with any technology purchase (hardware and software).

7) Develop a new hire guide specific to each department. For example, the following artifacts would be included in a Help Desk guide.

- Help Desk mission statement
- Organizational charts
- General information about vacation, sick leave, benefits, etc. unique to the Help Desk
- Scheduling guidelines
- Department Contacts
- Location of physical facilities – e.g., server room, telephone room, etc.
- Detailed, step-by-step procedures for tasks performed by the Help Desk
- Detailed review of job responsibilities

- Performance expectations and evaluation methods for routine tasks
- Call procedures
- Primary response times
- First-contact resolution
- Escalation procedures
- List of vendors who provide training
- Policies – e.g., virus protection, KCCD Acceptable Use Policy, PC standards, nonstandard software installations etc.
- 3rd Party Vendor Contracts
- Service Level Agreement

8) Tie training to performance goals and objectives.

9) Define clear expectations and set minimum performance standards.

10) Create and implement a joint database between IT and HR to track the quality and quantity of training opportunities.

11) Review professional development plans annually.

12) Seek grants to provide stipends for technology professional development.

IT Support & Services

A number of factors have combined over the past decade to make delivering quality support to IT users a tough challenge. The number of users and applications continues to expand dramatically; the IT environment is becoming increasingly complex; reliance on IT for business-critical operations is escalating; and budgetary constraints limit the ability to leverage new technologies.

Institutions are continuing to open up their IT systems to more and more people – both inside and outside of the institution. These users include employees, students, vendors, contractors and partners. Moreover, as IT permeates more and more business processes, the number of applications in the IT environment continues to grow, further increasing the burden on the IT staff.

Complicating matters even more is the move to service oriented software architectures. The greater number of interdependencies in this type of architect increases complexity and makes problem resolution more intricate. Additionally, IT services have become increasingly critical to institutions. Service interruptions can translate into a loss in revenue, productivity, and user confidence, jeopardizing the success of the institution.

Incident & Problem Management

Geographically or organizationally distributed support centers often use disparate processes for incident and problem management. Consequently, support quality can vary from center to center, and gaining an enterprise view of performance is virtually impossible. In many institutions users interact with the support staff through multiple channels – e.g., telephone, the Web, email, fax, walk-in, etc. IT management struggles with the need to capture all these interactions and ensure consistency and continuity across channels.

Institutions are tackling these support challenges by implementing incident / problem management products. Incident management focuses on responding to and resolving user issues as quickly as possible, minimizing the adverse impact on business operations and maintaining quality of service. Problem management focuses on correlating incidents to defects in the IT infrastructure and eliminating these defects to reduce the number of incidents.

While incident management is reactive in nature, problem management has both reactive and proactive aspects. The object of incident management is to react swiftly to resolve an incident and restore service as quickly as possible, while providing users with any necessary workarounds to get them up and running. Problem management is reactive in nature when it is in response to an unresolved incident and proactive when it is conducted to improve the overall IT infrastructure and prevent incidents from occurring.

A problem management process is often a result of an unresolved incident or set of incidents – and depends on the historical case, user, change, and asset or configuration item data related to those incidents to help identify root causes – incident and problem management are closely related. Consequently, incident and problem management processes should be tightly integrated. This integration permits the IT support staff to search out problems, associate them with related incidents, and provide valuable information to those responsible for root cause analysis and resolution of the problem.

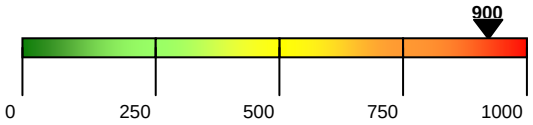
a. Finding(s)

KCCD uses disparate processes and applications for incident and problem management. College and district IT help desks capture and log call information using IssueTrak or HelpMaster Pro. Distance Learning, Interactive TV and Media Services help desks do not appear to capture and/or log call information.

Possible Impact

Disparate data sources, software and resources drive up the cost of providing support and services to the user community. There are also "hidden" support costs – e.g., when someone asks a coworker for help instead of calling the help desk. If the coworker can't solve the problem, another co-worker gets involved, and before long a small crowd has formed. In this case everyone stops doing their job. The cost of this type of support is difficult to measure because neither the help desk nor management is aware problems exist. Gaining an enterprise view of performance is virtually impossible when these types of conditions exist.

Suggested Priority for Resolution



Roadmap

1) Review all incident / problem management applications for effectiveness. Consider what functions KCCD may want to integrate to meet specific needs – e.g., CTI Voice Integration, Knowledge Bases, Remote Diagnostics, Change Management, Forecasting/Scheduling, Performance Analysis, Software Distribution, Customized Reporting, Asset Management, Service Level Agreement(s) etc.

2) Select one incident / problem management application that meets the needs of all help desks within KCCD.

   If the incident / problem management systems do not meet the requirements of KCCD form a project team to define project parameters – e.g., develop a requirements list, organize and prioritize requirements, conduct market analysis, conduct comparative analysis, score candidate products, assign performance scores and the analyze results. The project team should consist of college and district IT Help Desk representatives, Desktop Support / Network Technician representatives, Network Administrator representatives, Distance Learning representatives, Interactive Television representatives, Media Services representatives, Systems Analyst / Programmer representatives, Database Administrator representatives, Telecommunications Manager and User representatives.

   - Develop a business requirement document to include categories such as:

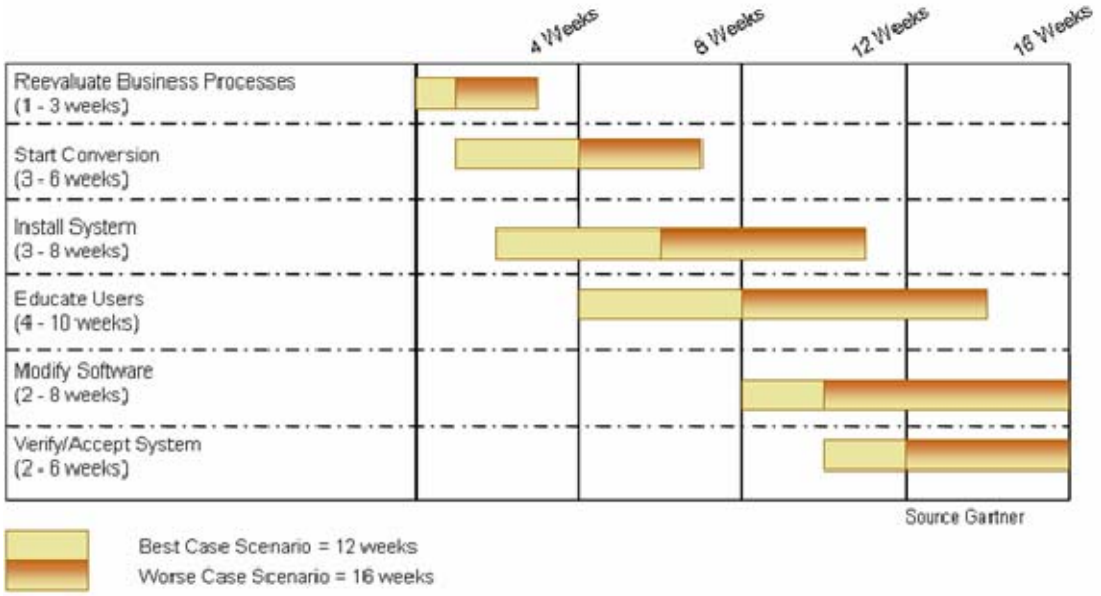
     - Business requirements (detailed requirements, technical requirements, installation / training / set-up and maintenance requirements, project management / reporting requirements, performance criteria for success, and performance penalties)

     - Technical environment (current hardware / software environment, technical architecture)

     - Proposal requirements (contents of proposal, references, key vendor personnel, selection criteria, documents to establish vendor financial stability)

- Evaluate, select and install an incident and problem management system. (Possible incident and problem management software packages to evaluate include Track IT, Heat, Magic, Remedy, etc.). The table below suggests key steps and associated time frames for an incident / problem management system.

Implementation Timeline



- Where possible adopt help desk processes based on the incident / problem management system workflow principles

3) Assign a college or district Database Administrator to maintain and make all changes to the incident / problem management system.

4) Record and track 100% of all calls via the web, phone, email, fax, walk-in, after-hours page, etc.

5) Consider implementing a call category methodology within the incident / problem management tool to include “category, type and item.” These categories should be intuitive and end-user focused.

- Typical top-level “categories” (usually 10 categories or less) are what end users will identify with the most and are most likely to make reference to when describing a problem or asking a question and include areas such as Network Access, Internet Access, Hardware, Software, Printing, Email, etc.

- The second level of categorization is by Item. Items are used to narrow the top-level categories down. For example, under the "Software" category include items such as Banner, Hershey, MS Office Suite (consider breaking category down into Word, Excel, PowerPoint, FrontPage, Access, Publisher, Project), Oracle, Adobe, etc.

- The third level of categorization is by Type. The type consists of "how to," "error messages," "problem", or "order/move/change" categories. For example:

  - How do I log into Banner
  - How do I obtain a Banner account
  - What are my Banner username and/or password
  - My computer has a virus. What do I do
  - How do I change my Banner privileges
  - How do I forward my email to another account
  - How do I connect to the wireless network
  - How do I get an ID/PIN for web access
  - I don't have my Banner User ID, what do I do
  - How do I contact SunGard HE ActionLine for Banner help
  - How do I change my network password
  - How do I setup a mail merge
  - How do I program a macro

6) Learn the Help Desk's arsenal of tools well – e.g., ACD, incident / problem management application (IssueTrak, HelpMaster Pro or other application), service level agreement, standard operating policies and procedures, etc. so that KCCD understands what the full capabilities are for gathering and reporting on help desk data.

7) Annually, revisit the incident / problem management tool for effectiveness.

Performance Metrics

Effective management of distributed computing environments requires the development of a consistent process for defining, tracking and measuring service levels. Well-defined management processes, which define the IT management infrastructure and specify the measurements, are as important as technologies and functional processes to the success of help desks. Unfortunately, many IT organizations are often unable to define consistent, value-added metrics, as it forces them to confront weaknesses and identify gaps in service coverage.

Support metrics provide an IT organization with a baseline for expectation setting and negotiation. With consistent measures, the IT organization can map the impact of new technologies on support, as well as justify tool acquisitions, head-count additions, and budget proposals.

a. Finding(s)

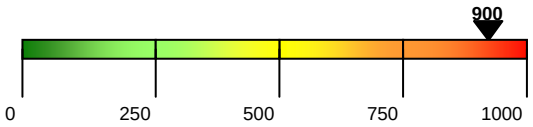
College and district IT help desks are not extracting, monitoring and / or reporting on a daily / monthly / quarterly basis the performance of the help desk.

Possible Impact

The lack of objective, quantifiable performance data increases the likelihood of making decisions based upon unclear criteria or unspecified factors, which may be highly unreliable. Lack of consistent metrics results in a situation where staff and management must act, at times in a vacuum, without key information being easily accessed. This results in decision making on important issues, such as funding projects, staffing, etc. particularly challenging when trying to ensure cost containment or controlling operational risks.

By not reviewing and discussing daily / monthly reports with IT management, the Help Desk cannot ensure tickets are being closed, schedule staff appropriately, or why end-users are calling (root-cause analysis to eliminate why end-users are calling). As a result, the benefits of performance metrics are not available.

Suggested Priority for Resolution



Roadmap

Measuring the service levels, operational performance, quality of support, and technology use is among the top of the reporting needs of management. The tools that are put in place must be able to provide reporting needed to operate the Help Desk, ROI statistics and to support the need for new technologies. Measurement and reporting is the key area that reflects all the other elements.

1) Use existing reports from the incident and problem management system (IssueTrak, HelpMaster Pro and / or home-grown application) to extract data before creating additional reports.

2) Assign a Database Administrator to create additional reports and make all future changes to the system.

3) Develop and utilize a *daily report* that includes the following categories to deal with current issues quickly and effectively. **SEE FIGURE 2 – PROPOSED DAILY OPERATIONAL REPORT.**

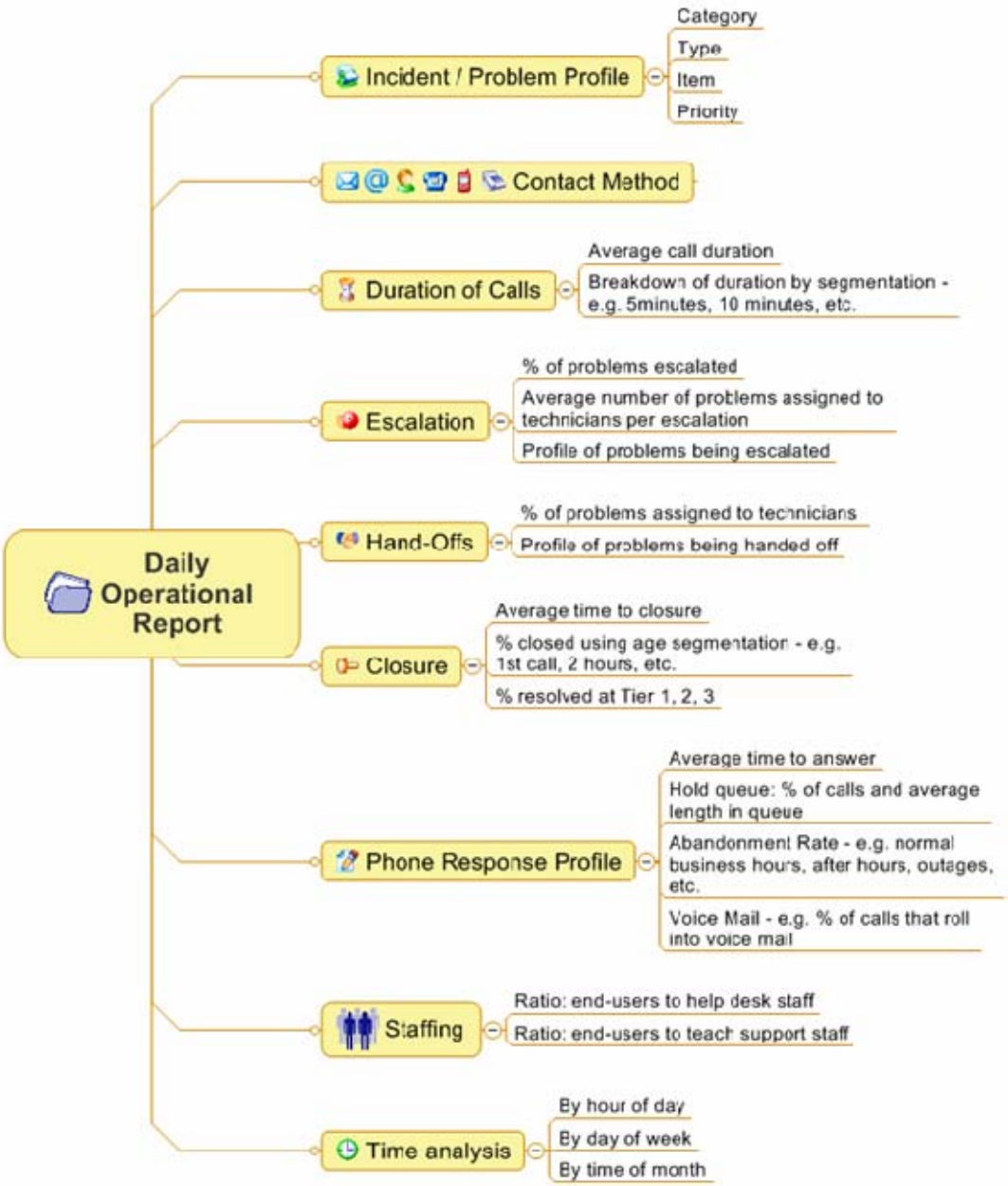


Figure 2 – Proposed Daily Operational Report

4) Develop and utilize a *monthly report* for IT Management summarizing changes in the environment. Possible categories include:

   - Number of Incident / Problem tickets (open, closed, resolved on contact, etc.)
   - Call breakdown by category, type, item
   - Number of workstations supported
   - Daily call distribution
   - Number of calls per workstation (Divide # of calls by # of workstations)
   - Change in Resolution Times
     - Within 1 hour
     - Between 1 and 4 hours
     - Between 4 and 8 hours
     - Over 8 hours

5) Develop and utilize a *quarterly report* for IT Management summarizing help desk call management statistics, performance against service-level agreements, client satisfaction surveys, operating costs, and areas of strengths and weaknesses.

6) Define and arrange monthly college and district IT Management meetings to discuss performance.

Service Level Agreement(s)

The primary objective of the college and district IT departments is to provide computing services that meets the business requirements of the user community. To achieve this, IT needs to understand those requirements and translate them into its own business objectives. Against those objectives IT can measure the service delivered as well as its own capability and performance in providing the services. To enable this to occur, the critical services and level of delivery required must be identified and agreements reached. Typically this is done through Service Level Agreements (SLAs), which are a formal written contract developed jointly by IT, the business unit and/or the institution.

a. Finding(s)

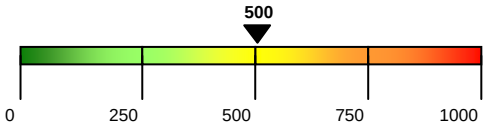
SLA's are not in place for the college and / or district IT / IS departments.

Possible Impact

A lack of understanding from both IT and the user community means goals and objectives are not defined. As a result, the user is dissatisfied with the service and typically looks for support elsewhere (coworkers, vendors, etc.) or escalates the pressure on IT to deliver. Both of these approaches are costly to the institution. When unmanaged decentralization occurs, there is a duplication of services and the benefits of the economics of scale of

centralized management processes are lost. When unmanaged pressure is put on IT, there may be an increase in cost and / or a loss in productivity as hardware and resources are thrown at the problem.

Suggested Priority for Resolution



Roadmap

College and district IT department's credibility is intertwined with quantifiable metrics and therefore should develop a service level agreement that is appropriate for their environment and not based upon industry standards from Gartner, Forrester, Data Monitor, etc.

1) Research current service levels (abandonment rate, average time to fix, customer satisfaction rate, first contact resolution, primary response time, availability of the network, etc.) to understand exactly what IT / IS is actually delivering.

2) Schedule meetings with college and district IT / IS representatives, Desktop Support / Network Technician representatives, Network Administrator representatives, Distance Learning representatives, Interactive Television representatives, Media Services representatives, Systems Analyst / Programmer representatives, Database Administrator representatives, Telecommunications Manager, User representatives and Vendor support to help with the development process.

3) Define and establish a service level agreement that contains both qualitative and quantitative measurements including, but is not limited to, the following:

   - Describe the service to be provided
   - Specify the volume of demand for the service
   - Define the timeliness requirements for the service
   - Specify the availability of the service required (availability is the product of a series of system components, any one of which can affect end-user availability – e.g. network equipment, front-end processors, network control software, workstations, servers, I/O devices, operating system software, operational support software, application programs, individual databases, etc.
   - Define the reliability of the service (reliability has to do with the comparison of actual availability to planned availability

- Quantify the compensation for providing the service (consider adopting a chargeback system)
- Describe the measurement procedures to be used

4) Obtain Executive Management approval.

5) Implement agreed upon service levels.

6) Report and discuss service levels with IT Governance, Infrastructure / Architecture Committee – e.g., DWITC, Information Security Committee, Network Committee, Academic Senate Committee, and Administrative Systems Committee as well as with college and district IT / IS staff.

7) Establish an annual process to review and update the service level agreement.

IT Staff Levels

Many institutions are asking what are the industry standard staffing to desktop / server / database work ratio. In short, there is no simple answer. Technology staffing cannot be determined by numbers of computers, software types, teachers or students alone owed to the unique complexity of each institution. Many other issues can impact how much support is required, and how easy it is to offer that support. Obviously the extent of technology usage in the institution is important. In addition, many less evident variables may mean that an institution needs more (or less) staff to properly manage its technology.

The following factors affect an institutions need for IT staffing.

- Network is centralized or decentralized
- Service level agreements in place
- Skill level of technicians
- How customized the environment is
- How self-sufficient users tend to-be
- The institutions culture and the level of funding for IT
- Geographical size of the district (buildings widely separated)
- The number of campuses / buildings
- Buildings are old and/or badly wired or set up for technology
- Computers are generally more than 2 years old or not of high quality
- Computers are a wide variety of brands, models and types
- Computer software installation is not centralized (all software installation and upgrades must be done at the individual computer)
- Computer maintenance is not centralized (repairs must all be done at the affected computer)

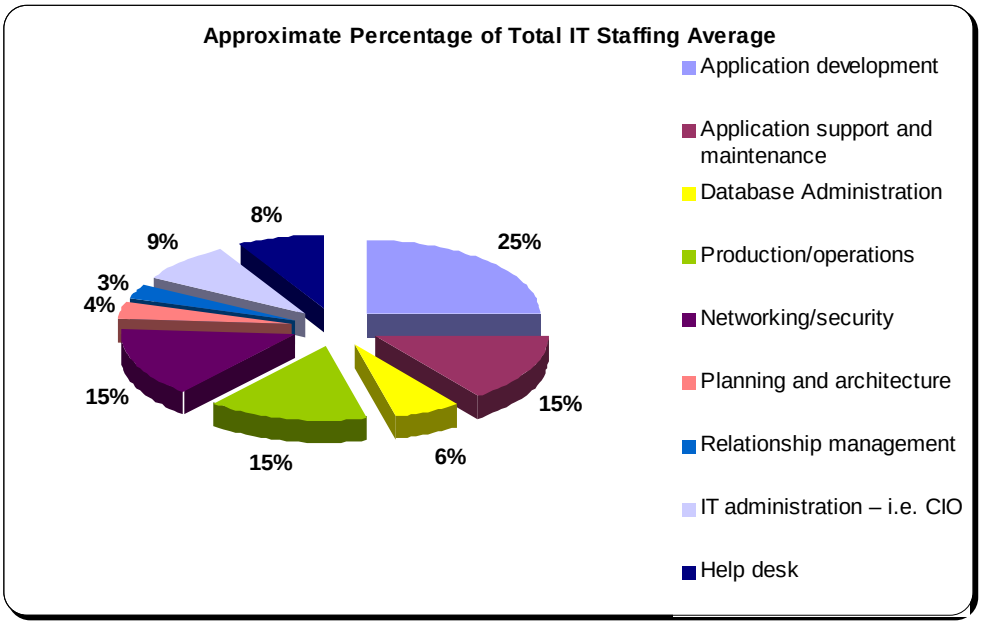
- Significant reliance on technology-based curriculum and / or Distance Learning using technology

Computers and other technologies play a significant role in instruction and administration for many institutions. While it is generally understood that hardware and software will be required to make technology available in institutions, the fact that there will need to be significant parallel expenditures for technical and instructional support is less well accepted. CIO's and IT managers / directors frequently try to find specific numbers, ratios and formulas from business and other venues, that they can use to request and justify additional technology support staff. Though the business world has developed various models for helping determine the appropriate number of staff needed to support technology, in general these models have not been used by institutions.

For purposes of this report the metrics below represent ranges for common IT functions. They are designed to give IT managers an idea of the typical breakdown of IT staff and common workloads.

"Globally and across all industries, as reported by Gartner, the average ratio of IT employees to all employees in the organization is between five and seven per 100 range. This number includes full-time IT staff, contractors, outsourcers and other external service providers. The average ratio of IT manager to staff ranges from 1-to-7 to 1-to-13."

Across all industries, the typical IT organization head count breaks out among the areas shown below.



Source: Gartner

In addition to the above Gartner reports the following:

- Typically, there's one project manager for every five to seven programmers
- One FTE can manage an average of five large database servers or 15 to 20 file and print servers
- To provide reasonable support (including administration, help desk and desktop support) in a PC/LAN environment, the average number of users per IT FTE will range from 26 to 48, with an average of 40
- Typically, one Web server administrator can support between six and 13 servers, with an average of 12
- In managing Windows NT environments, one FTE server administrator should be able to manage approximately 35 servers
- In the UNIX environment, one FTE server administrator should be able to manage approximately 11 servers

a. Finding(s)

The college and district IT departments believe they are inadequately staffed to support the technology needs of the institution. Performance metrics are not captured that would justify and / or validate the perceived need for additional staff.

Specific to the support of existing IT infrastructure and services, it is obvious that the quantities and qualities of IT staff at Cerro Coso College is inadequate to support its existing environment. It is not as obvious a deficiency in the other colleges and district office.

The only inefficiency noted in the current staffing model is the redundancy of staffing for the multiple Level 1 Help Desks throughout the district.

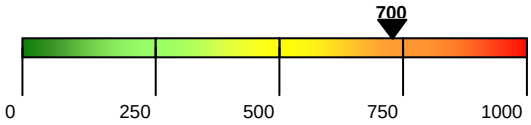
Specific to the support of new IT infrastructure and services, there is no obvious "bench" of the appropriate expertise to address the rapids of technology changes that continue to grow from year-to-year.

Possible Impact

As technology becomes more commonplace and complicated in institutions, decisions on technology support will ultimately have a corresponding impact on the students' learning environment. For example, limiting software to a core set of packages will result in less staff time for software support, which will save in terms of technical support, the tradeoff is that curriculum and instruction, as well as business processes, may be restricted.

The continued need for new technology will press the existing IT staffing levels given the limitations of budget. This is exacerbated by the limited amount of professional development training to keep maintain and improve IT staff skills.

Suggested Priority for Resolution



Roadmap

1) Stabilize IT staffing at Cerro Coso. The permanent IT staff and management at Cerro Coso should be recruited and put into place to effectively support the existing desktop, open lab, distance education, and network technologies.

2) Consolidate disparate help desks. The staffing, operations, equipment and facilities should be consolidated among the current varieties of Level 1 Help Desks within the district.

3) Minimize the addition of staff. Additional staffing and management skill sets are required for emerging technologies. Where possible, efficiencies should be sought in the temporary use of contractors, consultants, part-time staff, etc. In the rare case where the volume of work necessitates the hiring of full-time staff or management, these new positions should be placed at the district level and serve all colleges. The passage of time and escalating use requirements might eventually require each college to have such a position added for dedicated local support.

4) Establish a baseline technology requirement for most, if not all, jobs within the district. For example:

   - Troubleshooting technical problems
   - Providing basic technology information
   - Creating operating and training aids
   - Offering short training workshops
   - Developing technology training curriculums
   - Collaborating with teachers in using technology
   - Providing technical assistance to students

5) Establish benchmarks for the level of support KCCD wants to provide – e.g., Service Level Agreement(s).

6) Record and track 100% of all calls and solutions via the web, phone, email, fax, walk-in, after-hours page, etc. utilizing the incident / problem management application.

7) Utilize one of the following staffing models to assist in calculating the appropriate amount of technology support bearing in mind there is no magic formula.

- **Cost per workstation:** calculate the costs of each workstation over a several year period. There is a tendency to think of technology as a one-time cost, where in reality, the initial capital expenditure is only a small part of the total cost of having technology available

- **Ratio of number of computers to technical staff:** determine number of staff by ratio of technology support staff members to computers – e.g. 1:50, 1:250, etc.

- **Athena Project Formula:** staff members = (number of workstations/500) + (number of users/1000) + (number of clusters sharing servers, printers and other peripherals/15) + (number of applications supported/50) + (number of distinct operating systems and applications/1) + (number of software licenses required/25)

- **Help Desk Formula:** analyze hours available and call volume (time to process and resolve a call = average length of call) based upon problem management categories (data is segregated by type of problem typical in the help desk environment - e.g., hardware, software, printer, Internet and email) to determine optimum staffing levels.

  To determine the number of Direct Labor Hours Available per person reduce the number of theoretical hours available (2080) by the following factors: Holidays, Vacation, Breaks, Training, Projects, Administrative and Sick time.

  Utilization rate reflects that inbound calls arrive randomly, and that a new call rarely arrives at the exact moment an open call is concluded. The level of service required of analysts determines an “appropriate” utilization rate. Eighty percent (80%) and above result in long hold cues, high call-abandon rates and low user satisfaction. Sixty percent (60%) and below indicate an overstaffed operation and an underutilized work force. A good place to start is seventy percent (70%). See the tables below.

Direct Labor Hours Available Per Person						
	Daily	Annualized Daily	Weekly	Annualized Weekly	Annually	Totals
Work Hours Available			40	2080		
KCCD Holidays (in hours)					56	
Vacation (in hours)					80	
Breaks (in hours)	0.5	119				
Sick					40	
Total Work Hours Available						1785
Training (in hours)		0		0	40	
Project (in hours)	1.5	334.69				
Administrative (in hours)		0	2.5	111.56		1298.75
Total Potential Work Hours Available						
Utilization Rate					70%	
Weekly Direct Labor Hours Available						17.48

Source: HelpDesk 2000
*The numbers provided above are hypothetical and subject to change based upon KCCD data.

Weekly Direct Labor Hours Required --- HARDWARE		
Number of Problems/Events per period		76
Average Length of Event (hour) – call processing time (time + work time)	**X**	0.25
Labor Hours Required of 1 period		**19**

Weekly Direct Labor Hours Required --- SOFTWARE		
Number of Problems/Events per period		105
Average Length of Event (hour) – call processing time (time + work time)	X	0.16
Labor Hours Required of 1 period		**16.8**

Weekly Direct Labor Hours Required --- PRINTER		
Number of Problems/Events per period		75
Average Length of Event (hour) – call processing time (time + work time)	X	0.11
Labor Hours Required of 1 period		**8.25**

Weekly Direct Labor Hours Required --- INTERNET		
Number of Problems/Events per period		75
Average Length of Event (hour) – call processing time (time + work time)	X	0.09
Labor Hours Required of 1 period		**6.75**

Weekly Direct Labor Hours Required --- eMAIL		
Number of Problems/Events per period		54
Average Length of Event (hour) – call processing time (time + work time)	X	0.04
Labor Hours Required of 1 period		**2.16**

Source: HelpDesk 2000
*The number of problems/events per period and average length of event numbers provided above are hypothetical and are for discussion purposes only. The sample data / numbers should not be construed as valuable data.

Weekly Gross Staffing Level			
	Hours Required	**Hours Available**	**# of People Required**
Weekly Direct Labor Hours Required --- HARDWARE	19	17.5	1.1
Weekly Direct Labor Hours Required --- SOFTWARE	16.8	17.5	1.0
Weekly Direct Labor Hours Required --- PRINTER	8.25	17.5	0.5
Weekly Direct Labor Hours Required --- INTERNET	6.75	17.5	0.4
Weekly Direct Labor Hours Required --- EMAIL	2.16	17.5	0.1

Weekly Gross Staffing Level			
	Hours Required	**Hours Available**	**# of People Required**
Labor Hours Required per period for all categories	**52.96**		
Direct Labor Hours Available		**17.5**	
Gross Staffing Level			**3**

Source: HelpDesk 2000

8) Infuse technology training at every level of the institution. All employees must understand that professional development in the use and integration of technology is never ending due to technology's evolutionary nature.

9) Build professional development requirements into each contract.

10) Build technology support requirements into each contract.

11) Consider undertaking a staffing needs study for district and classroom information technology. It will help KCCD understand where personnel can best be utilized and what overlap would be acceptable for maximum operation. Such study must include an analysis of time needed to support all of the technology use areas at the colleges and district (not just computer-related use).

Support Structure

A major challenge for IT organizations continues to be creating a support structure that channels problems and requests for service requests to the best resource, while maintaining effective management and user satisfaction. Typically, there are four levels of support including:

- **Level 0 Self-Help (Intranet / Internet Strategy):** Level 0 is an Intranet / Internet self-support function, empowering users to solve problems via universal access to knowledge

- **Level 1 Service Desk (Business Focus):** Level 1 service desk is the front line of support and is the single point of contact for all technology-related problems – e.g., Banner, internal applications to shrink-wrapped software, hardware break/fix, telecommunications, media services, *i*TV, Distance Learning, etc. Level 1 resolves approximately 60 – 80% of all incoming support calls (email, telephone, web, fax, walk-in, voicemail, etc.). Unresolved support calls are passed to Level 2 or 3 staff
- **Level 2 Service Desk (Technical Focus):** Level 2 service desk provides support services beyond Level 1. Level 2 staff is typically involved in end-user training, systems and operations, desktop support, project services, application support software distribution, portfolio / asset tracking, change management, etc. Level 2 resolves approximately 15 – 25% of the total support call volume. Unresolved support calls are passed to Level 3 staff

- **Level 3 Service Desk (Strategic Focus):** Level 3 service desk provides support services beyond Level 2. Level 3 staff is typically involved with hardware / software vendors to resolve issues, handle a wide variety of issues concerning all aspects of the desktop and the network, are focused more on strategic planning and IT infrastructure, disaster recovery planning, capacity management, etc. Level 3 staff resolves the remaining 5 – 10% of support calls

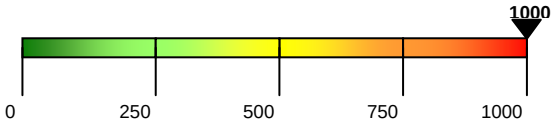
a. Finding(s)

The KCCD user community expects transparent, responsive, quality support for all IT services. The current IT support structure has been in place for some time. During that same time the rapids of technological change have advanced with limited adoption within all colleges in the district. During this same time of growing demand for IT services, the supply of budget has become strained.

Possible Impact

Maintaining the status quo of staffing quantities, skill sets and design will further erode both the colleges and the district's adoption and support of new technologies as compared to the expectations of new students every year. Unless there is a dramatic change in budget availability then the current staffing model will be hard pressed to support new technologies let alone the existing infrastructure.

Suggested Priority for Resolution



Roadmap

1) Establish a Level 0 Self-Help structure for all IT users in the district.

2) Centralize the seven Level 1 Service Desks that exist within KCCD to reduce costs, improve operations, and begin the retention of IT knowledge. **SEE FIGURE 3 – PROPOSED DISTRIBUTED IT SUPPORT STRUCTURE.**

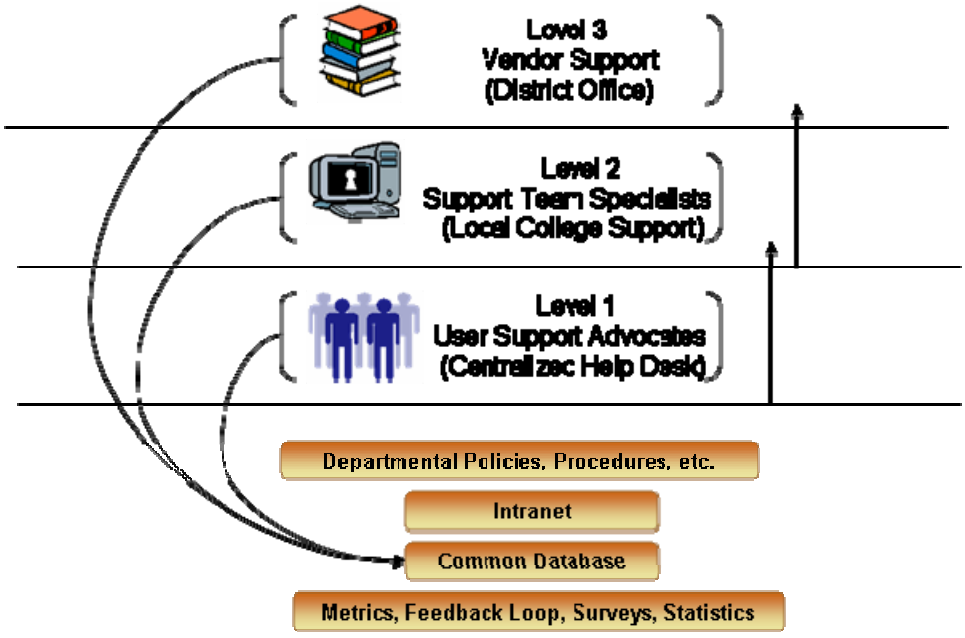


Figure 3 – Proposed Distributed IT Support Structure

3) Maintain and expand the distributed Level 2 and 3 Service Desks for break-fix desktop and network support at the three colleges.

4) Introduce a hybrid model of technology specialization to address the rapids of change in IT. Rather than create the duplication of rare staff skills in the presently missing technologies, it would be better to hire one to support that technology in the entire district. This individual can cross-train other support staff on the new technologies. This hybrid model

should be added to centralized reporting and active support to the colleges.

5) Designate a single point of contact for all technology-related support calls – e.g., Banner, internal applications to shrink-wrapped software, hardware break/fix, telecommunications, media services, *i*TV, Distance Learning, etc.

6) Define clear roles and responsibilities for the centralized, Level 1 help desk. For example:

- Log and track all calls and problems, and work orders / service requests received in the incident / problem management system
- Monitor, control and manage each ticket until it is resolved
- Document resolutions in the incident / problem management system
- Escalate confirmed and unresolved problems according to established procedures
- Coordinate 2nd and 3rd level support
- Provide monthly reports to IT management.
- Create and maintain operational documentation, processes and procedures
- Maintain communications with Level 2 and 3 IT support staff

7) Define clear roles and responsibilities for distributed, Level 2 support. For example:

- Document resolutions in the incident / problem management system
- Install, configure, upgrade, and maintain software applications on faculty and administration workstations and peripherals
- Install and configure new devices such as printers and modems with desired operating system and applications
- Setup account administration
- Re-image classroom machines weekly
- Diagnose desktop computer software, hardware, network and system problems
- Resolve desktop computer hardware/software problems
- Work with Level 3 staff to identify problems in their areas
- Create and maintain operational documentation, processes and procedures
- Identify and resolve systems oriented problems and document resolution in the incident / problem management system

- Provide support, when necessary, for the local area network and Internet connectivity
- Propose LAN changes, upgrades or tuning adjustments as necessary
- Coordinate with Level 3 to assist in or implement recommended changes, including onsite visits as necessary
- Maintain communications with Level 1 and 3 IT support staff

8) Define clear roles and responsibilities for hybrid, Level 3 support. For example:
   - Perform WAN / LAN network troubleshooting to isolate and diagnose common network problems
   - Upgrade network hardware and software components as required
   - Install, upgrade and configure network printing, directory structures, rights, security, software and file services
   - Manage enterprise email and calendar services and related spam filtering
   - Manage institution wide authentication and virus protection system
   - Maintain server room including security updates, end of life server upgrades, rack and cable plant management, and general condition of the room
   - Provide users with network technical support
   - Respond to needs and questions of users concerning their access of network resources
   - Establish network users, user environments, directories, and security for networks being installed
   - Install and test necessary software and hardware
   - Maintain communications with Level 1 and 2 IT support staff
9) Standardize on one incident / problem management application for recording and tracking all technology-related support calls.
10) Develop a central “User Support Center” website. **REFER TO THE COMMUNICATION PLAN / STRATEGY SECTION FOR ADDITIONAL INFORMATION.**

Grant Funding

Non-profit organizations have long enjoyed access to grant funding from a variety of government, corporations, foundations and private sources. Several areas have increased the availability of grants in recent years including security issues that can be addressed by new grants from the federal government. Properly used this can be a solid component of new funds for an institution.

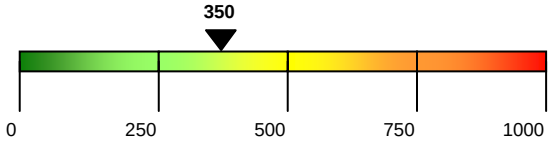
a. Finding(s)

There is no coordinated, system wide grant function within KCCD. Among the three colleges only Porterville has a part-time grant function specific to medical programs. Despite this there have been several independent initiatives throughout the colleges and district in bidding on and awarded grants over the years that require additional IT resources specific to staff, hardware and software.

Possible Impact

The technical currency of grant provided software and hardware is typically off the radar of IT management and support staff. www.grant.gov has become the de-facto application process for most available grants. The intensity of this process has been widely criticized as to rigorous and exhaustive and therefore is a disadvantage to smaller institutions. As such, much of the future grant money available will be awarded to larger schools that have coordinated processes and dedicated personnel to the writing of grants.

Suggested Priority for Resolution



Roadmap

1) Fund and hire / contract a full-time grant writing coordinator for the district.

2) Work with Academic Senate, DWITC, college IT committees and academic disciplines to determine appropriate grants that should be pursued.

3) Assure that relevant staffing, expenses, equipment and facilities required by the grants fit the programming and budget requirements of the institution.

Cost of IT Operations

Effect of IT operations have costs in many different budget categories in including facilities, capital equipment, recurring operating expenses, and staffing. Typical to most services within higher education, the cost of staffing becomes the predominant budget expense.

a. Finding(s)

There are no quantitative performance metrics collected that would offer a predictive model on IT staffing requirements for the colleges. Industry best practices typically use call volume examinations from the help desk as metrics to model staffing in the support of existing IT operations. Where help desk call volume has been recorded within the district, the volume is insignificant as compared to what should be recorded for an institution of the size and complexity.

There are efficiencies in a number of areas of recurring operational expense. These include the low-cost WAN infrastructure which uses the county's microwave, the pooling of software licenses at the college level, and the common use of an administrative system throughout the district.

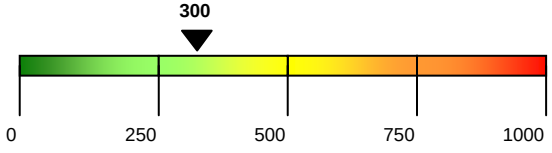
There is an impressive and reasonably modern collection of IT capital equipment used throughout the district. This includes servers, network components, network infrastructure, videoconferencing equipment and equipment supporting interactive television as well as online distance education. Owed to limited funding and in recent years there has been limited planning or replacement of capital equipment. The lack of comprehensive inventory on the state of, and the age of, the desktop computing environment is exacerbating the ability to effectively plan its replacement.

There is adequate and reasonable use of facilities for network operating centers as well as the district data center.

Possible Impact

IT staffing is typically the key focus of cost examination with an IT operations. There is always a sought-after, optimal balance between service expectations and the cost of additional staff. Operating expenses necessary to support existing capital equipment, facilities, and staffing typically have limited flexibility. Capital equipment replacement is most often ignored of all budget categories for IT operations.

Suggested Priority for Resolution



Roadmap

1) To avoid qualitative, anecdotal, or subjective decisions in IT staffing it is imperative to track key performance metrics along with client satisfaction. The consolidation and improvement in help desk operations will begin to provide these vital metrics. The additional use of client satisfaction surveys should provide metrics where support is not adequate and may need additional staff.

2) A full and detailed inventory of IT capital equipment throughout the district will provide the necessary planning data for a replacement plan and budget.

3) There are a number of alternative strategies for keeping the desktop environment current for student, faculty and staff use of modern operating systems and applications software. These should be investigated with a decision that will allow accurate budget forecasting for replacements.

Business Requirements & Critical Processes

The automation of business requirements represents a critical area where IT can help to improve the institution's delivery of mission-critical services. Unlike the implementation, support, and use of other IT infrastructure this area requires a high degree of effective IT consultation combined with active user involvement. The search for, and application of, best practices becomes a critical component to the successful optimization of any business process.

a. Finding(s)

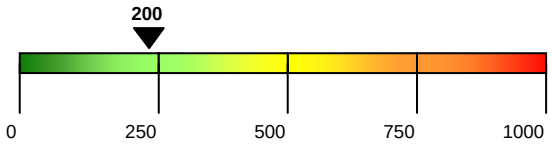
There are current efforts underway with the Banner finance and human resource systems used within the district to use them to improve business processes. The various steering committees for these functions have been assisting the navigation of this process. Key individuals from these functions have also been providing effective leadership to move these processes forward.

Specific to other business functions such as bookstore, counseling, maintenance and operations, library, etc. there are few cases where best practices are actively discussed or shared among similar departments between the colleges. One notable exception is the student services function. In very few cases were best practices investigated or sought from other similar institutions.

Possible Impact

Many automation processes fall short of optimum improvements as management and users seek to duplicate the existing processes without considering possible improvements. Lacking an active search for best practices within the institution, and at other similar institutions, prevents the maximized attainment of improved services. The result becomes a gap between incoming student's perceptions of expected services and automation and the institutions ability to deliver state-of-the-art services.

Suggested Priority for Resolution



Roadmap

1) Professional development training should be identified and obtained for similar business functions within the colleges. The focus of this training should be on seeking best practices and redefining business processes for optimum efficiencies and improved services.

2) Common business functions among the three colleges should meet on a regular basis to share and adopt best practices discovered internally and externally.

Asset Management

Because Non-Profit Organizations (NPO's) have no tax obligations they have little reason to track all capital equipment purchases and to place them on a depreciation schedule. Some NPO's will use formal asset management if they seek to depreciate over estimated economic lives so they have a more accurate budget forecast of replacement costs.

Most NPO's, including institutions of higher education, have suffered budget set-backs over recent years that quickly eliminated any asset replacement programs. When applied to IT assets, the resulting problem is a "surprise" total cost of hardware upgrade or replacement costs when new operating systems or application software demand faster platforms for their new functionality.

Asset management is a high-level process that integrates people, processes, and technologies to maximize end-user productivity, contain costs, and maintain compliance. A successful asset management program helps organizations maintain existing assets and budget new assets, cross-references financial and contractual documents, and is a decision-making tool that can have an impact on an organization in terms of time and money.

Benefits of implementing an asset management system include, but are not limited to the following:

- Improved accountability
- Reduced risks and exposures by effectively tracking service-level agreements, warranty and maintenance information, contract end dates and entitlements
- Improved efficiencies, by allocating assets most effectively and without duplication when all assets are known and managed

- Increased security with regular tracking and monitoring
- Maximized ROI by knowing where capital has been invested in assets
- Improved financial results, saving money by not purchasing or maintaining unnecessary assets, and reducing equipment and IT costs through predictive maintenance
- Improved reporting on vendor performance during the life cycle of the asset and contract, which is useful for contract negotiations and supplier management

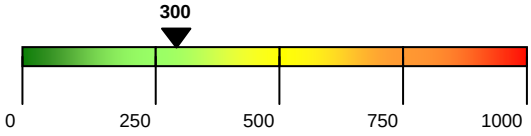
a. Finding(s)

Equipment with a value in excess of $5,000 is recorded in the district's equipment inventory system. Non-capital assets are not recorded. Bakersfield utilizes a home-grown system to record computer assets (Computer ID and Asset Tag). Cerro Coso records computer assets in the problem management system IssueTrak. It is unclear if or how Porterville records computer assets. An annual physical inventory is not conducted by the college or district IT departments and cross-referenced with the institution's equipment inventory system.

Possible Impact

Non-profit organizations, such as higher education, have no tax or financial reason to track small assets such as desktops, laptops, printers, etc. The lack of this inventory makes planning for software and hardware upgrades a highly reactive event and prevents metrics from being tracked which help to substantiate support staff ratios.

Suggested Priority for Resolution



Roadmap

1) Ensure asset management planning reflects a life-cycle approach. Limiting asset planning to a single phase will not lead to sound long-term decision about assets. **SEE FIGURE 4 – ASSET LIFE CYCLE.**

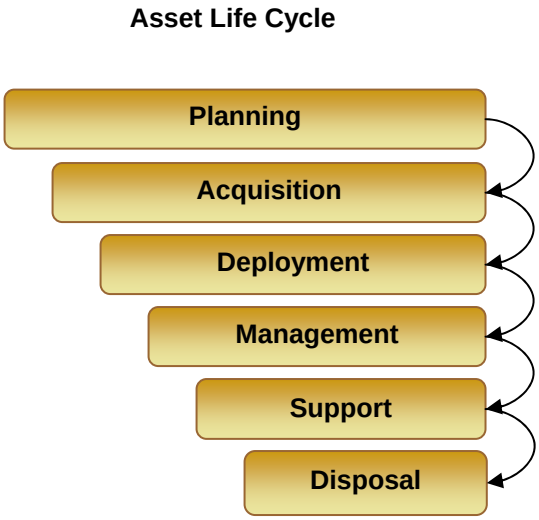


Figure 4 – Asset Life Cycle

2) Establish standard life cycles for IT equipment. **REFER TO THE ASSET REPLACEMENT PROGRAM SECTION FOR ADDITIONAL INFORMATION.**

3) Tag all IT related assets (capital and non-capital) prior to deployment.

4) Establish procedures to issue and inventory IT related assets (capital and non-capital).

5) Maintain an inventory of all IT related assets – e.g., desktop computers, laptops, cell phones, PDAs, software, etc. assigned to employees and contractors. The inventory report should be available for auditing purposes.

6) Collect and track all IT-related assets. Inventory attributes include but are not limited to asset type, physical and financial characteristics. **SEE FIGURE 5 – PROPOSED KCCD IT ASSET MANAGEMENT REPOSITORY.**

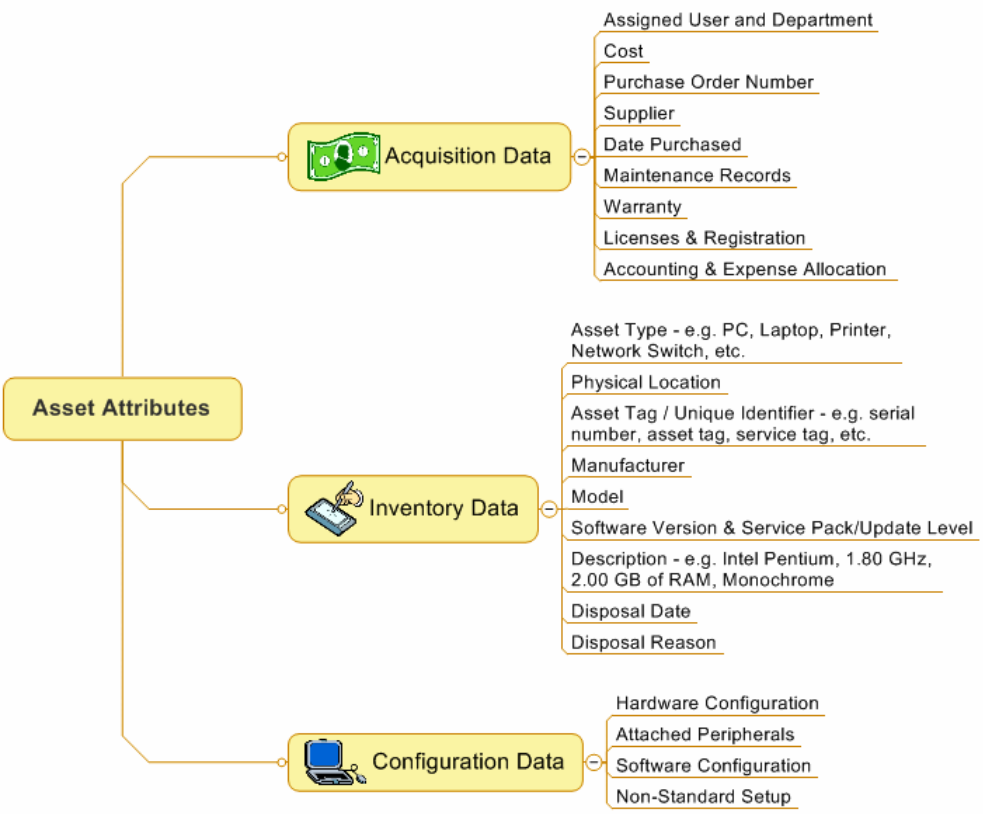


Figure 5 – Proposed KCCD IT Asset Management Repository

7) Conduct a physical inventory to reconcile IT asset inventory information on-hand for all capital assets with the institution's equipment inventory system at least annually. Investigate all discrepancies.

8) Ensure appropriate software licensing agreements for software used by department employees are in place and that the department is in compliance with those agreements.
9) Review, consolidate, analyze, and publish regular reports on IT assets.

10) Integrate IT asset management with Business Continuity Planning.

11) Consider investing in asset management tools (repository, auto discovery and software usage monitoring). Integrate the use of these tools with other strategic systems like HR, accounts payable/receivable, general ledger, purchasing, network and systems management, problem management system (e.g., IssueTrak, HelpMaster Pro, and change management. The integration provides a linkage of metrics between asset management and other processes.

12) Consider developing a district-wide strategic asset management plan that includes:

- An acquisition plan which defines the assets to be acquired or replaced in the planning period, and which establishes the sources and cost of funding acquisitions
- An operational plan which defines the use of existing assets and may include matters such as access, security, accountability and monitoring performance
- A maintenance plan defining which assets are to be maintained, the level of maintenance and the delivery of maintenance services
- A disposal plan identifying assets to be disposed of in the planning period, the expected proceeds on disposal and the application of the proceeds
- A funding plan which defines the options available for funding capital and recurrent asset costs
- A risk management plan which describes the risk management strategies and actions to be implemented for controlled assets

Asset Replacement Program

Desktop computers are now everyday tools for many faculty, staff and students. Historically, these purchases have been treated as large capital acquisitions, where institutions expect to see value from the purchase over time. The rate of technology change, however, has led to desktops becoming functionally obsolete after an increasingly short period. Investment in this type of technology is no longer a one-time expense; it is an ongoing operational expense that must be incorporated into yearly budget planning for colleges and universities.

Additionally, network infrastructure and design, high-end server performance as well as other related technologies have become virtually inseparable. The high rate of evolutionary change in server technology, the growing complexity of newer network topologies and operating systems, the advent of wireless and hand-held communication devices and the integration of voice, data (data streaming), video, et al have relegated today's network infrastructure to all but a brief life span. Moreover, the substantial resource requirements (disc, memory, processor power, etc.) of today's desktop software and enterprise applications, makes the useable functional lives of servers and network design even further interrelated.

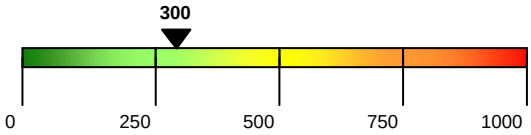
a. Finding(s)

KCCD relies on capital bond money to continually upgrade the network infrastructure as well as data center systems. There is no plan in place for the replacement of older desktops and laptops with new systems and / or for regular updates to desktop software. Both the District Office and Bakersfield College are in the process of testing several different tools to automate software deployment.

Possible Impact
Continued use of outdated equipment increases operating / support costs and potentially exposes the institution to unnecessary security risks. The following security issues support shorter replacement cycles for equipment:

- Outdated hardware systems are vulnerable to attacks at sign-on
- Older systems don't have adequate locking and password functions
- Security fixes and vulnerability patches are often no longer available for older systems
- Older operating systems often don't contain the necessary tools to identify and remedy system compromises
- The overall security risk for older systems is increased due to a lack of available technical support and defensive measures
- The more variations of different operating systems and application versions that the IT organization must support, the more complex and expensive that support becomes

Suggested Priority for Resolution



Roadmap
The current industry standard for a desktop replacement is 4 to 5 years. The primary user for whom the extended cycle is best suited is the standard mainstream.

The replacement cycle for laptops remains within the range of 2 to 3 years. Usage dynamics such as the mobility of laptops reduce their durability. Most hardware vendors commit to 4 years of parts availability for servers; therefore, 4 years is the reasonable upper limit for the life of a deployed server.

Software life cycle is predicated on the type of software and the hardware platform being used – e.g., hardware equipment changes, operating system changes, user needs, manufacture updating and terminating support for older versions.

1) Develop and establish an effective asset replacement policy that includes desktop / laptop computers, printers, telephone system, network infrastructure, wireless communication, servers, administrative hardware (Banner), classroom projection systems, portable classroom projection systems, digital cameras, handheld devices, computer labs, software, video network, grant-funded projects, etc. Caution should be given not to simply adopt the industry standard. Each college should evaluate its resources and plan for a replacement cycle that supports KCCD goals. The replacement cycle establishment process will quantify ways in which information resources can be managed cost-effectively, while still remaining responsive to the needs of the students, faculty and staff.

   The following decision points can assist KCCD in developing a replacement policy.

Step 1: Identify Management Principles

To begin the asset replacement life cycle process, KCCD may want to identify a few basic principles that define the role of IT in this process, establish a framework to evaluate the results of the effort, and consider the overall importance of technology to delivering services to students, faculty, and staff.

- Define and obtain executive support for technology management
- Define expected results from establishing a replacement cycle
- Identify benefits to justify costs
- Prioritize the effort in light of overall mission, goals and strategies

Step 2: Evaluate the Institution's Needs

An understanding of the end-user needs and support staff resources will directly impact the life cycle. A life cycle requires knowing how to gauge whether or not technology is meeting existing needs within current budgetary constraints. This requires an assessment of whether or not current computing resources meet the defined productivity requirements of the institution, college, division, department, computer lab(s) and / or workgroup under examination. For example, imagine that a newer PC performs certain processing tasks faster and more

efficiently than those currently used by a specific department. Also, assume that adopting this new technology would dramatically reduce the time that personnel currently spend on tasks using the current equipment. In this scenario, a PC might be replaced simply because the economic benefits gained through staff time and cost savings outweigh the expense of replacing the existing equipment.

- Assess current processes for technology support and maintenance
- Assess the availability of technology support staff
- Assess the needs of end users

Step 3: Evaluate Technology Factors

When all of the necessary preparation is complete, the next step is to look at the technology available on the market, understand how product cycles and technology change produce new equipment on a constant and frequent basis, and assess strategies for obtaining and deploying the equipment.

- Understand the rate of technology change
- Assess strategies and technology to provide adequate technology resources
- Incorporate training into the life cycle

2) Determine the reasonable point around which Total Cost of Ownership (TCO), performance obsolescence, warranty expirations, parts viability, market technical support, budget criteria and future reliability converge to favor equipment replacement.
The following tables below compare costs of exercising different desktop life cycles are only an example. This is not intended to suggest IT's support of a 3-year life cycle. Rather, it is provided solely as an example and may be helpful to KCCD in determining a refresh cycle.

3 Year Desktop Replacement Cycle

(Assumption: $750 desktop + $250 monitor + $40 shipping + 6% tax = $1,100)

3-Year Desktop w/ Monitor	Estimated Time	Estimated $ / Hour	Cost	Depreciated Cost
PC Procurement Administration	1.88	$65	$122.50	$40.73
PC Purchase	NA	NA	$1,100.00	$367.33
PC Install	0.56	$65	$36.40	$12.13
PC Upgrade Labor	0	$65	$0	$0
PC Upgrade Hardware	NA	NA	NA	NA
PC HW Break/Fix Labor	.56	$65	$36.40	$12.13
PC HW Break/Fix Replacement Parts	NA	NA	$150.00	$50.00
PC Software Support – e.g., drivers	1.5	$65	$97.50	$32.50
PC Disposal	.05	$65	$32.50	$10.83
Annual Hard Cost / PC	**-**	**-**	**-**	**$525.65**
Lost End User Productivity (Soft Costs)	12.5	$65	$812.50 (1 year)	$812.50
Total Soft and Hard Costs	**-**	**-**	**-**	**$1338.15**

Source: MetaGroup

4 Year Desktop Replacement Cycle

(Assumption: $750 desktop + $250 monitor + $40 shipping + 6% tax = $1,100)

4-Year Desktop w/ Monitor	Estimated Time	Estimated $ / Hour	Cost	Depreciated Cost
PC Procurement Administration	2.38	$65	$154.70	$38.68
PC Purchase	NA	NA	$1,100.00	$275.00
PC Install	0.56	$65	$36.40	$9.10
PC Upgrade Labor	0.375	$65	$24.38	$6.09
PC Upgrade Hardware	0	0	$150.00	$37.50
PC HW Break/Fix Labor	.56	$65	$42.90	$10.73
PC HW Break/Fix Replacement Parts	NA	NA	$180.00	$45.00
PC Software Support – e.g., drivers	3.33	$65	$216.45	$54.11
PC Disposal	.05	$65	$32.50	$8.13
Annual Hard Cost / PC	-	-	-	**$484.34**
Lost End User Productivity (Soft Costs)	18.5	$65	$1,202.50 (1 year)	$1,202.50
Total Soft and Hard Costs	-	-	-	**$1,686.84**

Source: MetaGroup

Financial Considerations

The following table provides cost comparisons between a 3-year and 4-year Desktop replacement cycle. This is an example of potential expenses related to Desktop replacement cycles. Estimates are for descriptive purposes only and do not reflect actual KCCD number of desktops or expenditures.

		3 Year Cycle	4 Year Cycle
Number of Desktops to Replace	5000	1667	1250
Cost of Desktop Replacement	$1,100	$1,833,700	$1,375,000
Potential Additional Costs	-	-	-
Additional Warranty	$100	-	$125,000
Additional OS Upgrade	$291	-	$363,750
Additional Parts / Labor	$400	-	$187,500
Total		$1,833,700	$2,051,250

3) Incorporate the needs of end users into the replacement cycle. Classify users into one of two categories – Leading Edge or Standard. **REFER TO THE GLOSSARY FOR DEFINITION OF TERMS.** The replacement schedule would vary based upon the classification of the technology user. For example:

   - Leading Edge Technology Users
     - Should maintain no more than two generations of technology
     - Should consider replacing desktops every second or third year, depending on applications in use
   - Standard Technology Users
     - Should maintain no more than two generations of technology
     - Should consider replacing desktops every four to five years, depending on applications in use

4) Establish a standard set of desktops / laptops for Leading Edge and Standard Technology users.

Desktop Software Environment

Windows Vista™ is the new operating system being released in 2007 by Microsoft. According to Microsoft, Windows Vista introduces powerful new technologies that will "help people do their best work". It's promoted to be a major upgrade with significant user functionality and benefits such as enhanced desktop search capabilities, easy navigational interfaces, increased collaboration tools for the mobile work force, greater security and compliance, and ease of implementation. 2007 Office is the most recent version of Microsoft's productivity suite. Formerly known as Office 12 in the initial stages of its beta cycle, it was released to consumers in January 2007. Office contains a number of new features, the most notable of which is the entirely new graphical user interface called the "Ribbon," replacing the menus and toolbars that have been the cornerstone of Office since its inception. Microsoft offers a variety of suites (8 to be exact) to address a diverse range of needs. See table below.

	Microsoft Office Basic 2007	Microsoft Office Home & Student 2007	Microsoft Office Standard 2007	Microsoft Office Small Business 2007	Microsoft Office Professional 2007	Microsoft Office Ultimate 2007 *NEW!*	Microsoft Office Professional Plus 2007	Microsoft Office Enterprise 2007 *NEW!*
Microsoft Office Word 2007	●	●	●	●	●	●	●	●
Microsoft Office Excel 2007	●	●	●	●	●	●	●	●
Microsoft Office PowerPoint 2007		●	●	●	●	●	●	●
Microsoft Office Outlook 2007	●		●				●	●
Microsoft Office Outlook 2007 with Business Contact Manager[1]				●	●	●		
Microsoft Office Accounting Express 2007[2]				●	●	●		
Microsoft Office Publisher 2007				●	●	●	●	●
Microsoft Office Access 2007					●	●	●	●
Microsoft Office InfoPath 2007						●	●	●
Microsoft Office Groove 2007						●		●
Microsoft Office OneNote 2007		●				●		●
Microsoft Office Communicator 2007[3]							●	●
Integrated Enterprise Content Management						●	●	●
Integrated Electronic Forms						●	●	●
Advanced Information Rights Management and Policy Capabilities						●	●	●

Source: Microsoft

Studies indicate any desktop / laptop more than two years old will not be able to run Vista; therefore, IT professionals need to plan ahead to make sure all the desktops / laptops within their organization have the basic system requirements and hardware provisions to transition smoothly. If not, it will slow down adoption, increase overall migration costs and possibly cause downtime for users. Hardware requirements include:

	BASIC (No Aero)	BETTER (Aero Experience)	BEST (Optimized Experience)
System Memory	512MB RAM	1GB RAM	2GB Dual Channel (2 DIMMS)
Graphics Memory	Integrated or discrete DirectX9 capable graphics card CD-ROM Drive	128 MB Graphics Card (integrated or discrete) Support for DirectX9 graphics with a WDDM driver Pixel Shader 2.0 and 32 bits per pixel	256MB Graphics Card
Processor	modern processor (>800MHz)	1 GHz 32-bit (x86) or 64-bit (x64)	Dual-Core
Hard Drive	>15GB free (recommended)	40GB capacity, >15GB free	7200 rpm
Window Vista Aero Experience	None	Aero enabled as a default, but performance may be compromised as more windows, applications and games are opened. DVD Readable Drive Audio output capability Internet access capability	Can enhance Aero experience and system performance

a. Finding(s)

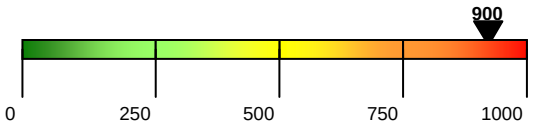
KCCD has no current plan for rolling out the new Microsoft versions that have recently been released to the market place. There are no known budgets, plans, impact analysis on hardware, or even discussions at this point. The only activity is with select IT faculties who have obtained trial versions and are selecting associated textbooks beginning in fall 2007. It is presently unknown how this will co-exist with other applications used in open computing labs and / or administrative systems. The lack of a comprehensive district inventory of hardware prevents an accurate impact analysis of upgrade, replacement, budget, support and training requirements.

Possible Impact

The introduction of the most current version of software and operating systems impacts many different academic programs as well as administrative users. While traditional IT courses have a paramount need to teach using the most current versions, non-IT academic disciplines typically have software which are not tested out on new releases of operating systems for some period of time. Most software companies wait for several patch updates to Microsoft releases until they begin to address their required updates. The dynamic mix of applications used by students for

various disciplines in the same open labs complicates the timeframe for the co-existence of several software versions. Administrative users typically have the least sense of urgency to migrate to new versions of software as the limited new functionality is mitigated by the risks of stable, secure and reliable operation of the new software.

Suggested Priority for Resolution



Roadmap

1) Begin discussions within the Academic Senate, DWITC, college IT committees and relevant disciplines to determine the desired dates for using the new Microsoft versions.

2) Assemble a project team. **REFER TO THE PROJECT MANAGEMENT SECTION FOR ADDITIONAL INFORMATION.**

3) Conduct a comprehensive inventory of all application hardware, desktop and laptop computers, printers, and servers as a prerequisite to identify their compatibility with Windows Vista. **REFER TO THE ASSET MANAGEMENT SECTION FOR ADDITIONAL INFORMATION.**

4) Collect and analyze the application inventory to determine compatibility with Windows Vista. There are thousands of applications and devices that are compatible with Windows Vista; however, **Certified for Windows Vista** devices and software have been tested to help ensure that they are compatible with the **premium** features of Windows Vista. Devices and software that carries the **Works with Windows Vista** logo are tested for **baseline** standards of compatibility with all PCs running Windows Vista. See logos below.

5) Create a test plan that describes the tests to be run, the expected results, a schedule for performing tests, and who will run each test. The test plan must specify the criteria and priority for each test.

6) Perform comprehensive testing on each hardware platform, testing both application installation and operation in a controlled environment. The test environment should mirror, as closely as possible, the user's network, including hardware, network architecture and business applications.

7) Test mitigation strategies. Create application mitigation packages. Test the deployment of the mitigation packages.

8) Identify core applications to be placed on new operating system image.

9) Develop and test the images of Windows Vista.

10) Choose a user population that represents a cross-section of the institution in terms of job function and computer proficiency to pilot the project.

11) Roll out the deployment to a small group of users. The primary purpose of the pilot is not to test Windows Vista. Instead, the aim of the pilot is to get user feedback to determine the features that may need to be enabled or disabled on Windows Vista.

12) Compile the pilot results and use the data to estimate upgrade times, the number of concurrent upgrades the college and district can sustain, and peak loads on the user support functions.

13) Develop a support plan that includes an escalation plan to deal with expected support calls and a training plan to ensure that support personnel are trained to handle users' questions. Schedule the training just prior to the rollout of Windows Vista and the 2007 Microsoft Office system.

14) Educate end users about the deployment process and new features and functionalities of the new products.

15) Develop a training and communication plan for faculty, classified / confidential staff, and management during the deployment of Windows Vista and the 2007 Microsoft Office system.

16) Publish knowledge based articles or FAQ's dealing with any possible issues the user may encounter after receiving their new or reconfigured desktop.

17) Publish resolution to issues in support articles, which could be searched and retrieved by support technicians.

18) Develop a multi-year budget for the replacement program as well as upgraded software costs.

19) Investigate alternative financing to enable an equipment replacement program.

Business Continuity Plan


Open Lab

The recovery of information technology services are just one area of institutional operations that need to be restored in the event of a disaster. Business Continuity Planning (BCP) is a process that helps organizations prepare for disruptive events – whether an event might be a flood of the Kern River, an earthquake such as the one on July 21, 1952 that leveled most of historic downtown Bakersfield's, or perhaps a power outage caused by a backhoe in the parking lot.

a. Finding(s)

Based upon verbal conversations, college departments have not identified or documented the functions and processes that are essential to them in the event of a disaster.

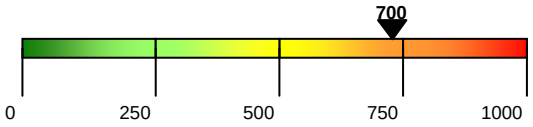
Possible Impact

In the event of a disaster, KCCD may not be able to coordinate appropriate measures to restore critical systems.

Service continuity controls should be designed to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and that critical and sensitive data are protected. These controls include:

- Environmental controls and procedures designed to protect information resources and minimize the risk of unplanned interruptions.
- A well-tested plan to recover critical operations should interruptions occur. If service continuity controls are inadequate, even relatively minor interruptions can result in losses, expensive recovery efforts, and inaccurate or incomplete financial or management information.

Suggested Priority for Resolution



Roadmap

1) Consider developing a Business Continuity Plan Checklist to help organize and put in place an emergency recovery plan for information systems/technology and computing groups in college departments. Include items such as:
   - Risk Assessment
   - Resource Assessment
   - Integration with Department Response and Recovery Planning
   - Interim Operation Plan – Prearranged Agreements for Resource Replacement

- Test, Evaluate and Update the Plan
- Recovery and Restoration

2) **REFER TO THE ROADMAP NAVIGATIONAL TOOLKIT SECTION – CONTINGENCY AND RECOVERY PLANNING: CHECKLIST FOR INFORMATION SYSTEMS FOR AN ILLUSTRATION.**

Disaster Recovery Plan

Cerro Coso Community College

Institutions must create technology profiles to accurately scope all IT systems that need to be included in a comprehensive Disaster Recovery Plan (DRP). Any systems missed during such a comprehensive scoping exercise can cause single point of failures in the event of a disaster.

The development of a DRP plan inclusive of strategies, policies and procedures must be approved and disseminated for all critical staff and users to follow in the event of an emergency. The absence of a plan can render chaos and certainly a delayed return to standard operation in the event of a disaster.

The regularly scheduled testing of an approved DRP is essential to assuring the quality of its effective return to normal operations. Such a test also discovers assumptions that are incorrect and cause vulnerability.

Most DRP's are developed based upon a historical snapshot of IT systems. The constantly changing IT environment mandates regular maintenance to an existing DRP with focus unit testing where changes have occurred.

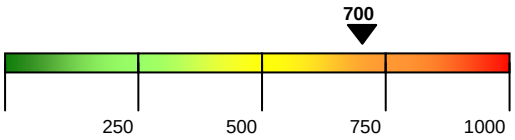
a. Finding(s)

Bakersfield, Cerro Coso and Porterville College as well as the District Office have an Emergency Operations Plan in place. Each plan has been tested; however, Porterville's plan was last tested in 2003. It is uncertain if these plans will meet the new Federal National Incident Management System (NIMS) requirements. On the other hand district IT does not have a plan in place to recover and restore essential IT operations in the event of an emergency.

Possible Impact

The reliance solely on a disaster recovery plan can leave many critical data center operations in an institution without alternative operational processes in the event of a disaster. The loss of facility or power or weather exception may cause critical IT operations in the institution to cease. If reasonable alternatives, where applicable, and can be identified then the institution may continue to fulfill its mission despite such events.

Suggested Priority for Resolution



Roadmap

1) Develop an IT Disaster Recovery Plan to include the following:
   - Overview / Objectives
     - Primary Focus
     - Assumptions

- Primary Objectives of the Plan
- Personnel
- Salvage Operations at Disaster Site
- Designate Recovery Site
- Purchase New Equipment
- Begin Assembly at Recovery Site
- Restore Data from Backups
- Restore Applications Data
- Move Back to Restored Permanent Facility

- Preparation
  - Disaster Recovery Planning
  - Recovery Facility
  - Replacement Equipment
  - Backups
  - DRP Document

- Backup Procedures

- Notification List

- Recovery Teams
  - Recovery Management Team
  - Damage Assessment Team
  - Facility Recovery Team
  - Network Recovery Team
  - Platform Recovery Team
  - Application Recovery Team
  - Administrative Support Team

- Activating the Plan. **REFER TO THE ROADMAP NAVIGATIONAL TOOLKIT SECTION – ACTIVATING THE PLAN FOR AN ILLUSTRATION.**
  - Determine Personnel Status
  - Equipment / Media Protection & Salvage
  - Establish The Recovery Control Center
  - Activating the DRP

- Damage Assessment

- Emergency Procurement

- Cold Site Preparation

- Platform Recovery

- Network Infrastructure Components
  - Topology Diagram
  - Configuration Specifications
  - Administrative Operating Procedures
  - Hardware / Software Inventory List
  - Configuration & Change Management Procedures
  - Service & Support Contact Information
  - Specific DR & Business Continuity Procedures
  - Backup & Recovery Procedures
  - OS & Application Install Security Checklist
  - Security Policy & Access Control Procedures
- Novell Servers (refer to above categories)
- Microsoft Servers (refer to above categories)
- Telephony (refer to above categories)

- Applications Recovery Procedures

- Maintaining the Plan

2) Ensure stakeholders are informed of the plan, processes and procedures.

3) Forward the plan, processes and procedures to the IT Governance committee for review and approval.

4) Schedule and conduct drills. Practice where a secondary problem happens and key people are hurt and unavailable.

5) Conduct an After Action Review. Check that information was not lost / accessed that violates the Patriot Act, HIPPA, etc.

6) Consider contacting California's Governance Office of Emergency Services (http://www.oes.ca.gov) division to receive information regarding the Homeland Security Preparedness Technical Assistance Program Catalog or visit http://www.ojp.usdoj.gov/odp/ta.htm. The Department of Homeland Security, Office of Domestic Preparedness (ODP) established a Homeland Security Preparedness Technical Assistance (TA) Program that provides direct assistance to state and local jurisdictions to improve their ability to prevent, respond to, and recover from threats or acts of terrorism involving chemical, biological, radiological, nuclear or explosive (CBRNE) weapons. TA provides a process to help resolve a problem and / or create innovative approaches. All TA services are available to eligible recipients at no charge.

Security

Bakersfield College

IT security is the implementation of security policies, processes, and devices to prevent the unauthorized access to network resources or the alteration or destruction of resources or data. Security policies are the basis for the security implementation; security processes and devices are used to enforce the policy.

This section *is not* intended to be a comprehensive security review. It will only highlight certain areas for improvement at a high level. All organizations should perform a full security audit on a yearly basis to ensure they are appropriately protected functionally, financially, and legally.

IT Security and Acceptable Use Policy

The first rule of network site security is easily stated: that which is not expressly permitted is prohibited. A security policy should deny access to all network resources and then add back access on a specific basis. Implemented in this way, a site security policy will not allow any inadvertent actions or procedures. The goal in developing an official site policy on computer security is to define the institution's expectations for proper computer and network use and to define procedures to prevent and respond to security incidents. In order to do this, specific aspects of the organization must be considered and agreed upon by the policy-making group. The policy begins with assessing the risk to the network and building a team to respond. Continuation of the policy requires implementing a security change management practice and monitoring the network for security violations. Lastly, the review process modifies the existing policy and adapts to lessons learned.

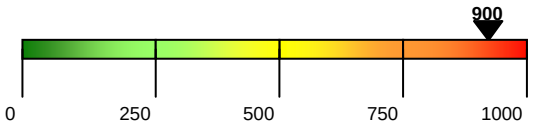
a. Finding(s)

KCCD does not maintain a well documented or enforced Security and Acceptable Use Policy.

Possible Impact

A formal security policy is necessary to establish guidelines for secure access to the information assets for business use, protect the infrastructure from factors that could affect the institution's profitability and growth, maximize the security of the infrastructure, and define responsibilities and expectations of all employees.

Suggested Priority for Resolution



Roadmap

1) Review RFC 2196, Site Security Handbook. It remains the definitive guide on security policies.

2) Policy creation must be a joint effort by a representative group of decision-makers, college and district IT / IS personnel, and day-to-day users from different levels within the institution. Decision-makers must have the power to enforce the policy; technical personnel will advise on the ramifications of the policy; and day-to-day users will have a say in how usable the policy is.

3) Expand upon the Information Technology Security Policy dated October 2006. Develop a security policy that comprises identifying the institutional assets, identifying the threats, assessing the risk, implementing the tools and technologies available to meet the risks, and developing a usage policy.

4) Develop an auditing procedure that reviews network and server usage on a timely basis.

5) Develop an incident response policy to create the processes and procedures that should be followed in the event of an incident.

6) Communicate the policy to everyone who uses the computer network, including employees, contractor, and students. Ensure the policy is reviewed on a regular basis.

7) **REFER TO THE ECAR RESEARCH BULLETIN ENTITLED "LOCAL IT SECURITY FOR COLLEGES, SCHOOLS, AND DEPARTMENTS: A HIGHER EDUCATION PERSPECTIVE", VOLUME 2006, ISSUE 24, DATED DECEMBER 5, 2006 FOR ADDITIONAL THOUGHTS ON CENTRALIZED / DECENTRALIZED IT SECURITY STRUCTURE.**

8) **REFER TO THE ROADMAP NAVIGATIONAL TOOLKIT SECTION – IT SECURITY FOR HIGHER EDUCATION: A LEGAL PERSPECTIVE FOR ADDITIONAL INFORMATION.**

9) **REFER TO THE POLICIES AND PROCEDURES SECTION FOR ADDITIONAL INFORMATION.**

Security – Data Protection (Identify, Locate, Classify, Prioritize)

KCCD relies heavily on its electronic data processing systems and the data stored in them to meet its educational, research, informational and operational needs. The risks to private data in the electronic environment have substantially increased. At KCCD, most electronic devices are directly connected to the KCCD network and the Internet. Data is increasingly mobile to desktop, laptop, and handheld devices, which need to be secured. Viruses, worms and malicious programs from the Internet as well as accidental and unintentional loss of data are substantially increased risks in such an environment.

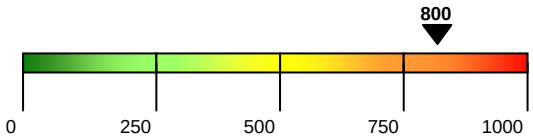
a. Finding(s)

KCCD has put in place a Confidentiality Policy detailing disclosure of educational records, employee personnel files, donor and alumni records, College systems and databases and electronic mail or facsimile

transmissions. The policy does not however address "technical" requirements to protect the data. There is no specific policy governing the download of KCCD data to portable media.

Possible Impact
There has been an increasing volume of the theft of data downloads from laptops and portable media, such as CDs, PDAs, memory sticks, etc. While employees may not intend the consequences of such a theft causing their institutions data to fall in to the wrong hands, the value of the data typically exceeds of the value of the media or machine particularly if it falls into the eventual hands of organized crime.

Suggested Priority for Resolution



Roadmap

1) Develop and approve a "technical requirements" security plan to protect private data on computers. Include items such as:

   - Configuration and maintenance
   - Authentication and encryption
   - Anti-Virus technology
   - Firewall or filtering
   - Access
   - Security event logging
   - Vulnerability scans
   - Backups and physical security

2) Store paper/electronic documentation in a secure area / directory.

3) Develop a policy to minimize the distribution of sensitive data, including the printout of sensitive information. Examples of sensitive data include but are not limited to the following:

   - Social Security Number
   - Trade secrets or intellectual property such as research activities
   - Birth date
   - Home phone number
   - Home address
   - Health records

- Student grades
- Location of assets
- Parking leases
- Anonymous donors
- Gender
- Ethnicity
- Citizenship
- Citizen visa code
- Veteran and disability status
- Linking a person with the subject about whom the library user has requested information or materials

4) Research the use of a removable expansion card for Personal Digital Assistants (PDAs). The card, also known as a personality card, is capable of storing all of a user's private information and data which is used within their PDA. By removing the card from the PDA, all of the user's private information and data may be removed from the PDA. The PDA may also be rendered totally or partially useless once the card is removed.

5) Assign a college / district IT / IS staff member to periodically review computers/portable devices for compliance with security policies and requirements.

6) Set a regular schedule to review computers/portable devices for compliance with security policies and requirements.

7) Record and track problems and corrective actions taken with computers/portable devices.

8) Ensure Academic and Administrative departments are aware of the plan and what their responsibilities are.

9) Review the policy on an annual basis.

10) **REFER TO THE ROADMAP NAVIGATIONAL TOOLKIT SECTION – SECURITY PLAN TO PROTECT PRIVATE DATA ON COMPUTERS FOR AN EXAMPLE.**

IT Security Program

Implementing an information security program is essential to ensuring that controls over information and information systems work effectively on a continuing basis. Part of the program includes appointing an information security officer to manage the program, establish a task force for conducting risk assessments, security tests and evaluation.

An information security program requires key elements including:

- Policies and procedures that –
  - are based on risk assessments
  - cost effectively reduce risks
  - ensure that information security is addressed throughout the life cycle of each system
  - ensure compliance with applicable requirements

- Security awareness training to inform personnel including contractors and other users of information systems, of information security risks and their responsibilities in complying with KCCD policies and procedures

- At least annual testing and evaluation of the effectiveness of information security policies and procedures, and practices relating to the management, operational and technical controls of every information system that is identified in KCCD's inventory

Another key element of an information security program involves promoting awareness and providing required training so that students and users understand the risks and their role in implementing related policies and controls to mitigate those risks. Computer intrusions and security breakdowns often occur because users fail to take appropriate security measures. For this reason, it is vital that employees who use computer resources in their day-to-day operations be made aware of the importance and sensitivity of the information they handle, as well as the business and legal reason for maintaining its confidentiality, integrity and availability.

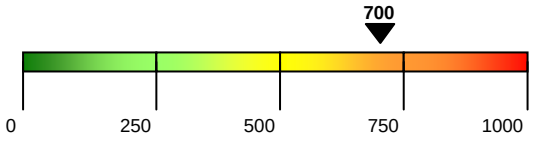
a. Finding(s)

KCCD has not fully implemented a security program. Discussions have begun as to the need for a Chief Information Security Officer (CISO) and establishing a security program.

Possible Impact

An institution needs a single fully empowered department to define, implement and control IT security lest all measures only be partially implemented and rendered ineffective.

Suggested Priority for Resolution



Roadmap

1) Establish an information security team that includes college and district IT / IS personnel.

2) Build an IT enterprise-wide security program that includes college and district IT, outside service providers, business partners, vendor and representatives from public safety, facilities and key data areas.

3) Provide training opportunities for the college and district IT / IS personnel.

4) Provide training opportunities to the user community based on their level of responsibility and access to sensitive information.

5) Encourage and support the acquisition of security certifications.

6) Record and maintain all training records and related documentation.

7) Involve Executive Management in security related decisions to ensure appropriate alignment between information security issues, IT parameters, digital assets and business objectives, allowing KCCD to stay focused on its mission.

8) Develop written procedures and guidelines. **REFER TO THE POLICIES AND PROCEDURES SECTION FOR ADDITIONAL INFORMATION.**

9) Design, develop and implement an Employees Guide to IT Security program to inform users of their IT security responsibilities. The program should address user roles and responsibilities, policies and procedures.

10) Promote awareness of the program. Suggested marketing tools include:

- Oral Briefings – have college and district IT / IS staffs visit departments on a regular basis
- *e*Mail – IT Security awareness email messages could be sent out periodically
- Online Commercials/Advertising – a commercial could be scheduled to appear on the computer screen at a predetermined time (once a month), when the user logs on. The user would have to click through the screen in order to continue the logon process
- Newsletters – create articles for the various college newsletters / brochures / web sites, etc.
- Desktop Icon – create an Employees Guide to IT Security icon on the computer desktop addressing security topics

11) Add a section to the Employee Handbook addressing IT Security and User Responsibilities.

12) Create an IT Security web site to include topical areas such as user password management, virus protection, handling security breaches, counteracting social engineering exploits, data privacy, etc.

13) Develop a computer based training program to promote awareness.

14) Assess, update and redeploy the IT security program continuously.

Physical Security

Physical security — controlling and recording personnel access to facilities — is critical to achieving data center availability goals. As new technologies such as biometric identification and remote management of security data become more widely available, traditional card-and-guard security is being supplanted by security systems that can provide positive identification and tracking of human activity in and around the data center.

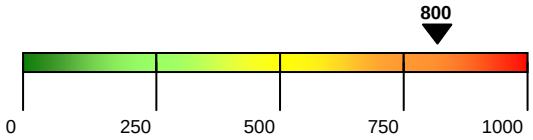
a. Finding(s)

KCCD does not currently use a video surveillance system to monitor ingress/egress of their data center or wiring closets. Door entrants are accessed via key and / or swipe card. The District Office data center is alarmed.

Possible Impact

In the event of a physical security breach, it is critical to quickly determine what happened, when it happened, and who caused it. A well designed video surveillance system plays an integral part in the event of an investigation.

Suggested Priority for Resolution



Roadmap

1) Implement a video surveillance system that covers all ingress / egress points of the data center as well as key areas within the data center. Place the cameras so that it is easy to identify an intruder and determine what assets may have been compromised. Camera locations can be made visible to provide an additional deterrent; however, they should be tamper-proof.

2) Create a policy on video recording that addresses the following:

- How will the video files / tapes be indexed
- Will they be stored off site
- Who will have access to them
- How long will they be kept before being destroyed

3) If budget allows, implement a video surveillance system that covers all wiring closets as well.

4) Post a sign at each entrance marking the computer room as restricted access and prohibits food, drinks and smoking in the facility.

5) Restrict access to those who need to maintain the servers or infrastructure of the room. If cleaning staff, 3rd party vendors, etc. must access the computer room they must be escorted by IT personnel.

6) Log and track all visitor activity. Require all visitors who enter the computer room to sign-in / sign-out. Keep logs for at least one year.

7) Require all visitors who enter the computer room sign a Non-Disclosure agreement.

8) Require all visitors who enter the computer room wear a photo ID identifying who they are and the organization they represent.

9) Limit the distribution of master keys to essential IT personnel only.

IT Infrastructure

Bakersfield College

IT infrastructure refers to the computerized networks, intelligent terminals, and accompanying applications and services people use to access, create, disseminate, and utilize digital information; the equipment, software, services, and products used in storing, processing, transmitting, and displaying all forms of information. IT includes data processing, office automation, multimedia, and telecommunications; the knowledge and skills of the people who design and operate the technologies which supply business solutions.

Data Center

The data center of an institution provides the secure, physical environment in which all mission-critical software applications reside. The performance, reliability, and availability of the software applications are partially dependent upon a stable hardware environment. A significant component of a stable hardware environment is the specialized physical environment in which it exists.

a. Finding(s)

The main data center for the district is located on the first floor of the Weill building in downtown Bakersfield. The facility has adequate floor space for expansion, has an orderly floor plan design, and makes good use of rack mounting for equipment.

There is a separated electrical system for all equipment in the data center with appropriate UPS power backup and an external diesel generator. There is also minimal backup lighting in the event of power outages.

The main ventilation system for the building has been damped off. There is a separate air-conditioning system with specialized filtration and humidity controls for this environment. There is no impact printing done within this environment.

Specific to physical security, there is a card system to access the environment but is not used in combination with a pin code. There is no audit record retained on entry. There are physical keys available to access all of these doors and non-IT staff is in possession of some keys. There is also use of remote cameras to view activities in this unstaffed area. Other keys and the primary security system are kept in the Maintenance and Operations area.

FM-200 gas is used as the fire suppression system and the building's water-based, fire extinguishing infrastructure has been shut off to this area.

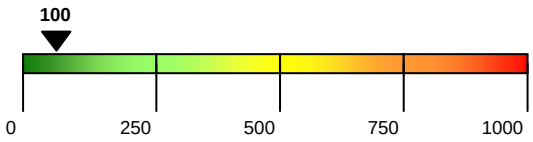
There are water sensors under the false floor and none of the adjacent walls join rooms that use water.

There is remote paging ability for all environmental systems that experience exceptions.

Backup tapes are stored locally in a vault and are routinely rotated to an off-site facility located two hours to the north.

Possible Impact
Traditional environmental systems that facilities provide are in adequate for a data center environment. Common air ventilation systems produce dust that reduces the reliable lives of computer hardware. The use of water for fire suppression can damage all the equipment and a data center. Having physical key access to a data center in the hands of any non-IT staff member becomes a critical security risk. Exceptions in any of these areas can cause critical systems to be unavailable for key business processes for extended periods of time.

Suggested Priority for Resolution



Roadmap
KCCD's data center environment is found to be the best practice and has few recommendations for improvements. The center would be ideal for the expansion and location of any other IT infrastructure provided throughout the district. Four minor recommendations are as follows:

1) Expand emergency, backup lighting in the facility and connect into the diesel generator.

2) Shift to a tool access security entrance system which combines a card access with a pin code. In the event cards are taken by unauthorized staff access will not be granted.

3) Begin to track those who access the facility and maintain this as an audit record.

4) Reduce the number of staff who has physical keys to access the environment. This should be limited to very few management and staff within IT. The only staff external to IT that should be in possession of a physical key should be Maintenance and Operations.

Network Infrastructure

A robust and comprehensive wide and local area network infrastructure has become the critical data highway for higher education. Both academic and administrative systems and users rely upon a network which has a high-availability, acceptable response time, and is adequately secure.

Higher education institutions now expect network services to be available any time and anywhere. This is a very similar expectation that many students have in the delivery of teaching and learning. These two expectations have a related link: network infrastructure is a key enabler to accessing teaching and learning materials.

a. Finding(s)

Local-area network infrastructure is reasonably well flooded within each of the colleges and the district office. Students are not allowed to plug their laptops into the network and open learning labs or elsewhere within colleges owed to security concerns.

The wide area network infrastructure connecting all colleges to the district office data center facility utilizes a low-cost microwave in coordination with the county government. T1 lines are used as backup when the microwave link goes down. Response time suffers using this contingency; however, disruptions have become less frequent since a contract, including service-level agreements and performance metrics, was entered into with the county.

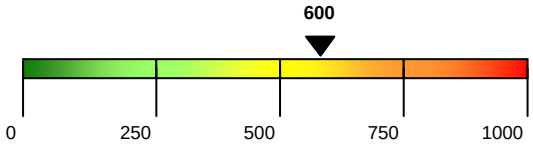
There is no standard wireless network access in use at the colleges or district office. There are a few pockets testing as testing this technology but with no plans of wider deployment owed to budget limitations and security concerns.

Possible Impact

Students and faculty now require more convenient access to network services to support the teaching and learning environment. The lack of such availability prevents, or at least limits, the use of new instructional and classroom technologies. This lack of availability also prevents students from gaining convenient access to materials which support their learning processes.

The use of these more modern teaching technologies has become widespread in higher education – particularly in the institutions that deliver distance education. The lack of the network infrastructure to support these linkages has now become a competitive disadvantage in seeking maximized enrollment.

Suggested Priority for Resolution



Roadmap

1) Develop a plan to allow students to plug their laptops into network accesses in open learning labs. There are appropriate security practices that can be copied from other similar institutions that would address any concerns on this issue.

2) Develop a plan for a wireless networking standard that can be deployed throughout the district with appropriate levels of security and performance. This should be deployed in the open computing labs, libraries, and cafeterias of each of the colleges as a priority.

Videoconferencing Infrastructure

Videoconferencing has become increasingly popular as a medium for both instruction and meetings in higher education. Like other IT infrastructure that has become critical to the delivery of mission-critical activities, there is an expectation of a high degree of availability, reliability, and appropriate security.

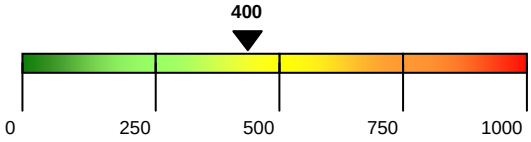
a. Finding(s)

There are pockets of support and expertise for the instructional and administrative videoconferencing systems throughout the district. There is different equipment used for instructional video conferencing, as there is for administrative videoconferencing. The need for resolution for operational exceptions has a high degree of urgency owed to the large number of people it affects particularly if it's interrupting instruction. The support model for this infrastructure varies from college to college and within the district. A separate, albeit small, help desk to support this area exists within Bakersfield College.

Possible Impact

As with most new technology, effective adaptation typically happens in pockets of innovative trials. Repeated trials that prove successful quickly spread its use and adaptation to other uses. Over time the redesign of its infrastructure may become necessary for its effective use to become more efficient. Original innovators can become less adaptive to iterative change. Fresh perspectives are usually required to develop new uses and more efficient procedures and operations.

Suggested Priority for Resolution



Roadmap

1) The spread of its common use within the district has created evolutionary pressures for the support of effective use of videoconferencing. A consolidation of help desk operations should include an expedient response to videoconference users throughout the district.

2) Examine best practices from other institutions for the use of a Video Operations Center (VOC) within the district. Such a VOC should provide stable and reliable operations, including adequate security for existing and new user applications. New user applications should grow to include its use for expanded professional development training within the district.

SWOT Workshop

Porterville College

The facilitation of a Strengths, Weaknesses, Opportunities and Threats (SWOT) Analysis, conducted by a SunGard Higher Education consultant, was held with key members of Kern Community College District's faculty, staff and management. The general purpose of the meeting was to begin discussions on the need for developing a strategic plan for information technology at Kern Community College District. Each of the key stakeholders within the institution shared their opinions on strategic planning elements of significant consideration to the institution.

The work session developed a key step in the IT strategic planning process, which is to analyze the strengths, weaknesses, opportunities, and threats – the SWOT analysis. Its primary purpose is to ensure that an institution is positioned to take maximum advantage of the capabilities of information technology to achieve their organizational objectives. Additionally, it provides a starting point to establish (or validate) a clear long-term direction for all technology projects and expenditures.

The SWOT Workshop was arranged by David Palinsky, Director of IT for the District. It was conducted at the Bakersfield College Fireside Room on Thursday, March 8, 2007 from 9:00 a.m. to 12:45 p.m. There was a high degree of engagement which rendered a significant number of suggestions to include in the SWOT.

In preparation for the on-site work sessions to review Kern Community College District strategic planning process for technology, the invited participants were asked to begin thinking about where they see technology supporting the mission and goals of Kern Community College District, how Kern Community College District can utilize technology strategically to advance the goals of this institution, and their vision of the role of technology in the system for the next five years.

Several documents were provided by the SunGard Higher Education consultants to the confirmed attendees in advance of the SWOT Workshop including:

- An overview of the elements of the SWOT exercise
- An outline of stakeholders whose perspectives must be considered in a SWOT exercise
- A notes outline for ideas they may have in advance of the exercise

The following individuals participated in the SWOT session:

SWOT FACILITATION PARTICIPANTS	
NAME	**DEPARTMENT / OFFICE / DIVISION**
Bill Moseley	Computer Studies, BC
Chris Romanovich (for Cindy Collier)	Allied Health, BC
Jim McGee	Information Services, BC
John Jaramillo	Educational Administration, BC
Kirk Russell	Library, BC

SWOT FACILITATION PARTICIPANTS	
NAME	**DEPARTMENT / OFFICE / DIVISION**
Kristin Rabe	Media Services, BC
Nick Strobel	Physical Science, BC
Rachel Vickrey	Mathematics, BC
Sue Granger-Dickson	Learning Support Services, BC
Corey Marvin	Information Technology, CC
Lisa Couch	Human Resources, CC
Mary Retterer	President, CC
Natalie Dorrell	Bookstore, CC
Donna Berry	Business Services, PC
Steve Schultz	Academic Center, PC
Virginia Gurrola	Financial Aid / Admissions & Records, PC
David Palinsky	Information Technology, DO
Eddie Alvarado	Information Technology, DO
Greg Chamberlain	Educational Services, DO
Mark Beam	Institutional Research, DO

The following individuals were invited to attend the SWOT session; however, due to prior commitments they were unable to attend.

SWOT FACILITATION PARTICIPANTS	
NAME	**DEPARTMENT / OFFICE / DIVISION**
Adie Geiser	Supportive Services, BC
Matt Hightower	CC Online, CC
James Carson	Academic Center, PC
Rickelle Syradahl	Science / Mathematics, PC

SWOT Agenda
The following agenda was used during the SWOT Workshop:

- Welcome
- Roles of the facilitator
- Review of advance materials provided to participants, including:
- SWOT document
- Key emerging strategies
- A review of stakeholders
- Group identification of possible internal strengths and voting

- Break
- Group identification of possible internal weaknesses and voting
- Break
- Group identification of possible external opportunities and voting
- Break
- Group identification of possible external threats and voting
- Lunch
- Final voting and review of all entries

SWOT Analysis
Strategic planning must include an assessment of the organization's environment because no organization operates in a vacuum. The very definition of strategic planning stresses the importance of focusing on the future within the context of an ever-changing environment - the myriad of political, economic, social, technological, demographic, and legal forces that change our world daily. Skill at assessing the environment and then being proactive in responding to that environment (i.e., – strategic planning, thinking, and management) determines who is effective in using their resources and, ultimately, who survives.

At the conclusion of a SWOT analysis, a strategic planner will have a database of quality information that can be used to make decisions and a list of critical issues which demand a response from the organization – the most important issues the organization needs to deal with in the strategic planning process.

Part of getting a clear view of the environment and dynamics of an organization is to look at it through others' eyes; both internal and external stakeholders' perceptions of the organization will add valuable information to the situation assessment. The SWOT technique, a simple and effective vehicle for collecting this information, helps focus the process by breaking it down into four broad categories:

S – What are the organization's internal Strengths?
W – What are the organization's internal Weaknesses?
O – What external Opportunities might move the organization forward?
T – What external Threats might hold the organization back?

Evaluating an organization's general strengths and weaknesses, as well as the strengths and weaknesses specific to each of its programs, typically includes assessments of:

- IT staff capabilities
- Quality of IT services
- Reputation of both the organization and individual services
- Administrative IT

- Desktop and networking infrastructure
- Academic IT
- Library and research systems

Successful organizations exploit strengths rather than just focus on weaknesses. In other words, this process isn't just about fixing the things that are wrong, but also nurturing what is right.

The same kind of thinking should apply to how an organization approaches its opportunities and threats – the external trends that influence the organization. These are usually categorized into political, economic, social, technological, demographic and legal (PESTDL) forces. These external forces include such circumstances as changing client needs, increased competition, changing regulations, and so on. They can either help an organization move forward (opportunities) or hold an organization back (threats) – but opportunities that are ignored can become threats, and threats that are dealt with appropriately can be turned into opportunities.

Stakeholder Identification
A successful SWOT analysis keeps in mind all key stakeholders of an institution. Which of these stakeholders are the primary beneficiaries of a successful IT strategic plan? Which stakeholders have been previously excluded from many benefits in the past who may now be included in future benefits? Key, primary stakeholders may include:

- Academic lab computer users
- Administrative computer users
- All Students
- Faculty teaching computer disciplines
- Other Faculty and staff
- Taxpayers
- Member Community Colleges
- Alumni

Additional, more specific examples of stakeholders who could be considered within an IT strategic plan include:

- Parents
- Legislators
- Community
- Public schools
- Accrediting bodies
- Foreign governments
- Vendors

- Employers
- Prospective students
- Media
- Businesses
- Unions
- Board of Regents
- Professional organizations
- Competitors
- Local city representatives
- Donors
- Grant sponsors
- Foundations

Board & Staff Perceptions of the Organization
Since the SWOT analysis is a primary means of receiving input from a broad and representative constituency, it is important to include as many staff and board (your internal stakeholders) as possible in the process. Their ideas and opinions might be collected through questionnaires, telephone or in-person interviews, facilitated organization-wide or small-group meetings, or a combination of these methods. Some organizations have board and staff meetings together to discuss their ideas and opinions, while others have them meet separately. A common and useful approach used during meetings is to brainstorm ideas onto flipcharts.

After the lists of strengths, weaknesses, opportunities, and threats have been recorded, the listed ideas can be grouped into logical topic or issue groups (e.g., – all the ideas related to staffing or program development should be grouped together) to make the data easier to present and analyze.

External Stakeholders' Perceptions
Just as a SWOT assessment allows an organization to collect a wide variety of perceptions from internal stakeholders, a SWOT assessment of those outside the organization can also add a great deal to the SWOT analysis. External stakeholders (such as clients, funders, community leaders, and potential collaborators) can give the planning committee insight into community opinions of what the organization does well, where it can improve, unmet community needs it might address, and other potential opportunities or threats.

Again, this information might be gathered through telephone or in-person interviews (preferably), questionnaires, or focus groups. In addition to their general perceptions of the organization's strengths, weaknesses, opportunities, and threats, external stakeholders might also be asked some questions specific to their outsider perspective. For example:

- What are the organization's strengths and weaknesses? What opportunities and threats does the organization face?
- What does the stakeholder need or expect (criteria for performance) from the organization?
- How well does the organization perform against those criteria (excellent, good, fair, or poor) and why?
- How well does the organization perform relative to its competitors?

KCCD Internal Assessment

The discussion on the internal assessment of strengths and weaknesses with the KCCD participants developed the following initial outline which appears in the order mentioned by participants:

STRENGTHS

- Good District IT staff
- Students can register online
- Students can check grades online
- Banner system kept current
- Strides to continually improve
- Good internal coordination and communication
- Outlook / Exchange productivity tool used throughout district
- District Help Desk fast to respond
- College Help Desk prioritizes
- IT system proven to be flexible
- Comprehensive network connectivity
- College (BC) IT responsive to end user needs
- High network availability
- Good focus on student use of technology
- Good choices of instructional delivery (*i*TV)
- Good administrative support for new ideas
- Students can check progress on degree requirements
- Good web information for students on web information
- User tips on IT web site and online user support
- All students have access to technology in open labs
- IT staff's knowledge base more multiple systems
- Online administrative forms and workflow for staff
- Online access for students
- Some provision of student email accounts

- IT provides custom reports
- Video technology infrastructure for administrative and instruction
- Economies of scale fro IT investment uses
- Cooperation between IT and Media Services
- Tools and media for groups to multi-task
- Provision of training
- Technology in place to make instruction more productive
- District data center facility and environment
- Strong district management support for IT
- Online instruction is well received as viable teaching mode
- Electronic support for student research needs including training
- Data available

WEAKNESSES

- Aging infrastructure
- Lack of money
- Data integrity
- Data stewardship
- Shadow systems and books
- Inadequate internal training
- Consistency of support across the district
- Lack of standard replacement cycle
- Not enough of the right type of IT staff
- Non existent Disaster Recovery Plan
- Inconsistent online delivery platforms
- Lack of trust within district and college groups
- Emphasis of speed over quality
- Insufficient security mechanisms
- Lacking of training and support for teaching with technology
- Insufficient classroom technology
- Lack of wireless access
- Inconsistent of support from the district to all of the colleges
- Inconsistent planning and project management
- Assumptions on digital divide
- Lack of full online interaction with students
- Lack of a data warehouse or datamart
- Inconsistency on data reporting particularly with online students
- Inconsistent district processes
- Lack of data validation
- Gap between technologies and students with special needs

- Gap with students with limited financial resources for technology
- Lack of resources for innovation
- Technology is not a central part of district planning – alignment of IT projects with district goals
- Inconsistency on communications between IT and users
- Web pages need updating
- Culture of resistance to change
- Resistance to committing to change
- Pathways to end-users affected by decisions

KCCD External Assessment

The discussion with KCCD participants on external assessment of opportunities and threats within the environment developed the following initial outline:

OPPORTUNITIES

- Utilize technology to support regional programs and courses – e.g., career and technology education
- Increase online enrollment and marketing
- ARCC (Accountability Reporting for Community Colleges)
- More use of portal technology
- Use of *e*Commerce for student transactions – e.g., books online
- Web site used for marketing
- Utilization of mobile technology
- Alternative scheduling and delivery
- Better internal communications
- Use of list serves with students
- Use of MySpace, YouTube
- Use technology to improve data integrity
- Grant for funding technology
- Larger student population owed to county expansion
- Use IT to partner with local businesses and schools
- Internal funding opportunities for innovation
- Use technology to make it easier for students to submit transcript
- Better use of EDI – e.g., student transcripts
- Student transfer ease within district
- Student employment and internship
- Use technology to market to families
- Technology outreach to parents and businesses
- Use IT to identify students at risk early and to get them back on track
- Improve room utilization

- Improve access to student assessment process
- Standardize interfaces in distance education offerings
- Online tutorials in instruction
- Improve access by disable students
- Deliver enrollment management tools
- Fund raising with alumni and foundations
- Improve student connections for retention
- Online classes for staff development
- Track students that drop out to determine why
- No Child Left Behind creates pathways for under-prepared students CAHSEE
- CALPASS (data sharing consortium) to track student process
- Work closer with community services for training – e.g., fire department, law enforcement
- Partnerships with businesses for training
- Accreditation cycle for self-examination
- Program review and use of instructional technology
- Improve administrative efficiencies
- Use of conferences to learn and development

THREATS

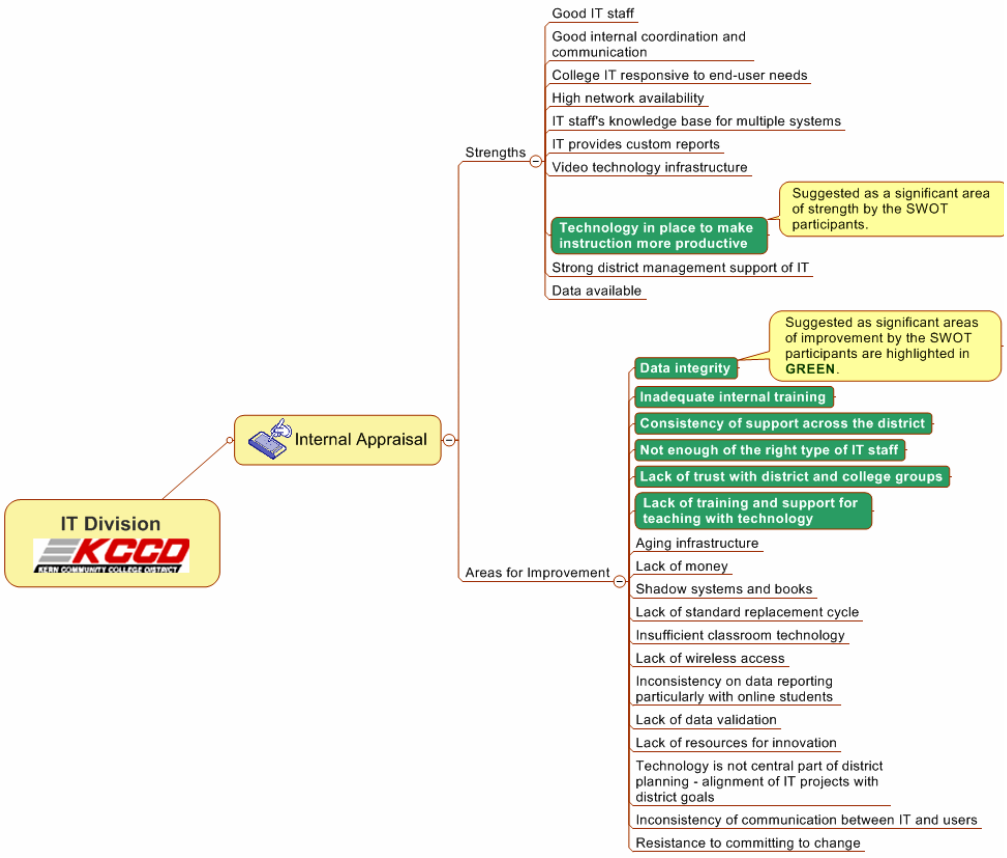
- Increasing student demand and expectation of the technology
- Online and distance education competitors
- IT Security threats
- Rapid of technology change
- Total cost of ownership and return on investment on technology
- Regulatory interventions
- Unfunded mandates
- Compliance reporting
- Increasing population beyond college and district capability
- Microsoft & Vista
- Skill level of staff for technology usage “No Staff Left Behind” cost
- Emergency preparedness for disasters
- State funding policies and predictability
- Expectations from businesses on state-of-the-art technology
- Aging infrastructure
- Enrollment fluctuations
- Public opinion and perception
- Changes in society on how students learn information
- Students and society changing ways they relate to technologies used in

higher education

- Students learning is more hyper-linked and less linear
- Increasing technical divide
- Distributed college environment across large geographic boundary
- Distribute learning across all colleges; can no longer operate in a vacuum
- Societies perception of information value and college's role within that
- Cal State's recruitment of students

Possible Strategies

In a follow-on session, participants were allowed to "vote" on the most significant of strengths and weaknesses. Each participant was allowed one "extraordinary" vote and five "significant" votes that enabled a group sense of the most significant issues. **SEE FIGURE 6 – SWOT ANALYSIS OF ISSUES RECEIVING ONE OR MORE VOTES.**



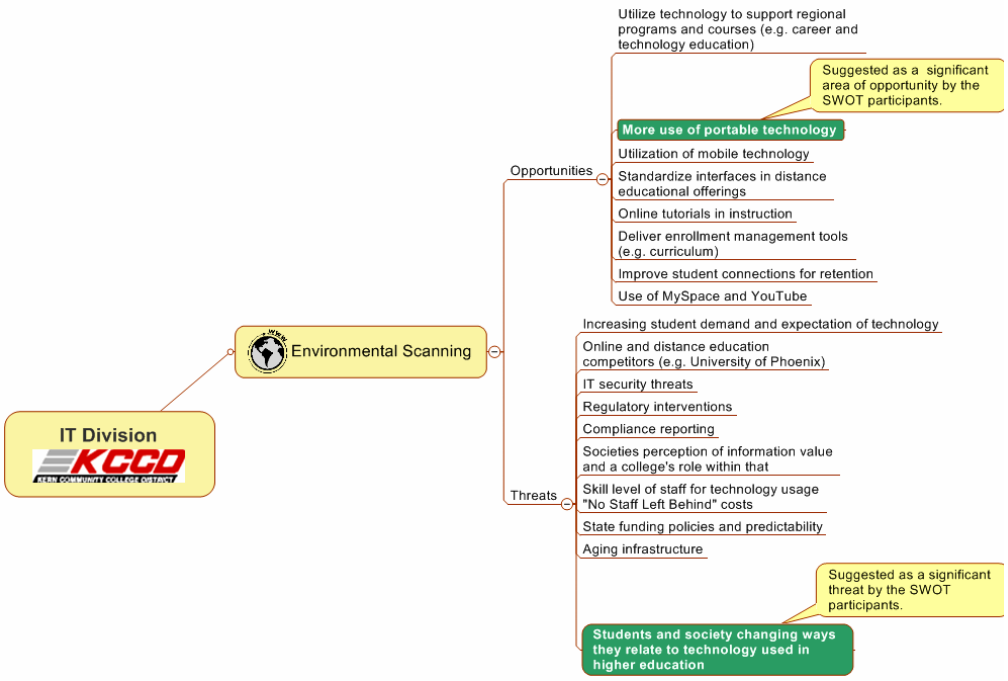


Figure 6 – SWOT analysis of Issues Receiving One or More Votes

The difficulty assimilating the typically lengthy items contained within a SWOT analysis can be contained by two techniques:

- Begin consideration of only the items receiving the most “votes” – e.g. at least one extraordinary vote or at least three significant votes
- Use a SWOT analysis to present these most popular items in a single geometric instance

There are two different approaches for the development of strategy from the SWOT analysis. The first approach attempts to match strengths to pursue opportunities, defend against threats, or to help rectify weaknesses across the SWOT analysis. The second approach develops strategies for the collection of items within each of the four categories. Both approaches should be considered in the Kern Community College District’s next stages of strategic plan development. While the workshop conducted on-site stopped short of discussion possibilities within either approach, examples for each area can be offered to continue deliberations.

1st Theme

By selecting a subset of the high vote issues, several subset "themes" can be derived and represented in cruciform charts. From these cruciform charts, a SWOT analysis can be conducted which may offer some strategies to be pursued. The following cruciform chart sifted significant issues that are specific to IT infrastructure.

Strengths	Weaknesses
- High network availability - Video technology infrastructure - **Technology in place to make instruction more productive**	- Aging infrastructure - Lack of money - Shadow systems and books - Lack of standard replacement cycle - Insufficient classroom technology - Lack of wireless access - Lack of resources for innovation
Threats	**Opportunities**
- Increasing student demand and expectation of technology - Online and distance education competitors (e.g. University of Phoenix) - IT security threats - State funding policies and predictability - **Students and society changing ways they relate to technology used in higher education**	- Utilize technology to support regional programs and courses (e.g. career and technology education) - **More use of portable technology** - Utilization of mobile technology - Standardize interfaces in distance educational offerings - Deliver enrollment management tools (e.g. curriculum) - Improve student connections for retention - Use of MySpace and YouTube

Analysis of the cruciform chart suggests the following strategy:

- Increase the accessibility of IT for teaching and learning by students and faculty

Relevant qualitative, long-term goals underpinning this strategy include:

- Expand network availability to laptops brought into colleges by students
- Support the expanded use of teaching and learning using popular student devices such as iPOD's
- Expand the use of portable computing devices to faculty
- Introduce wireless access in key areas for students and faculty
- Promote the district and colleges with a presence on new social networks including MySpace and YouTube

2nd Theme

The next cruciform chart sifted significant issues that are specific to data usage and training.

Strengths	Weaknesses
- Good internal coordination and communication - IT provides custom reports - Data available	- **Data integrity** - **Inadequate internal training** - **Consistency of support across the district** - **Lack of trust with district and college groups** - **Lack of training and support for teaching with technology** - Shadow systems and books - Inconsistency on data reporting particularly with online students - Lack of data validation - Resistance to committing to change
Threats	**Opportunities**
- Online and distance education competitors (e.g. University of Phoenix) - IT security threats - Regulatory interventions - Compliance reporting - Societies perception of information value and a college's role within that - Skill level of staff for technology usage "No Staff Left Behind" costs - State funding policies and predictability - **Students and society changing ways they relate to technology used in higher education**	- Deliver enrollment management tools (e.g. curriculum)

Analysis of the cruciform chart suggests the following strategy:

- Empower staff with self-service data and expanded IT training

Relevant qualitative, long-term goals underpinning this strategy include:

- Expand the use of self-service data access through portal technologies, web access and data warehouse tools
- Expand the use of data-driven planning
- Introduce “anytime – anywhere” training for all staff on current and emerging

IT topics

- Expand the use of enrollment management tools to increase student enrollment

3rd Theme

The next cruciform chart sifted significant issues that are specific to IT staff and management processes.

Strengths	Weaknesses
- Good IT staff - Good internal coordination and communication - College IT responsive to end-user needs - IT staff's knowledge base for multiple systems - Strong district management support of IT	- **Inadequate internal training** - **Consistency of support across the district** - **Not enough of the right type of IT staff** - **Lack of trust with district and college groups** - **Lack of training and support for teaching with technology** - Lack of resources for innovation - Inconsistency of communication between IT and users - Resistance to committing to change
Threats	**Opportunities**
- Increasing student demand and expectation of technology - IT security threats - Skill level of staff for technology usage "No Staff Left Behind" costs - State funding policies and predictability - **Students and society changing ways they relate to technology used in higher education**	- Utilize technology to support regional programs and courses (e.g., career and technology education)

Analysis of the cruciform chart suggests the following strategy:

- Evolve the quantities and skills sets of IT staff and management to improve and appropriately expand services to all stakeholders supporting the mission of the colleges and district

Relevant qualitative, long-term goals underpinning this strategy include:

- Introduce training for IT management and staff on emerging issues such as security, mobile technologies, wireless, etc.

- Track consistent and complete metrics on equipment and users to derive a formula for allocating the appropriate types and number of IT staff within the district and college
- Introduce new staff positions where volume of work necessitates the addition of dramatically different skill sets

Service Delivery Measurement / Customer Satisfaction

District Office

During March 2007 a survey was conducted to assess service levels and user satisfaction with college and district IT departments. Full-time faculty, adjunct faculty, classified / confidential staff and management were randomly selected to participate in the survey.

The purpose of the survey was to:

- Measure the satisfaction and importance of college and district IT / IS services at baseline
- Inquire which additional or improved services would be most valuable
- Give users a voice to influence college and district IT / IS service priorities and potential initiatives

Methodology

The online survey was distributed to approximately 500 randomly chosen users of college and district IT / IS services. College and district IT / IS staff were excluded from participating. The following table represents a summary of the population and sample size estimates.

Campus	Position	Number of FT		Rev FT		Sample	
Bakersfield College	Classified	206		188		124	
Bakersfield College	Faculty	255		254		144	
Bakersfield College	Mgmt	24		24		14	
Bakersfield College Total		**485**	**58%**		**58%**		**56%**
Cerro Coso	Classified	64		61		40	
Cerro Coso	Faculty	70		70		47	
Cerro Coso	Mgmt	12		12		7	
Cerro Coso Total		**146**	**17%**		**18%**		**19%**
District	Classified	39		34		18	
District	Mgmt	18		17		8	
District Total		**57**	**7%**		**6%**		**5%**
Porterville	Classified	59		55		39	
Porterville	Faculty	82		82		55	
Porterville	Mgmt	6		6		4	
Porterville Total		**147**	**18%**		**18%**		**20%**
Grand Total		835		803		500	

Campus	Position	Number of FT		Rev FT		Sample	
Bakersfield College	Classified	206		188		124	
Cerro Coso	Classified	64		61		40	
District	Classified	39		34		18	
Porterville	Classified	59		55		39	
Classified Total		**368**	**44%**		**42%**		**44%**
Bakersfield College	Faculty	255		254		144	
Cerro Coso	Faculty	70		70		47	
Porterville	Faculty	82		82		55	
Faculty Total		**407**	**49%**		**50%**		**49%**
Bakersfield College	Mgmt	24		24		14	
Cerro Coso	Mgmt	12		12		7	
District	Mgmt	18		17		8	
Porterville	Mgmt	6		6		4	
Mgmt Total		**60**	**7%**		**7%**		**7%**
Grand Total		**835**		**803**		**500**	

The survey spanned a range of topics including:

- Information Technology Services
- Instructional Technology Services
- Help Desk Services
- Network Services
- Portable Technology
- User ID, Passwords and Privacy
- Demographics

The survey was designed through a collaborated effort with KCCD and administered by SunGard Higher Education to ensure objectivity and confidentiality.

Where “other” freeform comments were requested, these have been cut and pasted exactly as entered with no corrections to spelling, grammar or punctuation.

Highlights

There was an interesting mix of responses to the satisfaction with several IT services. Among the highest scores was Internet services. The lowest average response was training which corresponds with many of the findings during the assessment phase.

Spam proved to be the most significant concern among IT issues. The use of a variety of portable computing devices was significant.

There was a large selection of help desks that are referred to when assistance is required. While most scored reasonable satisfaction rates their frequency of use appears to be low. The resolution rate for problems showed some significant duration.

By far the most interesting outcome was on the topic of IT security in questions 25 through 29. Half of all respondents use a common password for different logon applications; however, the majority of users change these passwords infrequently. Enough users share passwords or write them down for to pose a significant risk. Finally, there is significant storage of confidential or sensitive information to portable devices.

The survey intends to provide baseline measurements on overall satisfaction with IT services within the district. Its annual use should provide continuing data as to the improvement in key service areas as well as the emergence of new concerns and issues.

High Satisfaction Scores
The 2007 survey highlighted some service competencies recognized by the KCCD community.

Category	Score Scale: 1 - 5
Help Desk courteously	4.60%
Help Desk treated in a friendly manner	4.55%
Help Desk patiently	4.52%
Help Desk Professionalism	4.40%
Help Desk customer oriented	4.22%
Internet access from College / District office facilities	4.21%
Help Desk ability to solve your problems	4.19%
College web site services	3.94%
College Web Site Services	3.94%
Library technology	3.88%
Outlook eMail and related services	3.86%
Banner Web	3.79%
Telephone	3.74%
Computer Labs Workstation Availability	3.70%
PC and printer support	3.69%
District Web Site	3.67%
Computer Labs Software Availability	3.64%
Video Conferencing for Conducting Meetings	3.60%
Online Course Management System	3.58%

Opportunities for Improvement

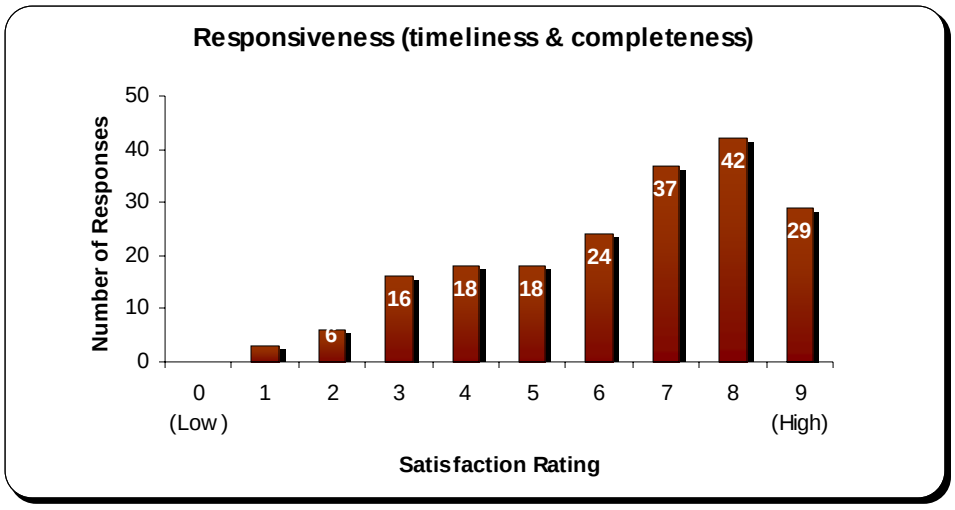
Category	Score Scale: 1 - 5
Training	2.90%

Survey Results

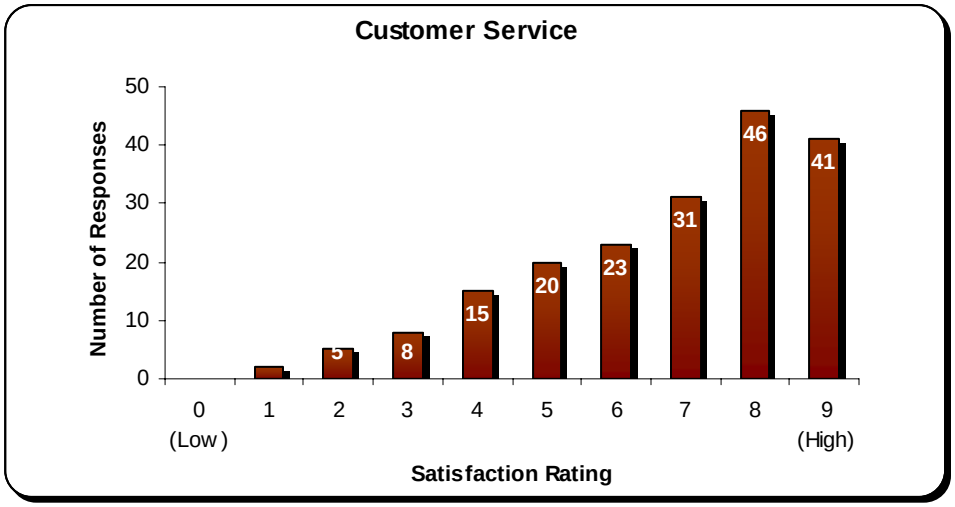
Information Technology Services

1. Using your impressions of College and District IT departments please rate the following:

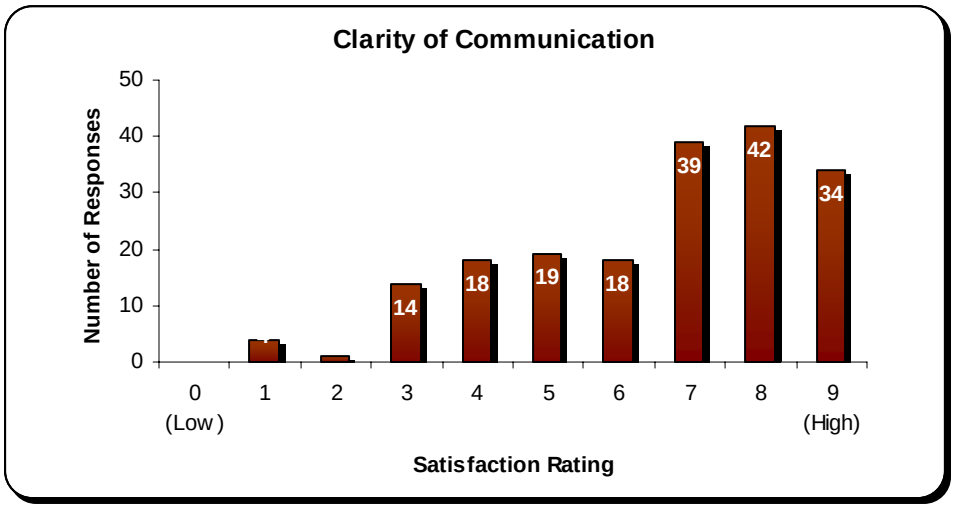
QUESTION 1A = RESPONSIVENESS
AVERAGE SATISFACTION RATING 7.35
TOTAL RESPONSES 193 OUT OF 194



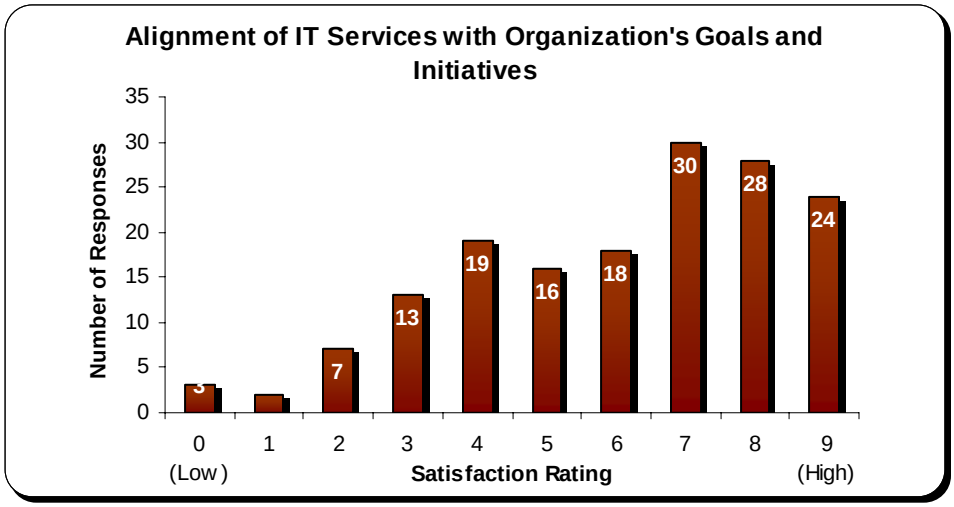
QUESTION 1B = CUSTOMER SERVICE
AVERAGE SATISFACTION RATING 7.74
TOTAL RESPONSES 191 OUT OF 194



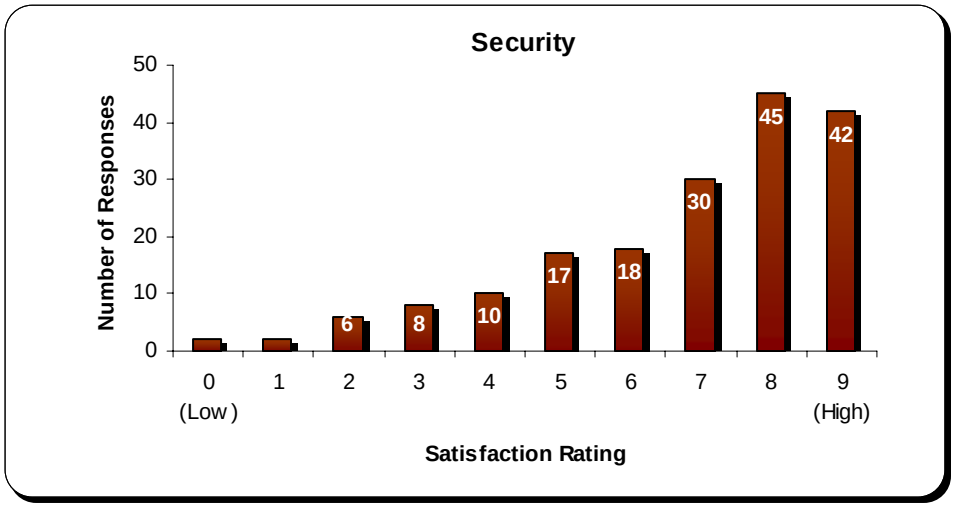
QUESTION 1C = CLARITY OF COMMUNICATION
AVERAGE SATISFACTION RATING 7.55
TOTAL RESPONSES 189 OUT OF 194



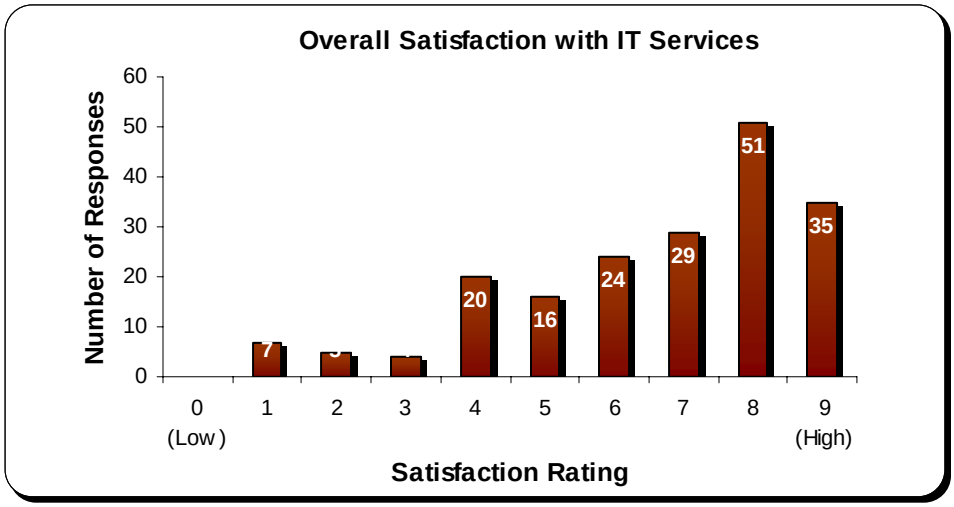
QUESTION 1D = ALIGNMENT OF IT SERVICES WITH ORGANIZATION'S GOALS / INITIATIVES
AVERAGE SATISFACTION RATING 7.06
TOTAL RESPONSES 160 OUT OF 194



QUESTION 1E = SECURITY
AVERAGE SATISFACTION RATING 7.77
TOTAL RESPONSES 180 OUT OF 194

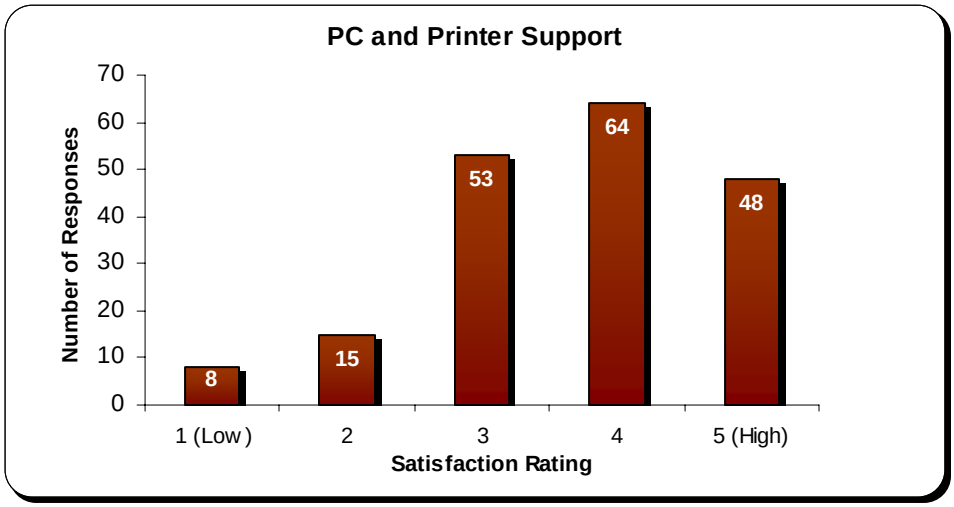


QUESTION 1F = OVERALL SATISFACTION WITH IT SERVICES
AVERAGE SATISFACTION RATING 7.59
TOTAL RESPONSES 191 OUT OF 194

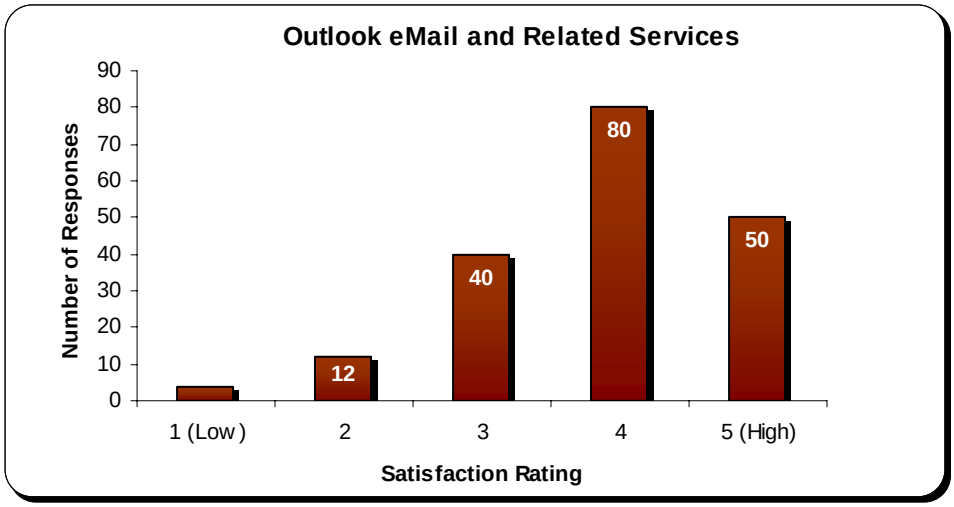


2. How satisfied are you with the following IT service offerings?

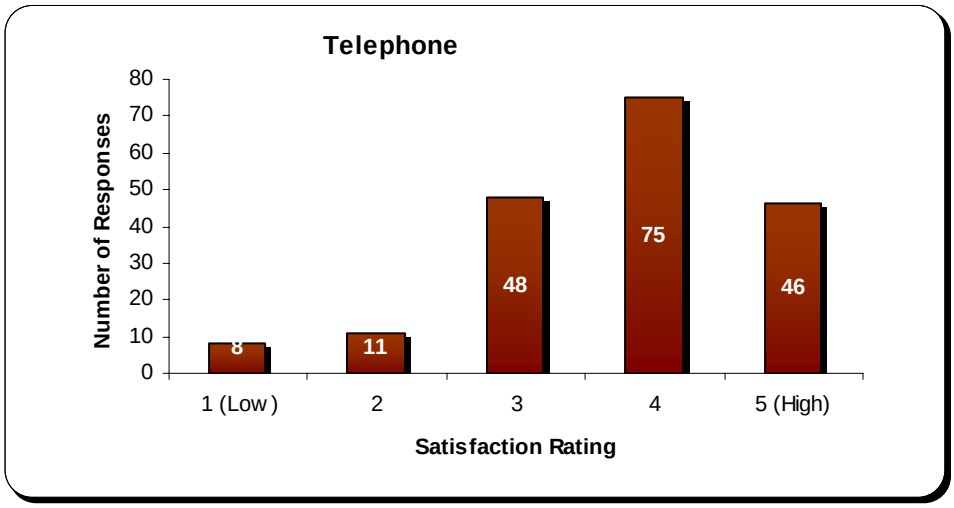
QUESTION 2A = PC AND PRINTER SUPPORT
AVERAGE SATISFACTION RATING 3.69
TOTAL RESPONSES 188 OUT OF 194



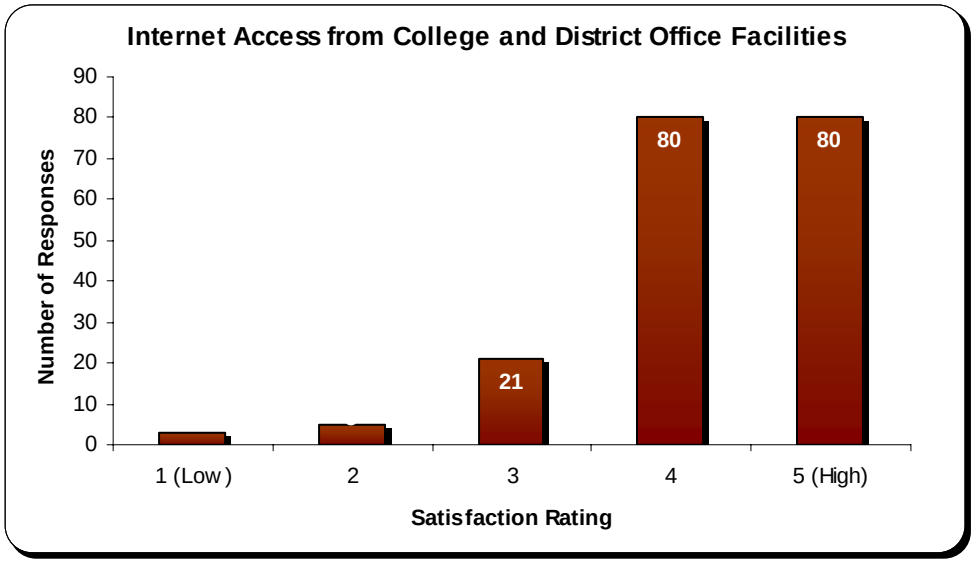
QUESTION 2B = OUTLOOK EMAIL AND RELATED SERVICES
AVERAGE SATISFACTION RATING 3.86
TOTAL RESPONSES 186 OUT OF 194



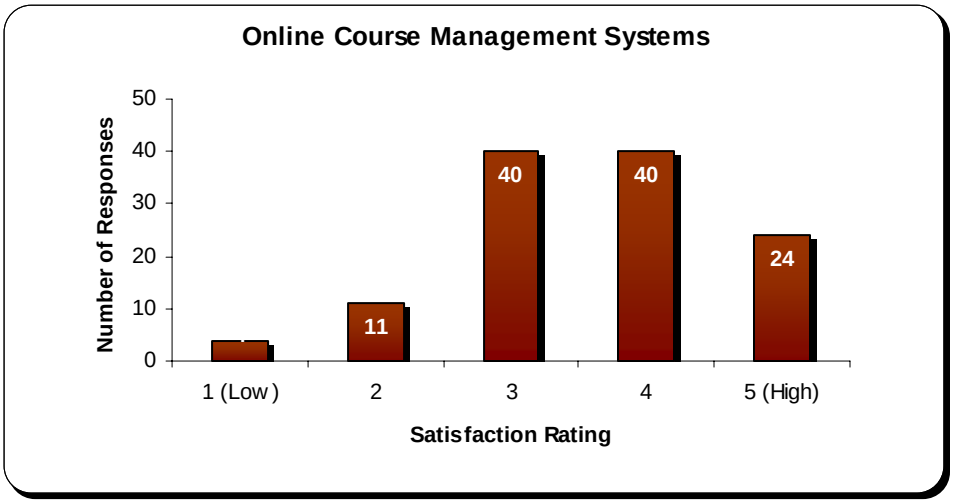
QUESTION 2C = TELEPHONE
AVERAGE SATISFACTION RATING 3.74
TOTAL RESPONSES 188 OUT OF 194



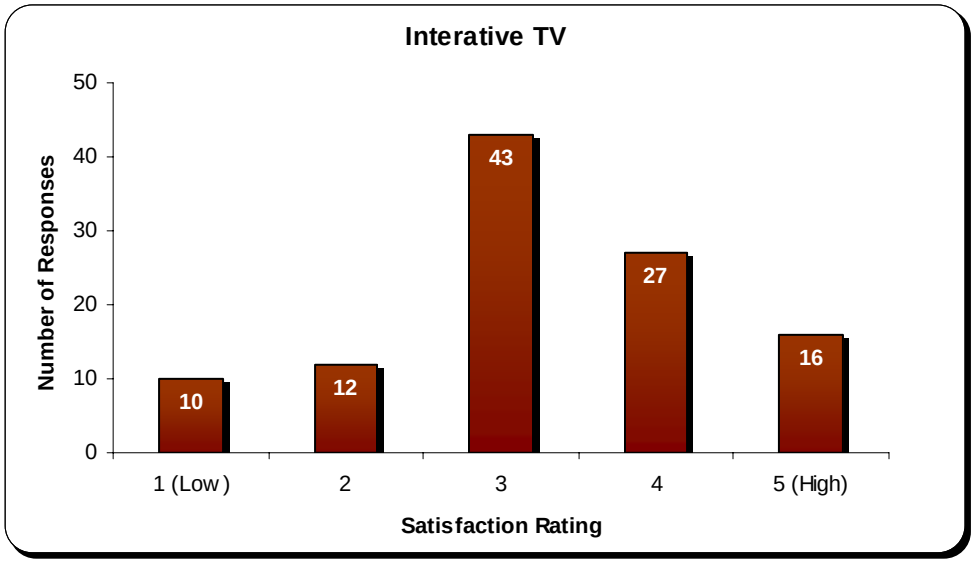
QUESTION 2D = INTERNET ACCESS FROM COLLEGE AND DISTRICT OFFICE FACILITIES
AVERAGE SATISFACTION RATING 4.21
TOTAL RESPONSES 189 OUT OF 194



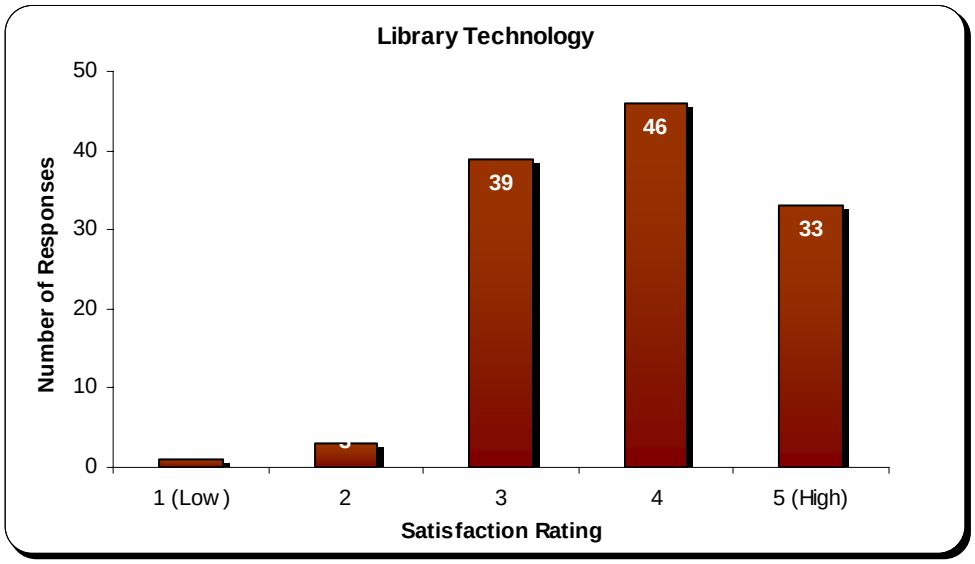
QUESTION 2E = ONLINE COURSE MANAGEMENT SYSTEMS
AVERAGE SATISFACTION RATING 3.58
TOTAL RESPONSES 119 OUT OF 194



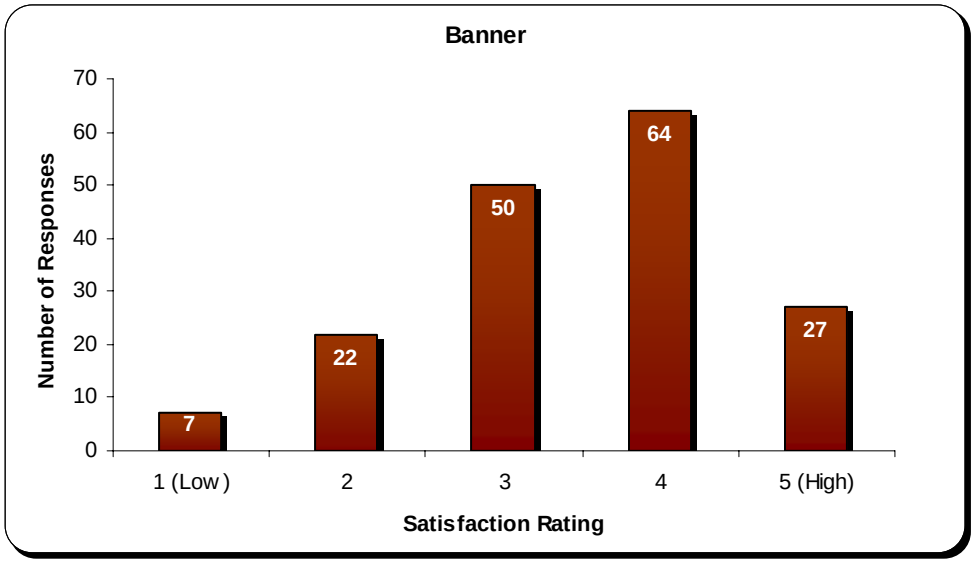
QUESTION 2F = INTERACTIVE TV
AVERAGE SATISFACTION RATING 3.25
TOTAL RESPONSES 108 OUT OF 194



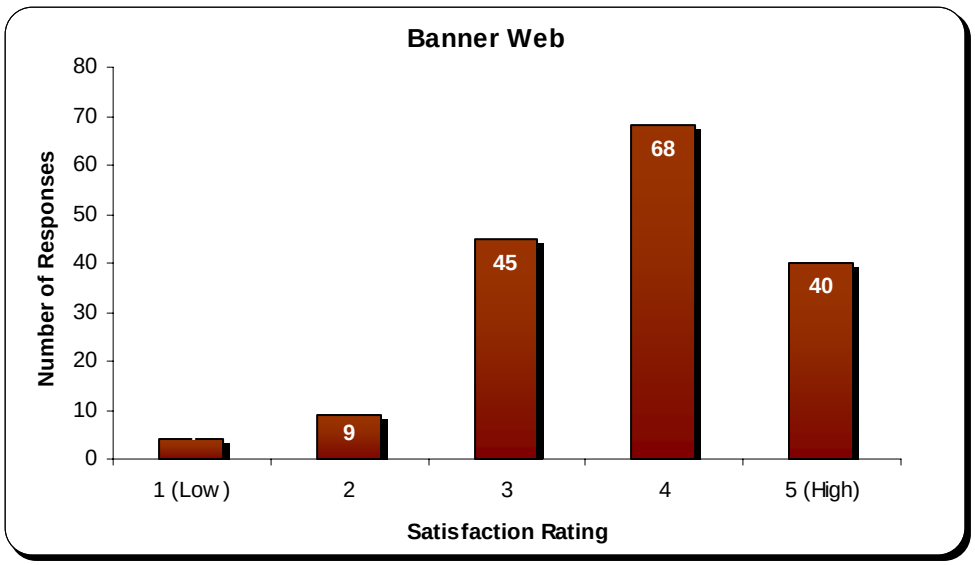
QUESTION 2G = LIBRARY
AVERAGE SATISFACTION RATING 3.88
TOTAL RESPONSES 122 OUT OF 194



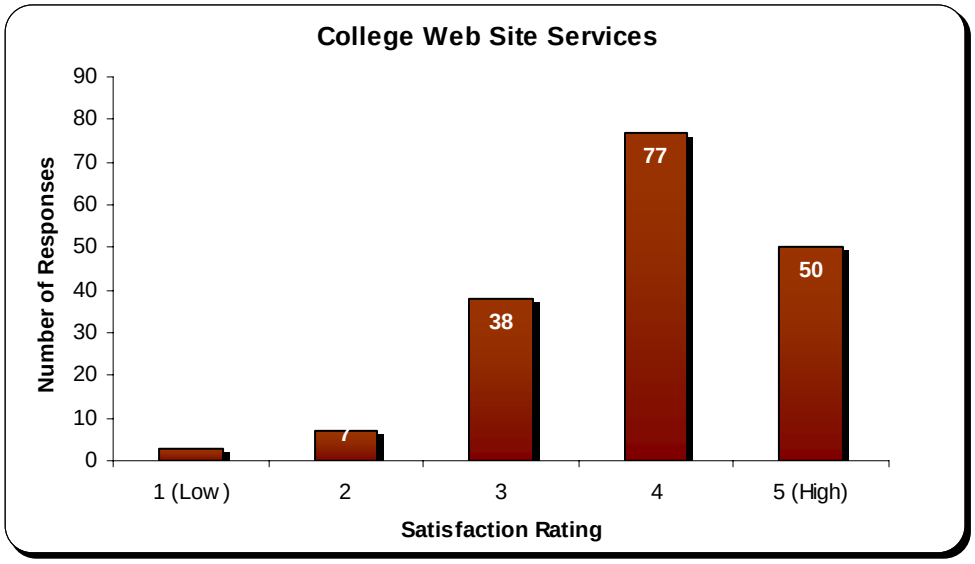
QUESTION 2H = BANNER
AVERAGE SATISFACTION RATING 3.48
TOTAL RESPONSES 170 OUT OF 194



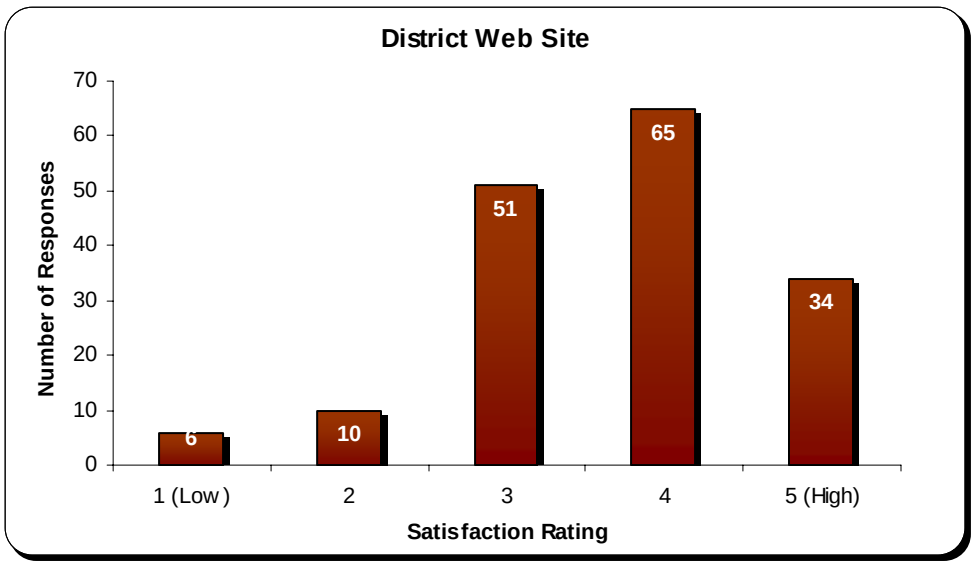
QUESTION 2I = BANNER WEB
AVERAGE SATISFACTION RATING 3.79
TOTAL RESPONSES 166 OUT OF 194



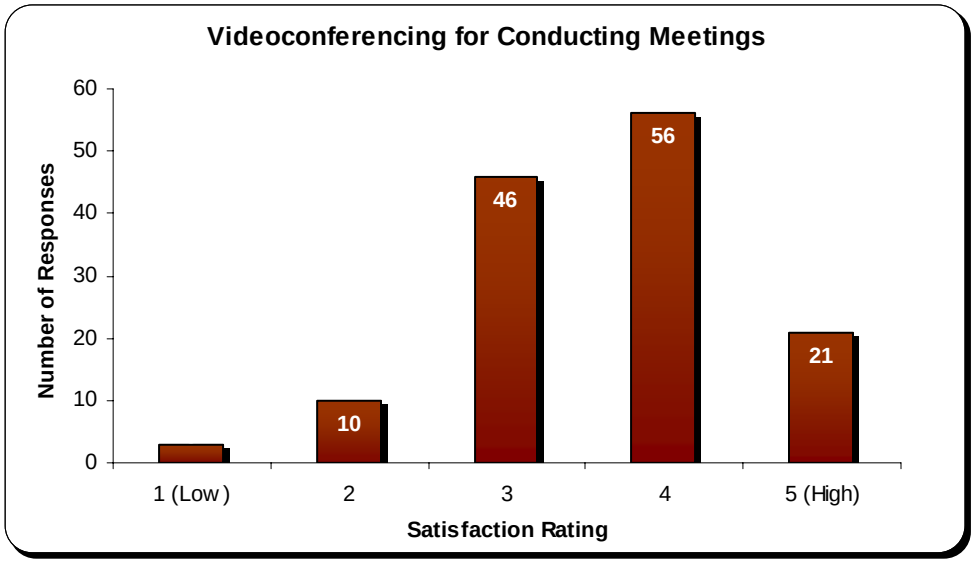
QUESTION 2J = COLLEGE WEB SITE SERVICES
AVERAGE SATISFACTION RATING 3.94
TOTAL RESPONSES 175 OUT OF 194



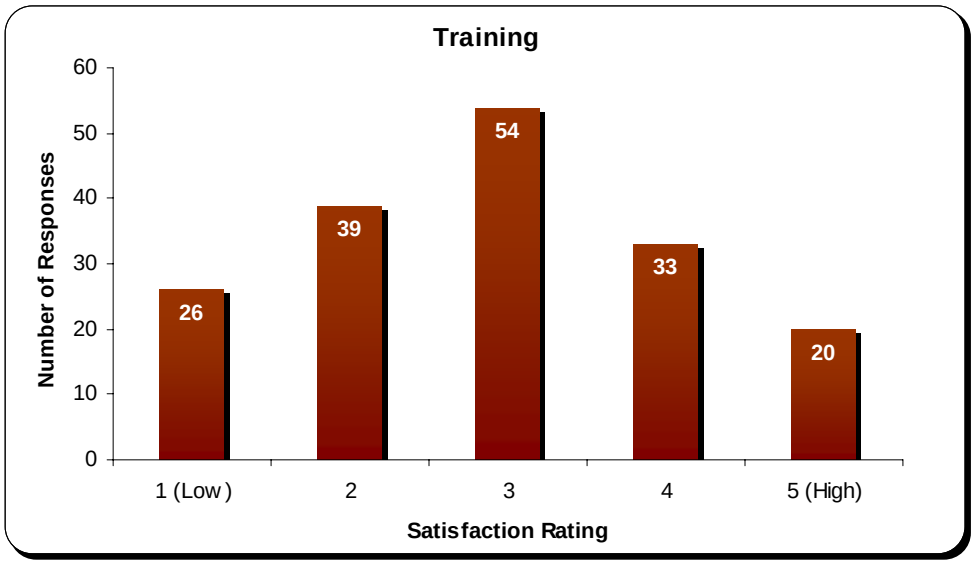
QUESTION 2K = DISTRICT WEB SITE
AVERAGE SATISFACTION RATING 3.67
TOTAL RESPONSES 166 OUT OF 194



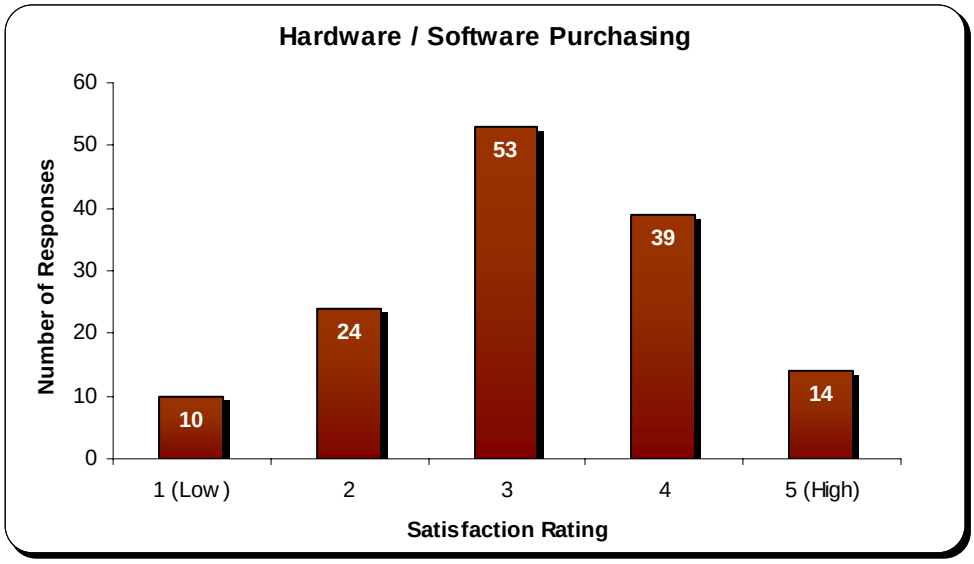
QUESTION 2L = VIDEOCONFERENCING FOR CONDUCTING MEETINGS
AVERAGE SATISFACTION RATING 3.60
TOTAL RESPONSES 136 OUT OF 194



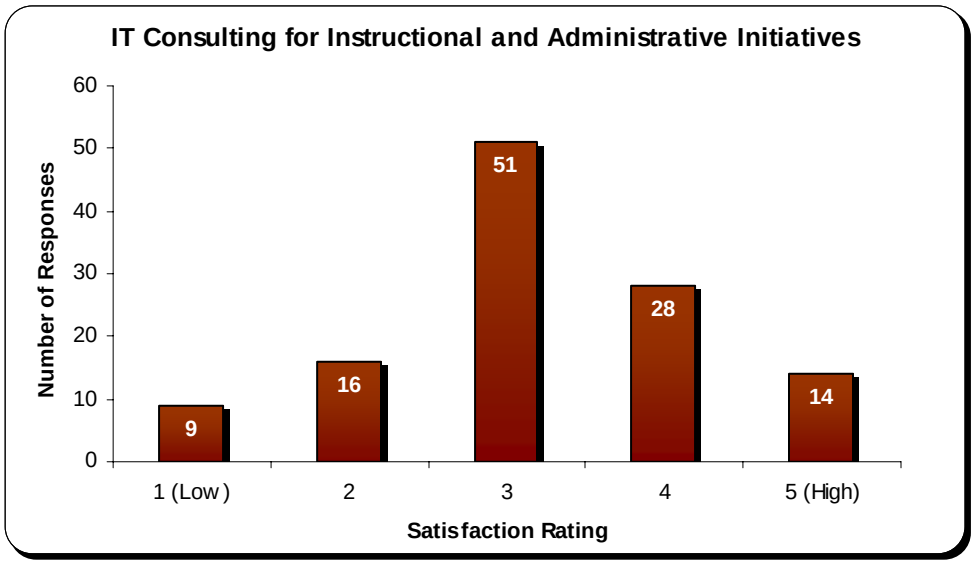
QUESTION 2M = TRAINING
AVERAGE SATISFACTION RATING 2.90
TOTAL RESPONSES 172 OUT OF 194



QUESTION 2N = HARDWARE / SOFTWARE PURCHASING
AVERAGE SATISFACTION RATING 3.16
TOTAL RESPONSES 140 OUT OF 194



QUESTION 2O = IT CONSULTING FOR INSTRUCTIONAL / ADMINISTRATIVE INITIATIVES
AVERAGE SATISFACTION RATING 3.19
TOTAL RESPONSES 118 OUT OF 194



3. Please describe what would increase your satisfaction with the IT service offerings? TOTAL RESPONSES 115 OUT OF 194

- Serious attention needs to be paid to the network on our campus. The network is very, very slow, and sometimes non-existent in my office. The phone system is antiquated and cranky. I would like some sort of automated computer station replacement policy in place, so that we do not have to beg for money to replace computers in our instructional labs.

- For one, on this survey there should be an 'N/A' selection - there are MANY of these things I have not got experience with, and so I selected 'average' to mean 'N/A'

- Our college IT dept is completely unable to support the needs of our instructional dept, they don't enough personnel, the lack training, there is no budget for recurring costs of ownership. Our IT Dept has been in a death spiral since 2000 and is now completely unable to support the instructional needs of our dept (Media Arts). I think that it is clarifying that we have mission critical needs to be met that aren't even on the list to be prioritized in number 4 below.

- I was more comfortable with the previously eMail format from at home before we went to Outlook. Individual e-mail messages often open automatically, though I might manually want to simply delete an e-mail that looks suspicious. I would hope more training and staff would be provided for such training. We are limited on the amount of training that can be given. The recent change to the phone voicemail system seems a little slower that the previous system offered for purposes of retrieval. When networked printers go down, the problem is usually not reported immediately. Some print jobs sit 'in limbo' for long periods of time before people realize from a remote location that there is a technological or mechanical problem. It works out a little bit like 'out of sight, out of mind'. Often these networked printers are in a location with no one overseeing its function (or lack thereof). Some of the points above have been left blank since I may not have personal experience with certains items being asked for.

- Faster response time when critical networking is needed to teach a class. If the IMAP address is changed, an email should be sent BEFORE the address is changed, not AFTER!

- More printers and get rid of Banner. It is messing up our course offerings and interfering with our ability to offer certain classes.

- The upgrade to the phone system was not an improvement. The sound quality of recording is poor, it is not user friendly, and I'm sick of having my password expire. We can no longer tell if a call is coming from on or off campus (a feature of the old version)and there are often glitches in the answering system.

- PC support is excellent. Printer support is ok. It is probably not the fault of IT, but employees need toner for their printers. IT use to support toner too. I

wish we could go back to the good old days. The hub is a real pain to retrieve jobs across the building. It slows down speed and efficiency my area. Banner support is great. It appears to be out of date in function, even the new Banner 7.3, because a lot of the functions added in the beginning are archaic and clumsy. For example, in SEADTL, the choice list has A-Z choices when people only use about 5 of them. Any obsolete information ought to be deleted and the rest streamlined for modern use. Things have changed a lot since the beginning of Banner, now that everything is 'online'. More importantly, the data gathered in banner would be best served by putting results in ban web. For example, all the transcripts that have been evaluated in SHATATR would be easier to view in ban web. Also, the matriculation function that we use internally, ought to be available for viewing in each student's record so that the student can see if they have completed Orientation, Assessment, Counseling, and the SEP. It's great information, just not in the right place to help students. There may be more functions in banner's database that would be even more valuable transferred to Ban Web.

- Additional funding for: *Additional IT staff A*vances in technology *Training: Skills and communication

- More training. More timely responses (i.e. more support personnel to do the work). Better usability in BannerWeb and Course Management Systems. Better support and designated personnel for iTV.

- if more training were available for staff as new products are available

- response time in repairs. my 'D' drive has been broken for over 6 months and still is not fixed.

- Improve the process for evaluating accessibility to electronic and information technology. (dept. websites, instructor websites, online curriculum and information, etc.) Although this is not just the responsibility of IT, they are part of the process. Increased and improved training for faculty and staff.

- Hire more qualified people. Make communication regarding downtime/changes more accessible. For example, the change of exchange server addresses was sent out in an email. Those of us who weren't on campus during break had no way of getting the new address. It could have been listed on the IT website. Or, employees could have been told that they had to log in to the system on campus to get the new address. Make support available for labs in the evenings when we teach classes and use the labs.

- Wireless access for teaching online from home.

- Preview and input sessions before software decisions. All pros and cons of the depth of the software and to what capacity it can hold.

- The college IT depaartment is great. The problem is that it is severly understaffed. The district IT is unresponsive and very difficult to reach. We

wait for more than a month to have a LCD bulb changed.

- To have better support for the CBORD ID System
- Faster service.
- Responsiveness and completion of job related systems at the college level. It is rediculous how long it takes to get a job accomplished. I put in an order through help desk in April and it was not completed until the end of February. This was a work stoppage issue and they could have cared less.
- Improved responsiveness and attention to expressed needs.
- Training, training, training in Banner! Not enough training is done at the campus levels, in my opinion.
- Better equipment and more training.
- more training..... Note: some questions above are not relevant and are services are not used.....should be a section that indicates: not applicable.
- There is an assumption that everyone understands everything. Those of us trying to keep up with changes are often left behind. There needs to be some kind of ongoing informal support system. Clark Parsons tries to fill that role in addition to everything else he's expected to do.
- Fewer times without email access.
- Regular opportunities for training on various capabilities of Banner.
- a quicker turn around time between reporting a problem and having someone respond would increase my satisfaction.
- Banner Training and have someone who can create reports from banner when requested without having to beg for them.
- Faster banner system, more training. Spam and amount of storage for outlook messages.
- Be able to run more reports myself.
- More availability for videoconferencing. Accessing the new outlook from exchange is more cumbersome, and trying to open attachments can be a pain.
- Our students need wireless Internet access while they are on campus. It should be available from most locations on campus. The faculty computers are very old. A replacement cycle should be established and FOLLOWED. Attemps have been made to limit spam but the present soulutions seem marginal.

- Everyone should get new computer hard. Not just a few.
- Telephone System is difficult and confusing.
- Increase Internet connection speed in Mammoth. There needs to be a software/hardware upgrade replacement plan.
- ..Campus meeting on status of current Banner problems and/or get input from end users on what some of the problems are ..need to increase the speed of Banner usage
- Need interactive whiteboards for use on campus; need new updated computers; what training??; purchasing??
- Faster response time. Getting more answers.
- Training, getting banner to run effectively, especially during peak usuage
- More detailed banner training
- Give all instructors a laptop instead of a desktop.
- It seems we use too many consultants. We should train our own staff and utilize them as resources.
- Quicker service. It seems as if our IT staff is overloaded. They serve the entire BC campus and are often working on another problem elsewhere on campus when you need them. submitting an online work order is even slower and less responsive. Since we have become so dependent on computers to do our jobs, it is imperative that an problems which impede workflow be immediately solved. Also, we are behind the times when it comes to students' needs. Why don't we have wireless Internet access? Other colleges have managed to resolve the security issues.
- Quicker response times at the college IT level. Current staffing is low so that is to be expected, but this occured when fully staffed. BanWeb is very slow, making completion of work extremely frustrating. BanWeb training is very lacking. The trainer is not very knowledgable in all aspect of Banweb. Most questions are answered through other staff, or through trial and error.
- Responsiveness. Staff support for interactive TV I don't know if I'm dissatisfied with Banner or with the lack of a customer service attitude from the staff, data crunchers who use Banner
- Clear communication, efficiency, a comprehensive plan that is communicated to the faculty and staff.
- More budget available for IT
- Local techs be more responsive to the needs of professors. I personally have had rude remarks made to me by Chris a tech on campus at PC numerous

times.

- Better safeguards against spams, junk e-mails. Better coordination between District IT and campus needs such as certain reports/data needed and meeting timelines of requests. Improve access to my entire workstation workstation (as if I'm working from my office) from anywhere else as long as there is internet connection.
- more timely upgrades of machines. can't call cell phone numbers from my office.
- Easier Banner access so we don't have to close one screen to get to another. ALL accessed info needed by individual should be all on one page
- More support staff (network administrators and network technicians). Banner is cumbersome at best and results in holding the organization 'hostage' to a perceived inability to provide data. This problem may be a function of a lack of training. It may also be a matter of a sort of messianic zeal typical of most IT staffs to view any question about access to MIS data as a breach of security.
- More modern equipment. More training.
- IT is doing an excellent job, particularly since I now have a laptop computer in my office.
- I am still waiting for the computer and flat screen that I was told I was on a list for 2 years ago when I first arrived. My computer is a dinosaur---many difficulties!
- Better equipment and more timely service
- Overall, I am pleased with what IT offers however, the area which has decreased over years is that of telephone maintence. When there is a problem with the telephone, I feel that IT is not as timely in follow up with telephone matters.
- reports and downloading of financial aid information in a timely manner with out errors.
- To find a way to get rid of schedule+ and work directly with banner regarding scheduling.
- Because I am very satisfied with the offerings I use, the only thing that might increase my satisfaction would be to increase the number of IT individuals available on the campus. Our guys are really great;it is just that sometimes they are stretched a bit thin because of the campus demands.
- Many of the above do not apply to me or I have never used some of those services, but the most important thing you can do increase mine and everyones elses satisfaction is to hire more help. The people you have here

at the IWV campus are wonderful but they are spread way too thin as is everyone else on this campus.

- List of offerings meets and exceeds needs.
- Even if the problem is minor, for example, the computer is running slow. I would like IT to look at it, fix it and don't wail until computer is out of commission and all is lost due to the thinking the user is the problem. We could be the problem, in not reconizing what is our fault and what is the computers fault with it running slow.
- Individual color printers
- As a new employee, being more aware of potenialities of system capabilities; some sort of suggested training of how/why/when to use specific aspects of IT.
- Application training
- Allowing access to internet with my personal computer through campus wireless system. Most colleges allow faculty and students to access campus wireless systems. We are moving backwards because of district paranoia. Any negative choices above are because of district IT. My campus IT people are the best!
- It's mostly a speed of response issue. This does not imply a slow work rate, but more likely to be due a very high work load.
- Specific person to contact for each campus. This gives one point for all problems. The contact person could then route the problem to the correct person.
- WiFi on campus and at the Weill for those of us who need to use our laptops would greatly increase my satisfaction with IT. However, it's hard to criticize IT, at BC or the district, simply because it is a massive job and overall they do a terrific job addressing questions and problems that arise.
- I think the main training of users (outside of banner) is done through BC prof development center and not part of IT
- More timely assistance, more training, more support personnel, more guidance for equipment utilization, district committment to improving services
- I would like to see basic training sessions done each semester on the various technological equipment/software available in the classroom or administratively, whether it be existing equpment/software or newer equipment/software. This training would be open to staff and instructors alike. Visual aids on the equipment would be helpful after the training session to have on hand throughout the semester to refer to. The training needs to be done to refresh memories, especially if you use the equipment infrequently during the semester.

- more currency with computer hardware and software for faculty
- Completion of IT service requests would increase my satisfaction. The problems are usually assessed in a timely fashion but resolution of the problem is usually never completed. I've been waiting for probably four months for resolution to some problems.
- more trainings in relation to up grades of software. Information on IT services available. Timely response on IT questions or problems.
- Staffing levels seem to be low, people are 'spread too thin'.
- Increase in Network Technicians. It is difficult to keep Network Technicians at the College due to the workload and sometimes staff's interaction with Technician is somewhat unappreciative. Everybody is frustrated because their computer is not working,and as a result, creates bad ineraction between the two.
- input from the actual or end users as to major software evaluation and purchases instead of unilateral decision at the district level...get users in on the decision making
- They need to hire more personnel to handle the work load.
- Office printers would be great. More banner training on budgets.
- I think we need a wireless connection on campus; other campuses are able to resolve security issues, so I cannot understand why we can't. Communication is often a problem: questions aren't always answered via phone or email. (Foor example, sometimes passwords are changed without notifying faculty who use computer classrooms.) Sometimes other changes are made to services without adequate explanation, i.e. our off-campus access through exchange this winter. Our new email/spam protection is a mess. We often wait a long time for service. Our IT service needs to be immediate when we are so dependent on technology. (The appear to be over worked.) When work is done on our computers, we need to be notified. Changes were made over winter break that has caused some 'permanent' changes and we were not even notified that work was going on. Software that previously was installed is still not working on the affected computers after 7 weeks.
- Keeping us informed with the latest upgrades on our computers and training along with it.
- Overall I feel the service is already good but I also think planning for future needs is fairly important at this time. To maintain a technical edge we need to make sure all faculty and staff have up-to-date technology at their workstations. I believe that something needs to be put into place that allows the loading of software programs onto office computers that does not require an IT person's support.

- Campus IT seems responsive to my needs. District IT seems to have the attitude that the campuses support them, not the other way around as it should be. More consultation with campuses prior to committing to and implementing new systems.

- Better blocking of spam, particularly sexually-oriented messages that manage to get through filters no matter what IT tries. A college website with a better search engine. A more efficient e-mail system that filters messages into folders, so some automatically can be deleted. It's crazy that we have to spend time deleting messages, and then must delete those we just deleted. Overall, I think IT does a fine job with the limited resources budgeted for it. We want everything, but the district doesn't allocate the people, equipment, software, or training needed to work on concerns. For example, I believe that the online registration process at BC could be streamlined, but finding a person to work on this with admissions is difficult due to IT's tremendous workload. I envision IT as the old stadium, slowly crumbling away until a massive bond measure was passed. Why don't we fix things now?

- Training at times I can attend seems to be missing this year. I teach labs so most afternoons are not available for me. Friday mornings are available. In the above list of questions there should be place for a 'not applicable' answer. For example, I have never used videoconferencing so I gave it a 3 response.

- I need a printer closer to my work station: I use to have one until IT decided we didn't need to complete our work - I share with 14 people - Now I have to print every page and walk many steps to retrieve my document or else it disappears - this is a big problem when I work on large documents as most of mine are - time and effort wasted on walking to the printer. Help desk is great - Training is something to be desired. Not enough help in technical support.

- Faster response time to help desk requests.

- We need in depth workshops for staff training in Excel, Word, and Outlook. Advanced outlook features. Not just a 2-hour training and that's it. Perhaps 1/2 day. I don't like on-line help tutorials. Also, IT should be providing all staff with a publication of Excel training, etc.

- This survey should NOT combine College AND District IT - they are two separate areas and provide different services... Also, this survey should have been run through a spell-check program ('InteraCtive TV'). KLT/BC

- Training on Banner, Inform Help Desk if changes have been made so they can forward the message if you call. Don't have a person on Help Desk that really can't help you much or really don't want to take the time to help or don't know how to help.

- I think the attitude of the campus IT would help soften any inconvenience I may have with the time it takes to get my repairs or assistance. An

additional person may be helpful also.

- Timely responsiveness Proactive planning and action keeping processes simple
- More staff at my college.
- Faster service and training in Banner Web
- Making certain there is improved communication between District and the campus IT divisions
- A more consistant treatment of Campus / District employee needs. More required training on basic business software (ie MS Office) with bench marks to show completion. Increasing the confidence and skill of the employee (classified, faculty, & Administration) would bring better quality and accuracy to the colleges and district.
- I'd like to see more training offered for the programs we utilize. Consider purchasing Adobe Acrobat for use by all staff and faculty.
- Our college IT service has improved in the last 8 months but see the need for additional position to cover that department.
- I wish that Mackintosh computers were available as an option for those of us who use them at home.
- We just need more people. We need better budget support for purchasing. We need to seriously look at if ITV is worth the costs going in to it. As a 3 college district, we need to be using video conferencing more not less. I am not really able to discuss District level support, because I rarely use it.
- More information regarding the online courses needs to be communicated to all staff. We need to be knowledgeable so this can be communicated to our personal network.
- Clear description of what they service and what training is available to staff.
- Update faculty equipment to handle current software and program demands.
- More printers, less sharing = more productive
- Banner Web needs some fixing
- I think it would be helpfull to be provided with Banner training at the very least, annually. Testing new upgrades is ok but if you don't take/make the time to do it you would learn it if specific training sessions were offered.
- A larger budget for IT equipment.
- Wireless - More innovative planning, better and more explicit connection

between district-wide strategic planning initiatives and technology plans. Better emphasis on training and instructional best practices for faculty. Better support for faculty and staff innovation and initiatives through programs such as mini grants for projects, course development and other new ideas.

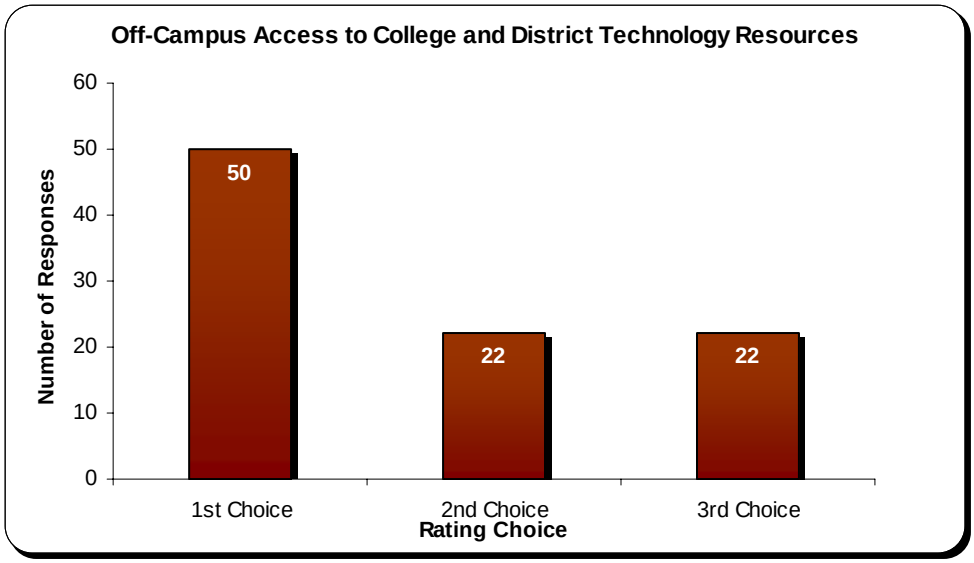
- Improved ITV audio.
- My computer is pretty old at this point, and it takes a long time to 'wake up' each morning. A more current school computer would be nice. I do wonder how much longer my office computer can hold on at this point.
- more training availability for instructor web pages. I would like to have a web page. I teach at COS too and I am able to use Blackboard to post all of my classes even though I do not teach an online class at this current time. They have also linked the faculty to @ONE for free training.
- Network in Fine Art building is slow, IT has failed to remedy the problem

4. Please select in order of importance to you the top three (3) items from the following list you believe that college or district IT should offer. Rating: 1 = first choice 2 = second choice 3 = third choice

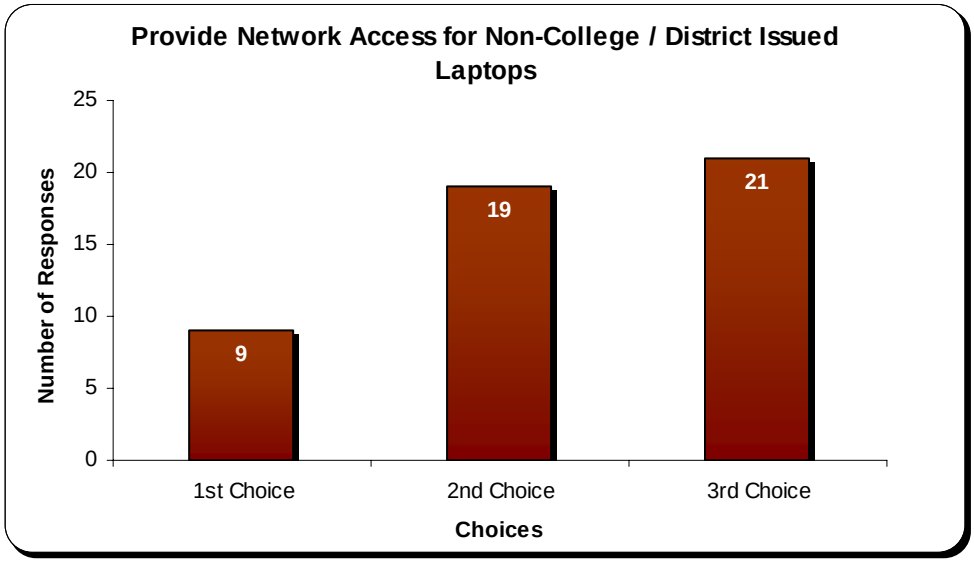
   The top choices are as follows:

Category	1st Choice	2nd Choice	3rd Choice
Off-campus access to college / district technology resources	50 votes	22 votes	22 votes
Expanded Wireless	36 votes	30 votes	28 votes
Student Support Help Desk	20 votes		22 votes
On-line Ordering / Purchasing of College Products and Services		26 votes	22 votes

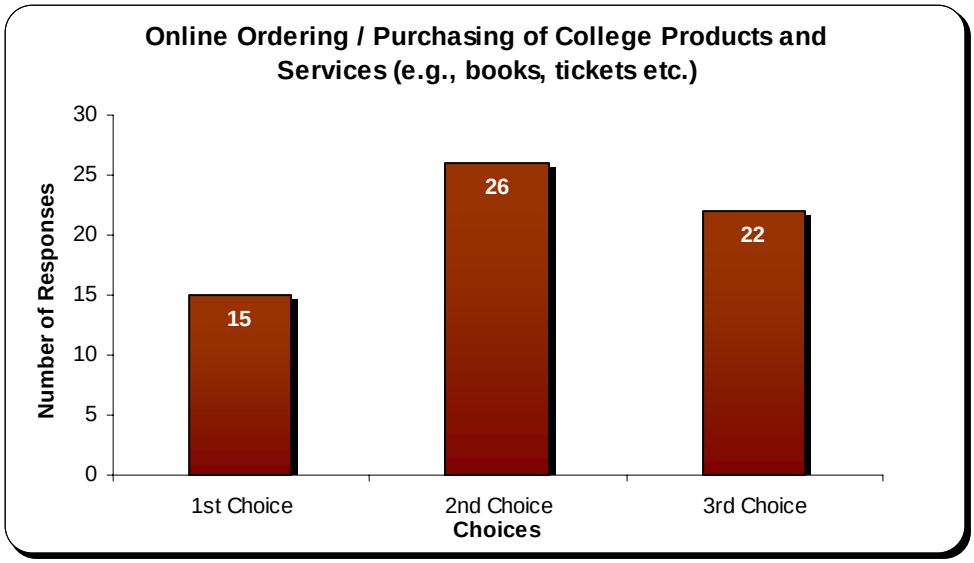
QUESTION 4A = OFF-CAMPUS ACCESS TO COLLEGE / DISTRICT TECH RESOURCES
TOTAL RESPONSES 94 OUT OF 194



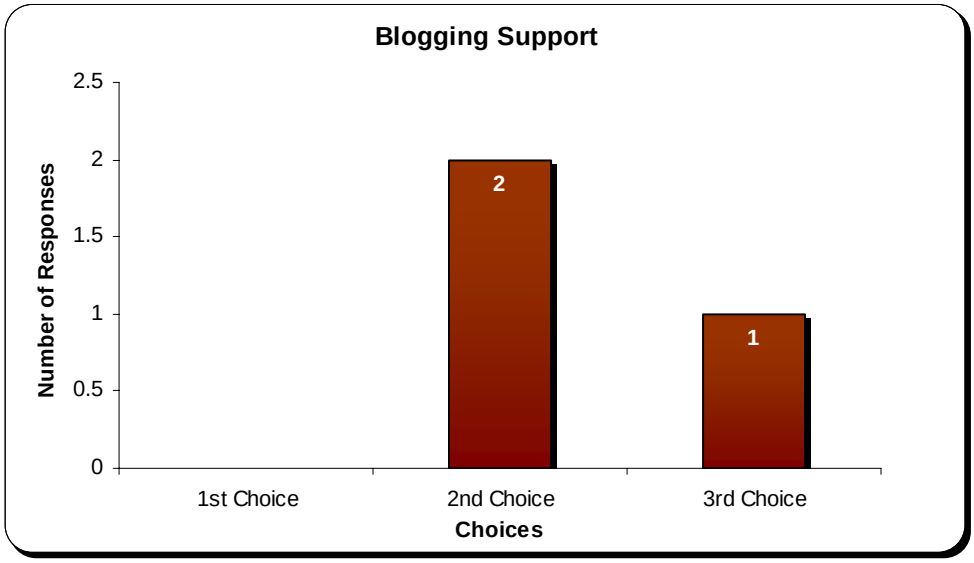
QUESTION 4B = PROVIDE NETWORK ACCESS NON-COLLEGE / DISTRICT ISSUED LAPTOPS
TOTAL RESPONSES 49 OUT OF 194



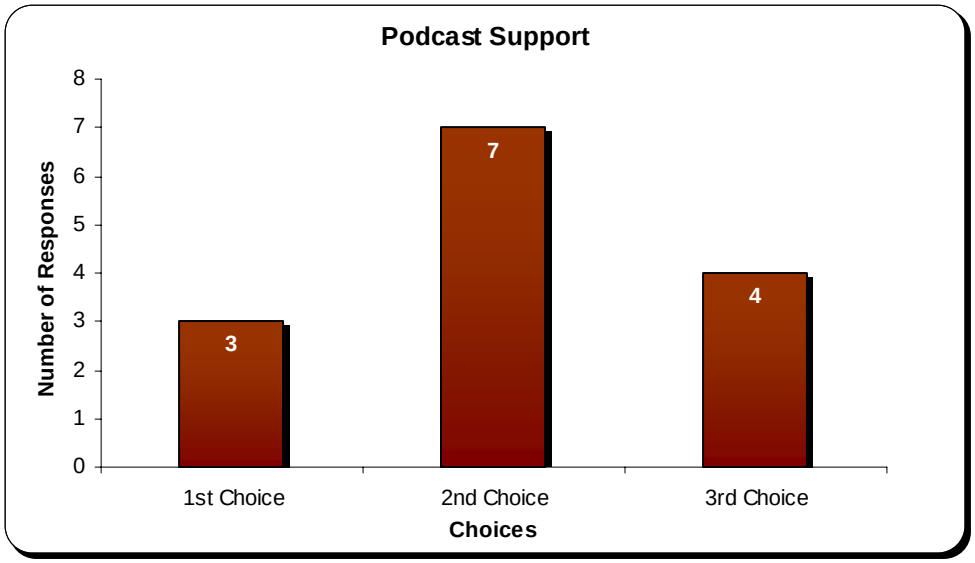
QUESTION 4C = ONLINE ORDERING / PURCHASING OF COLLEGE PRODUCTS / SERVICES
TOTAL RESPONSES 63 OUT OF 194



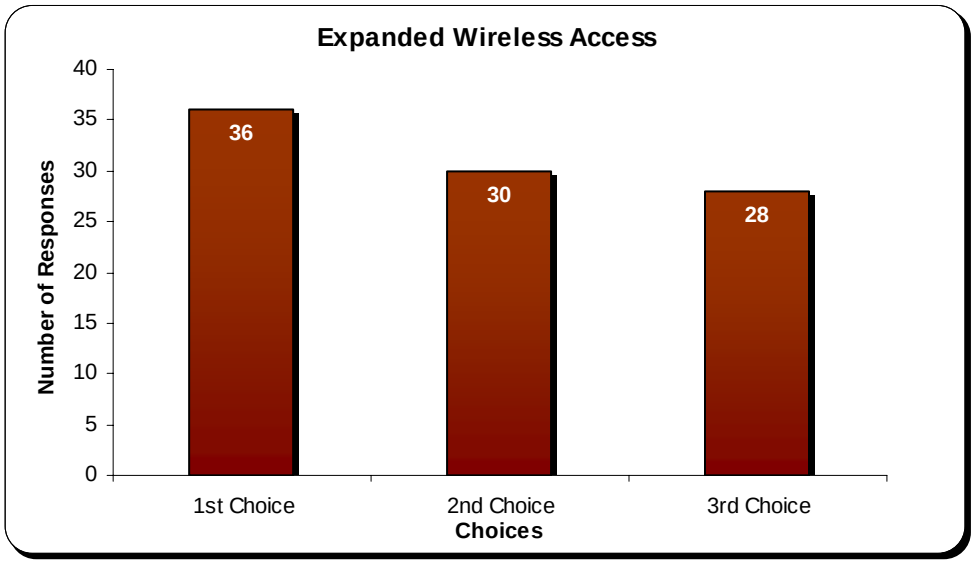
QUESTION 4D = BLOGGING SUPPORT
TOTAL RESPONSES 3 OUT OF 194



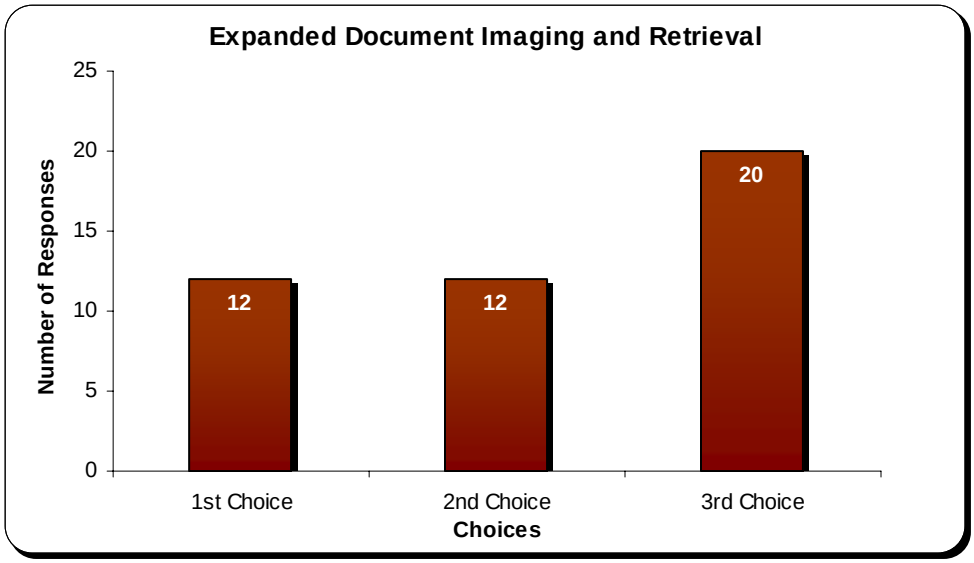
QUESTION 4E = PODCAST SUPPORT
TOTAL RESPONSES 14 OUT OF 194



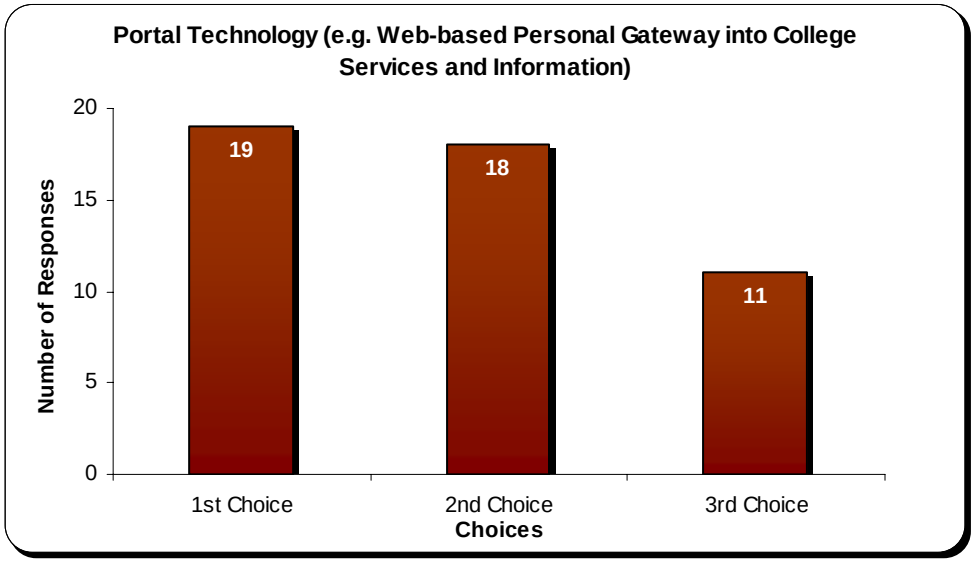
QUESTION 4F = EXPANDED WIRELESS ACCESS
TOTAL RESPONSES 94 OUT OF 194



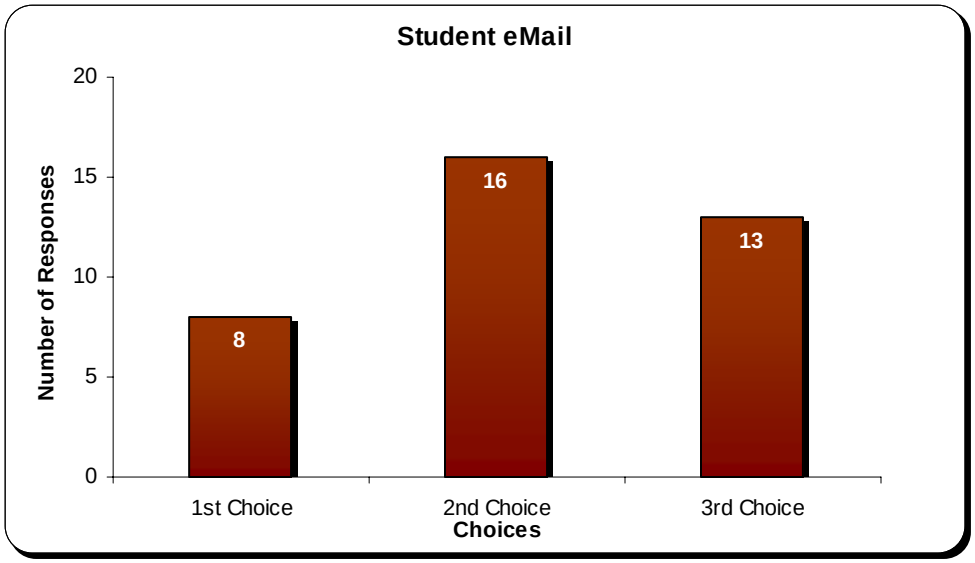
QUESTION 4G = EXPANDED DOCUMENT IMAGING AND RETRIEVAL
TOTAL RESPONSES 44 OUT OF 194



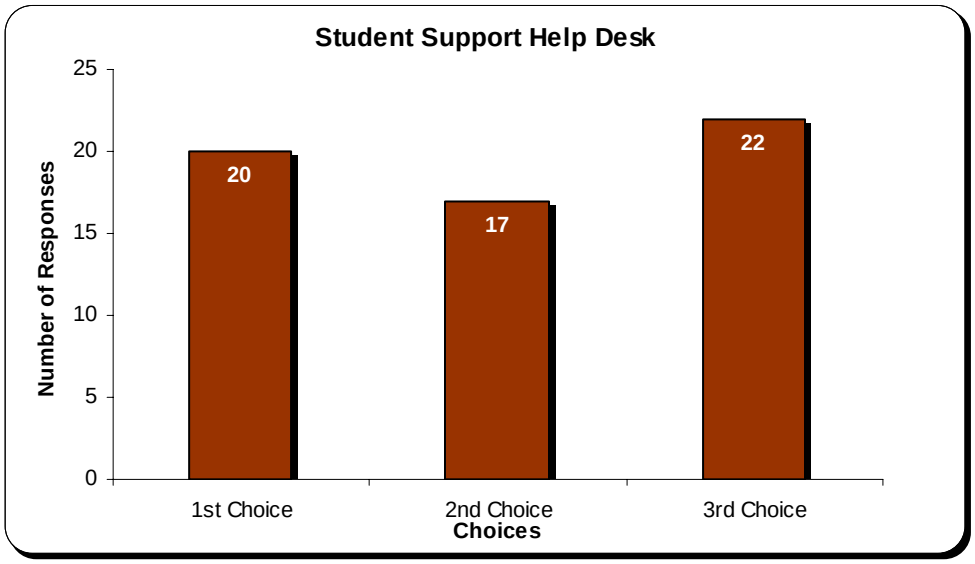
QUESTION 4H = PORTAL TECHNOLOGY
TOTAL RESPONSES 48 OUT OF 194



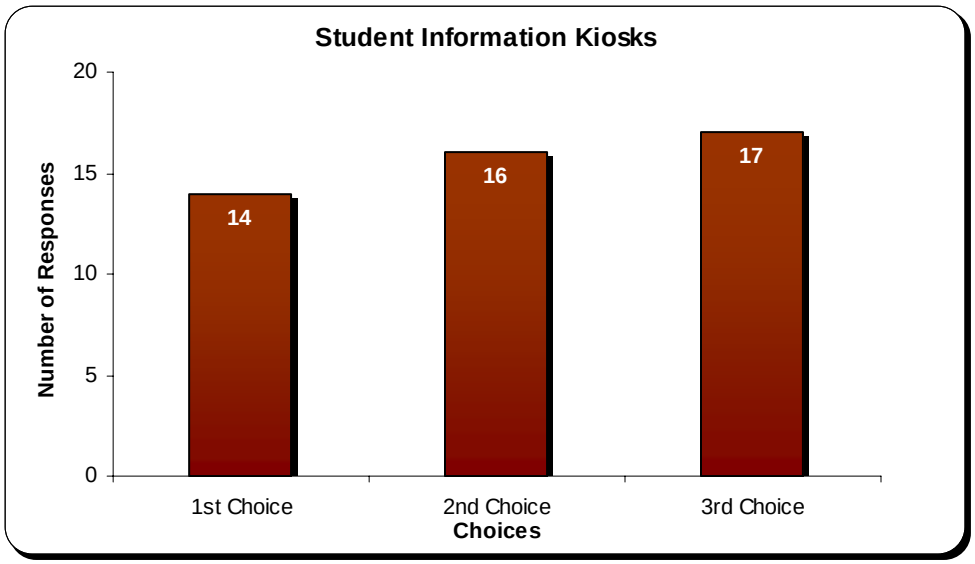
QUESTION 4I = STUDENT EMAIL
TOTAL RESPONSES 37 OUT OF 194



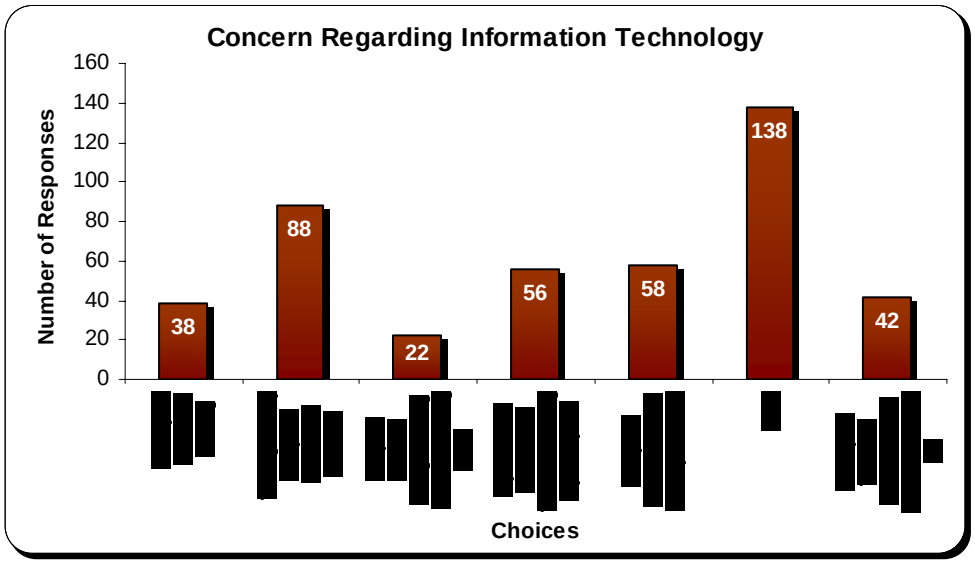
QUESTION 4J = STUDENT SUPPORT HELP DESK
TOTAL RESPONSES 59 OUT OF 194



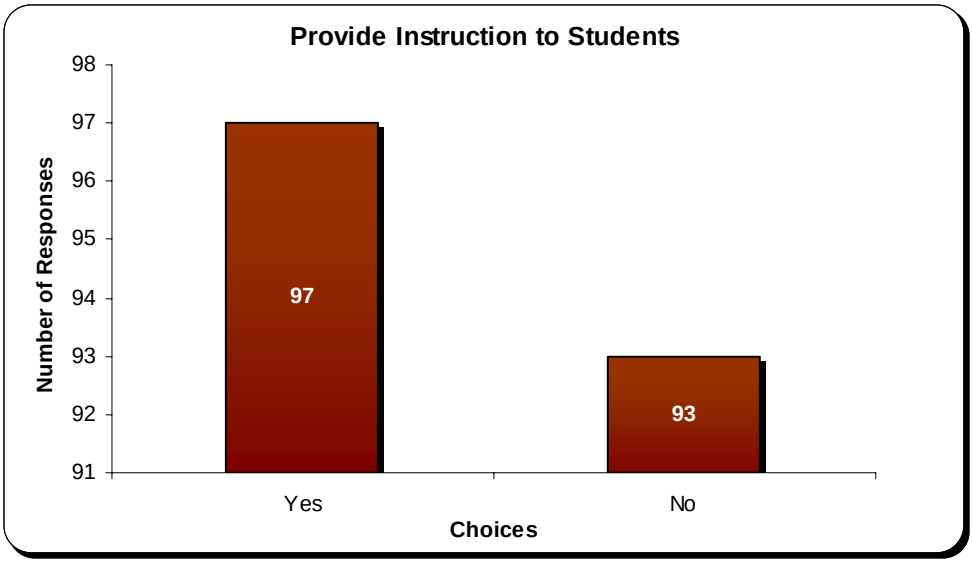
QUESTION 4K = STUDENT INFORMATION KIOSKS
TOTAL RESPONSES 47 OUT OF 194



5. Which of the following concern you regarding information technology? Check all that apply. TOTAL RESPONSES 182 OUT OF 194

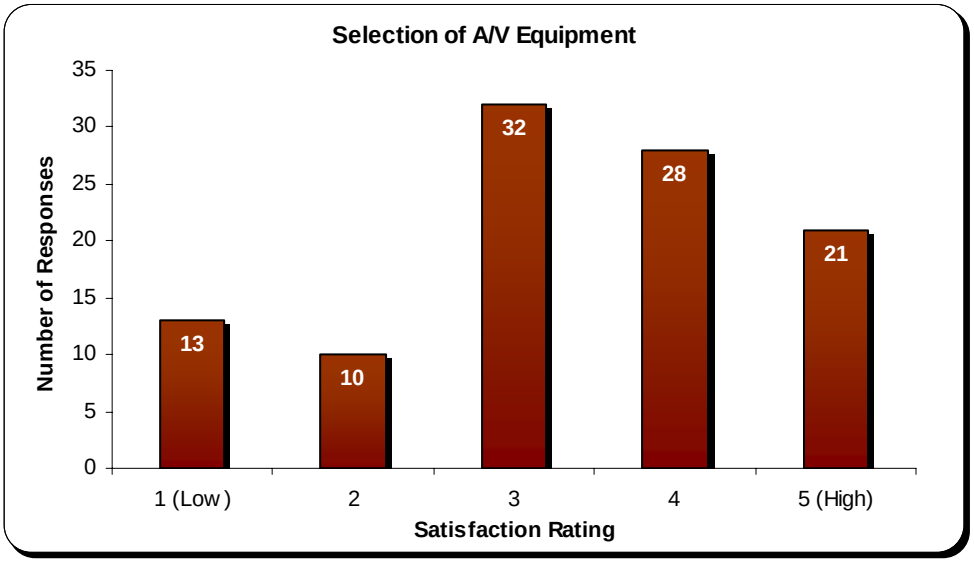


6. Do you provide instruction to students? If the answer is yes continue to question 7, if the answer is no please skip to question 9. TOTAL RESPONSES 190 OUT OF 194

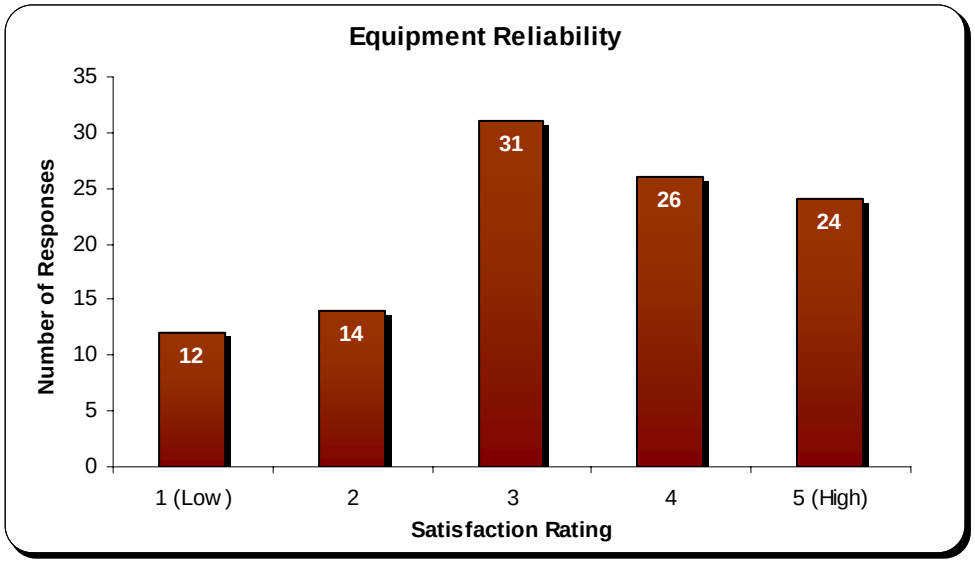


7. How satisfied are you with the following aspects of audio-visual services?

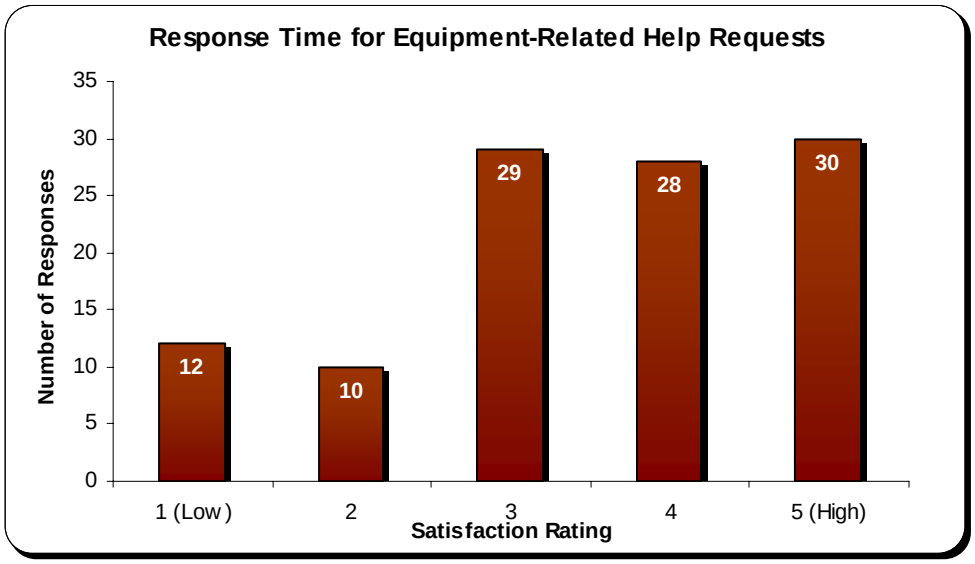
QUESTION 7A = SELECTION OF A/V EQUIPMENT
AVERAGE SATISFACTION RATING 3.33
TOTAL RESPONSES 104 OUT OF 109



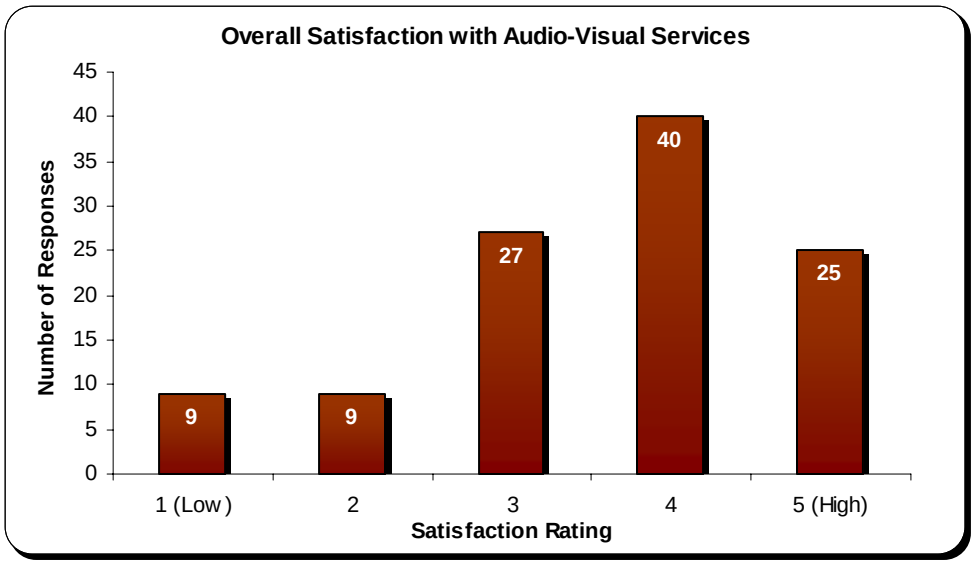
QUESTION 7B = EQUIPMENT RELIABILITY
AVERAGE SATISFACTION RATING 3.34
TOTAL RESPONSES 107 OUT OF 109



QUESTION 7C = RESPONSE TIME FOR EQUIPMENT-RELATED HELP REQUESTS
AVERAGE SATISFACTION RATING 3.5
TOTAL RESPONSES 109 OUT OF 109

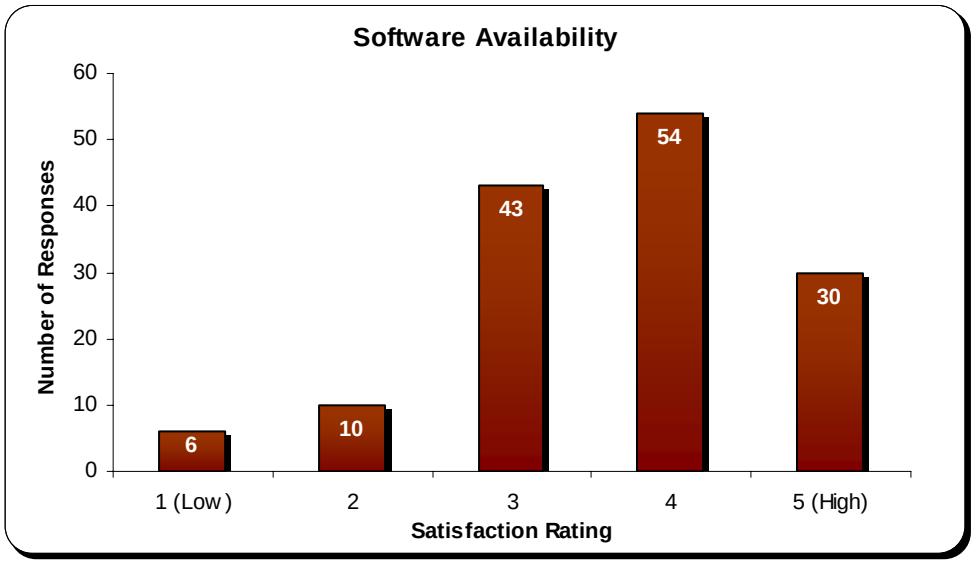


8. How satisfied are you with audio-visual services overall? TOTAL RESPONSES 110 OUT OF 194

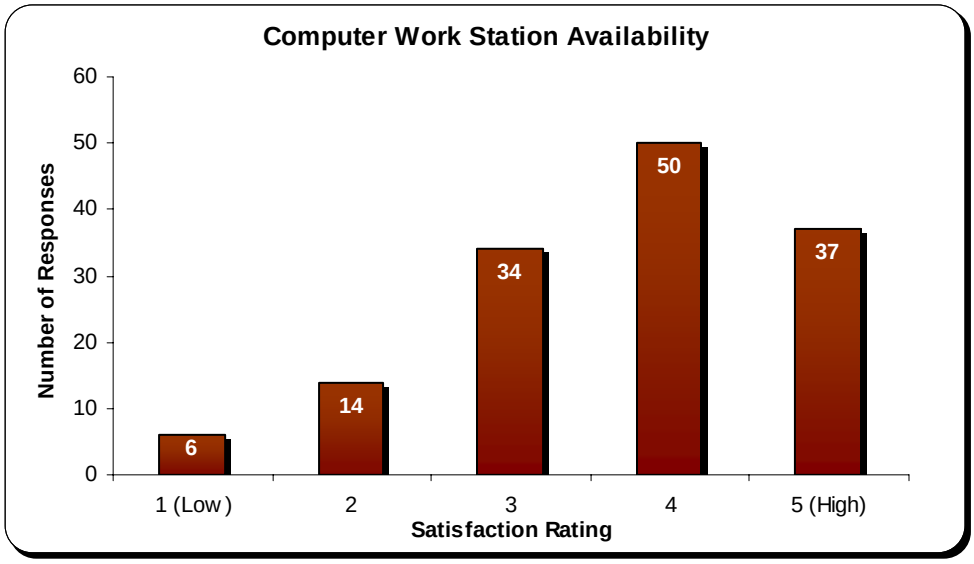


9. How satisfied are you with the following aspects of your college's Computer Labs?

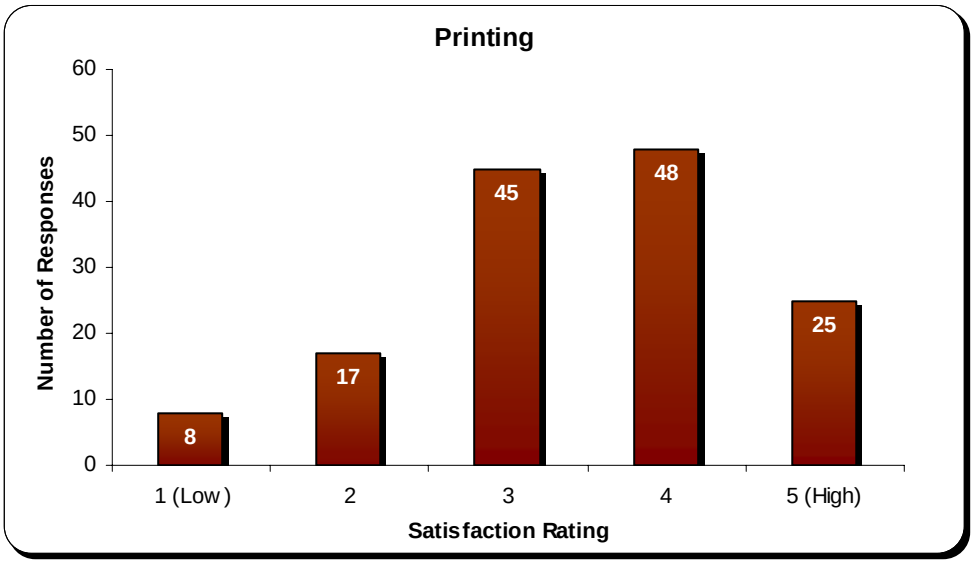
QUESTION 9A = SOFTWARE AVAILABILITY
AVERAGE SATISFACTION RATING 3.64
TOTAL RESPONSES 143 OUT OF 194



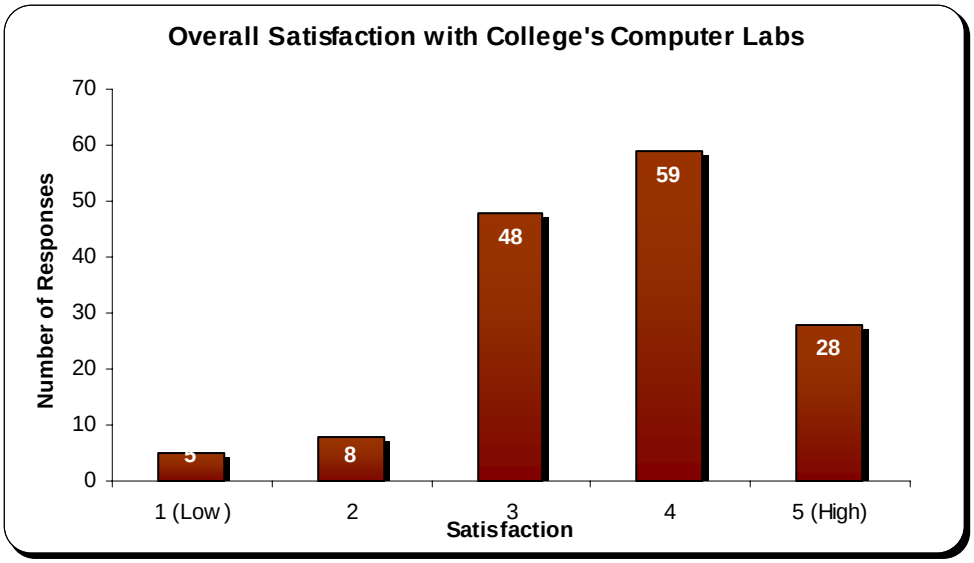
QUESTION 9B = COMPUTER WORK STATION AVAILABILITY
AVERAGE SATISFACTION RATING 3.71
TOTAL RESPONSES 141 OUT OF 194



QUESTION 9C = PRINTING
AVERAGE SATISFACTION RATING 3.45
TOTAL RESPONSES 143 OUT OF 194



10. How satisfied are you with your college's Computer Labs overall? TOTAL RESPONSES 148 OUT OF 194



11. What additional software or services would you like to see in your college's Computer Labs? TOTAL RESPONSES 55 OUT OF 194

- I would like the ability to easily deny students access to the internet.
- Our college IT dept is unable to support our instructional lab needs for our dept (Media Arts). As a result, our dept faculty serve as the tech support - working out of classification.
- I would like to see more services provided at the Delano site. I believe if we are providing a new building, it needs not only the equipment, but the staff. Extra staff should be provided. I do not use the Computer labs at the BC campus often, but I am impressed with the large number of computers available.
- I need to be able to install my own software on my office computer. Currently we are required to contact IT to install software since our office computers are password protected and do not allow instructors to install their own software. I test audio/video applications and need to install new software almost daily. It's ridiculous that I have to contact IT every time I need software installed.
- Nearly every lab needs more computers -- particularly the Computer Commons.
- The Career Center Lab needs an updated printer for students.

- Student e-mail service.
- additional training available for students, especially in the Library Computer Commons. Students who are lost cannot get even minimal help.
- Address accessibility of all computer labs software, hardware, and furniture.
- upgraded printers. Better workstation ergonomics.
- more printers and access to them
- We need more technicians so we can service the computers in the lab.
- Vista and the NEW Office 2007
- The Delano College students and staff are the last person to obtain quality equipment. We receive everyone elses hand me downs. When faculty and classified staff obtain new equipment, the like dept staff do not receive same. The training for faculty and classified has been poor at the Delano Center.
- Prepay of student printing with a credit or debit card at the help desk instead of having to go to the business office to pay.
- I work in student activities and I really haven't heard any comments on the computer lab from the students. I don't use the Computer Lab, so I personally don't know.
- None
- Up-to-date software
- Software used in the instructional programs
- smart labs; graphics software
- There is a need for more computer availability. We have to share the lab with Computer/English classes. Constant complaints from Students about that.
- I have not utilized the college computer labs, so I am not familiar with the availability of equipment or workstations.
- Additional computer labs!!!
- We have ongoing compatibility issues between softwares. This negatively impacts student progress. I'm not sure how it can be resolved, I just know it's an ongoing problem

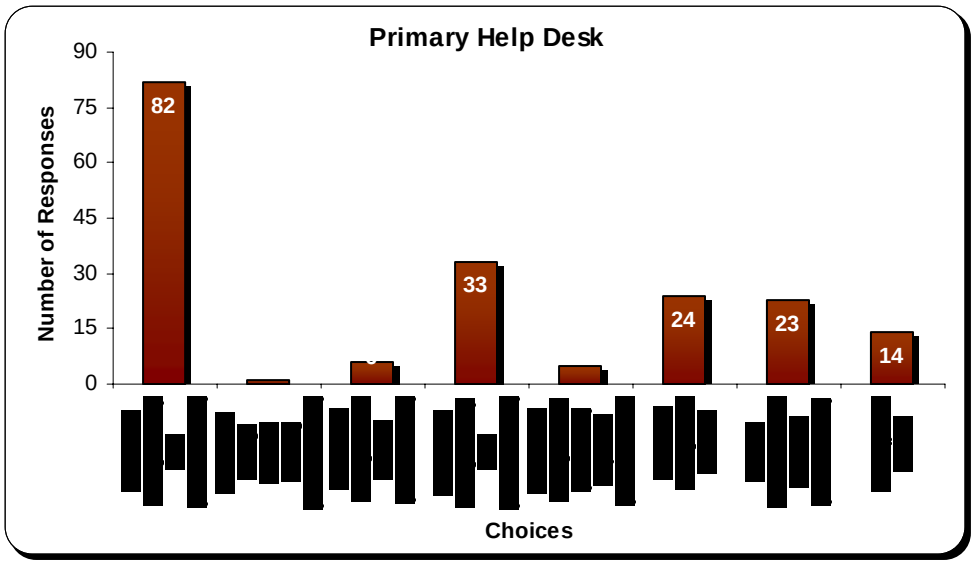
- All software or services provided to students should have components for students with disabilities. Alex and Plato are not accessible.
- Updated equipment-computers etc.
- More computer availability at peak times.
- When ordering new computer stations, we need to keep in mind to order an accessible computer station in that lab as well based on ratio(meeting minimum standards so that assistive technology software can be installed for student use). If this is completed in the beginning, it would not need to be retrofitted later which is more costly.
- Little things like RealPlayer and other plug ins so that students can view files from the online classes (for instance, the online speech class uses rm files, but they CANNOT be viewed from the computer lab).
- More computers and printers.
- The students may benefit from being exposed to another office suite such as Open Office. It is free and would allow students who explore it to begin thinking about the similarities between software programs rather than getting stuck every time they are faced with a new program.
- Better Spam filter!! I really dislike receiving all the junk emails. It takes up way too much of my alloted computer space and time, especially when my computer is constantly telling my mailbox it too full.
- Faster and More computers
- I don't use these resources
- adobe captivate
- We are getting more open source software installed on some of the equipment. This could be expanded.
- I would like to be able to load software unique to my department, but hopefully this will happen in the near future.
- I have noticed at the Delano campus' computer labs that printing items not picked up by students is a problem. This creates such a waste of paper which students haven't paid for. Either have an individual be a constant presence to assist/instruct people in the lab or have a set up that students' pay before printing their pages. As it is now, there are student workers at one lab but is doing double duty as a receiptionist, therefore, that student is not in the lab at all times. At the other locations, students' must go outside the lab to the administrative office to get their printing job and pay, because no one is available to monitor the printer in the lab at all.
- Trained student workers familiar with assistive technology applications

as well as the mare familiar applications.

- Not sure.
- None
- I have spent a total of two hours in the faculty computer lab in 13 years.
- If this refers to the classrooms, they often are not ergonomically correct and are very unattractively configured (in some cases--the Humanities lab, for example.) If you are referring to the computer commons, more work needs to be done to free computers for students doing academic work rather than students entertaining themselves.
- They are fairly complete now.
- Thanks to AV, we finally have speakers that work with computers in H52. Up until last week, the sound only worked with the DVD player. I would like to be able to bring in my wireless laptop and use it in a campus computer lab without checking out 'portable' equipment from AV. (You need to be a pack mule to carry this stuff anywhere.) I would like to see a better instructor work station in this lab, as well as a list of computers that aren't hooked up to Vision. AV staff has been tremendous in trying to help with all requests despite limited budgets and staff.
- I like the audio visual available in lecture halls and would like this to be available in science labs.
- I work at a site that does not have a computer lab.
- Complete line of all software packages used in onsite and online courses. More IT staff: techs, help desk, network admins.
- College issued student emails
- No comment
- ITV equipment is a real bane. If we are going to continue with this modality, we need to really rethink what the program needs. We should not just have high tech AV in the ITV rooms.
- A relatively minor request: set the default for Word documents to one inch on all sides, especially in H-52.
- I don't use college computer labs.
- None
- I wish there was better access to all computer and printing services for adjunct faculty. Especially for those of us who teach primarily on the Delano campus.

Help Desk Services

12. Which Help Desk do you primarily call for assistance? TOTAL RESPONSES 188 OUT OF 194



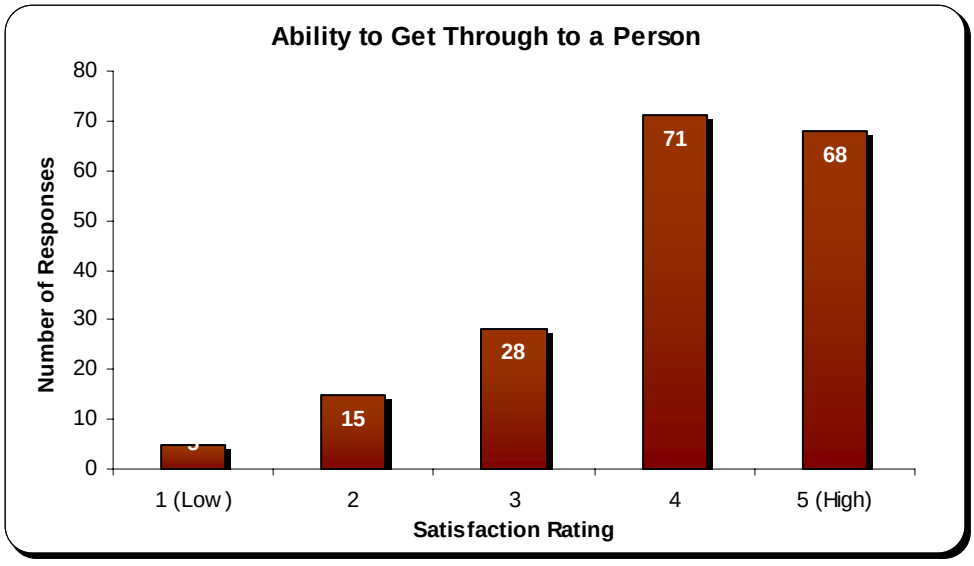
Other (please explain):

- I no longer attempt to receive tech support through our college help desk. I do it myself.
- I use both BC IS Help Desk and the BC Media SErvices helpdesk (I can not use both radio buttons above).
- I always contact CeCe
- I deal with MBS mostly, so my contact is Dana Ttsaw, other wise I ask Steve Adams and if he can't help me, he calls someone.
- Kristin is great--always helpful and courteous.
- I use the online form for BC.
- I call the LSC Help Desk for Banner Related Issues and the CCC IT Help Desk for personal computer issues. The responses to the questions below rate the LSC Help Desk. The responses for the CCC IT Help Desk are lower.
- banner help desk
- I call the LSC Help Desk and the BC IS Help Desk equally. It depends on what I am needing help with.
- I generally call Judy Ahl directly and she is very helpful in solving our problems...we need more like her!

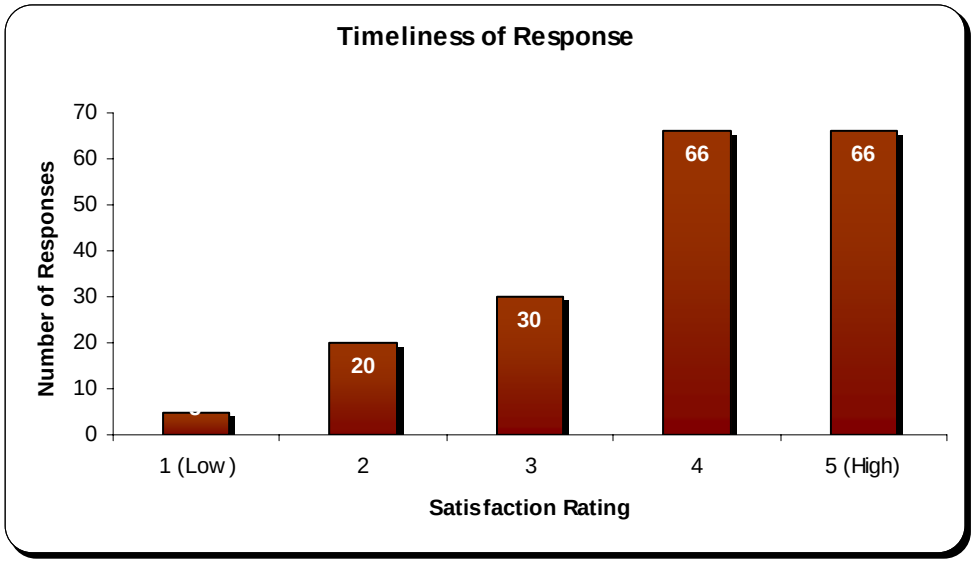
- I first ask other faculty members in my area for assistance and then call the BC IS Help Desk.
- I call a specific technician
- I'm doing this from home but I call the # with CEce and brian
- I always contact Judy Ahl, who does a fabulous job.

13. Please rate your satisfaction with the following Help Desk areas.

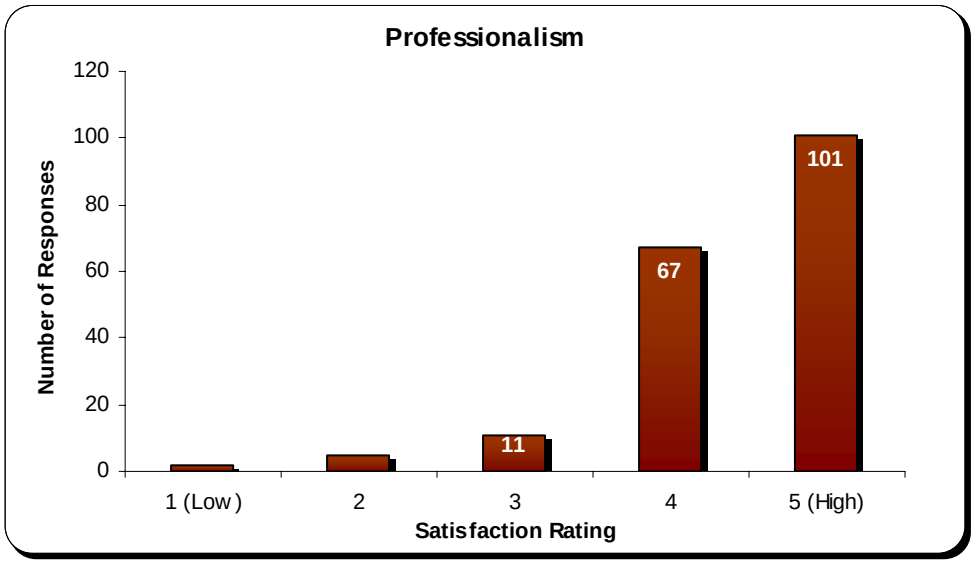
QUESTION 13A = ABILITY TO GET THROUGH TO A PERSON
AVERAGE SATISFACTION RATING 3.97
TOTAL RESPONSES 187 OUT OF 194



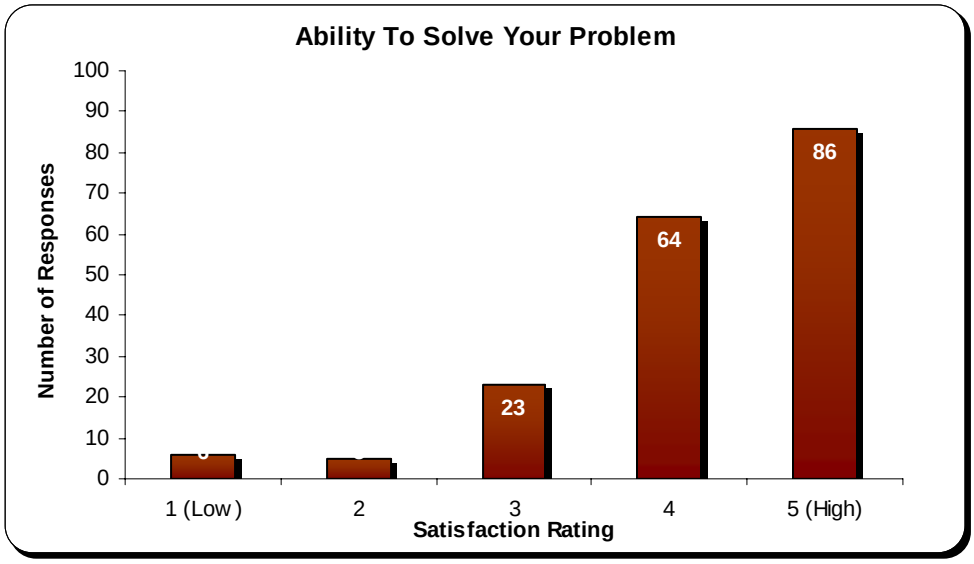
QUESTION 13B = TIMELINESS OF RESPONSE
AVERAGE SATISFACTION RATING 3.9
TOTAL RESPONSES 187 OUT OF 194



QUESTION 13C = PROFESSIONALISM
AVERAGE SATISFACTION RATING 4.4
TOTAL RESPONSES 186 OUT OF 194



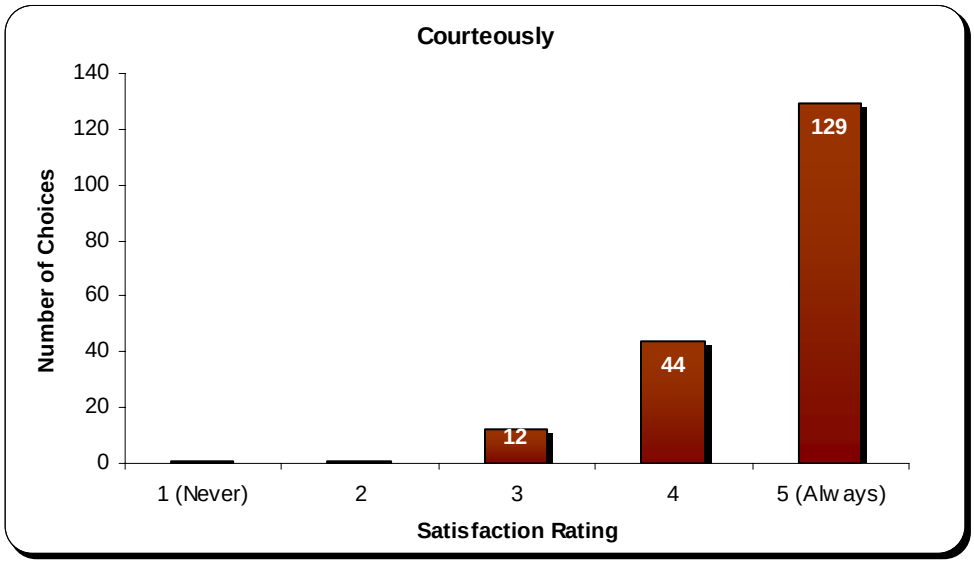
QUESTION 13D = ABILITY TO SOLVE YOUR PROBLEM
AVERAGE SATISFACTION RATING 4.19
TOTAL RESPONSES 184 OUT OF 194



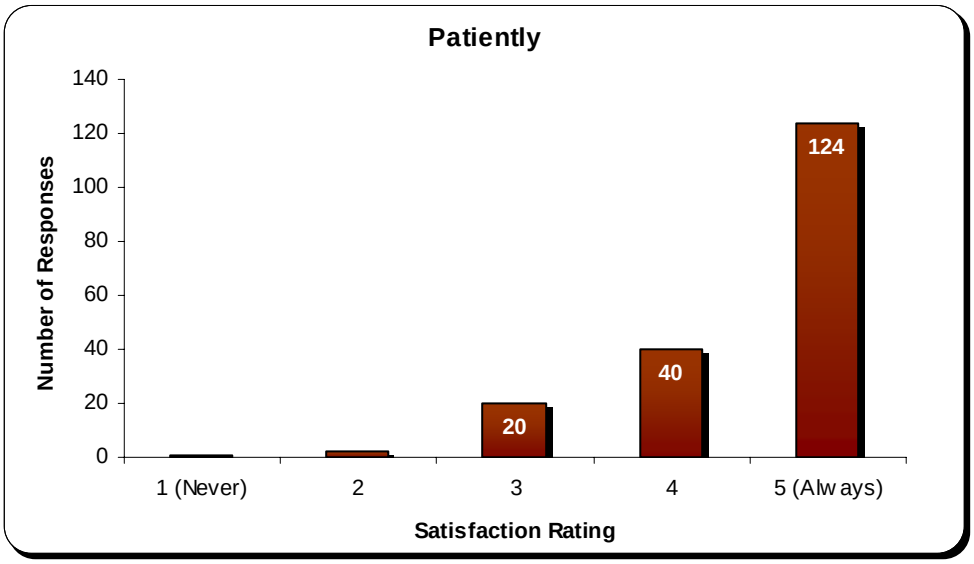
QUESTION 13E = CUSTOMER ORIENTED
AVERAGE SATISFACTION RATING 4.22
TOTAL RESPONSES 185 OUT OF 194

14. Thinking about all of your interactions with the Help Desk staff mentioned above which rating on the scale below best describes the frequency with which you were treated?

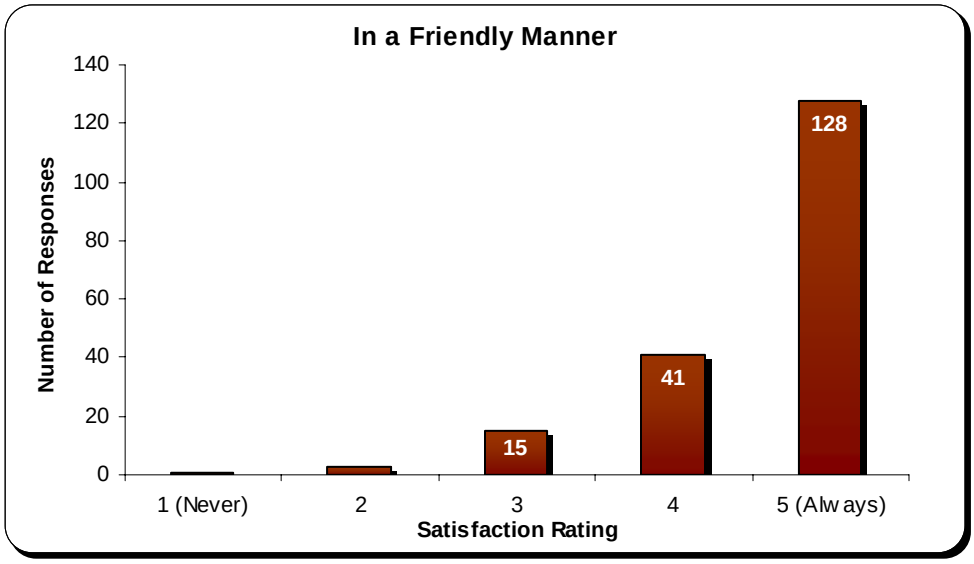
QUESTION 14A = COURTEOUSLY
AVERAGE SATISFACTION RATING 4.6
TOTAL RESPONSES 187 OUT OF 194



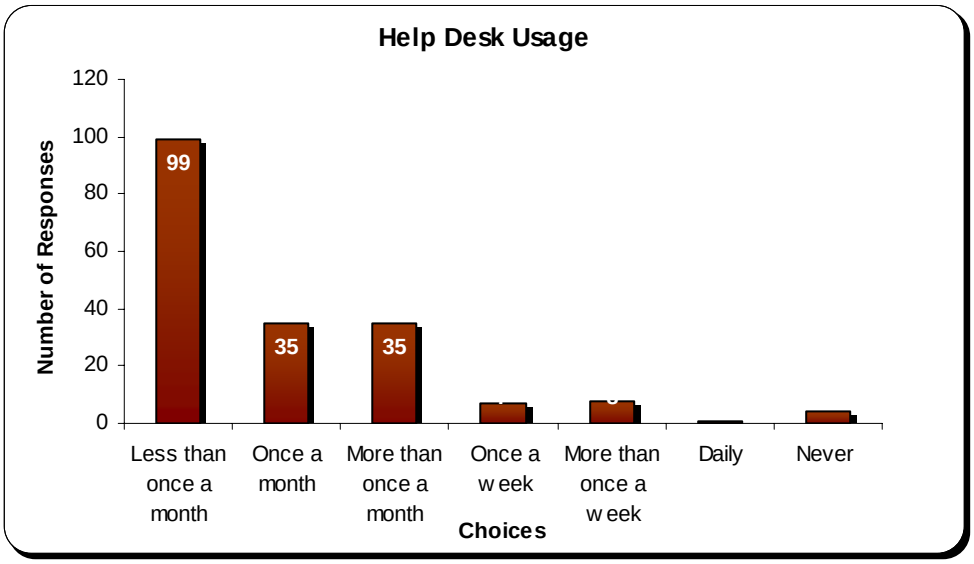
QUESTION 14B = PATIENTLY
AVERAGE SATISFACTION RATING 4.52
TOTAL RESPONSES 187 OUT OF 194



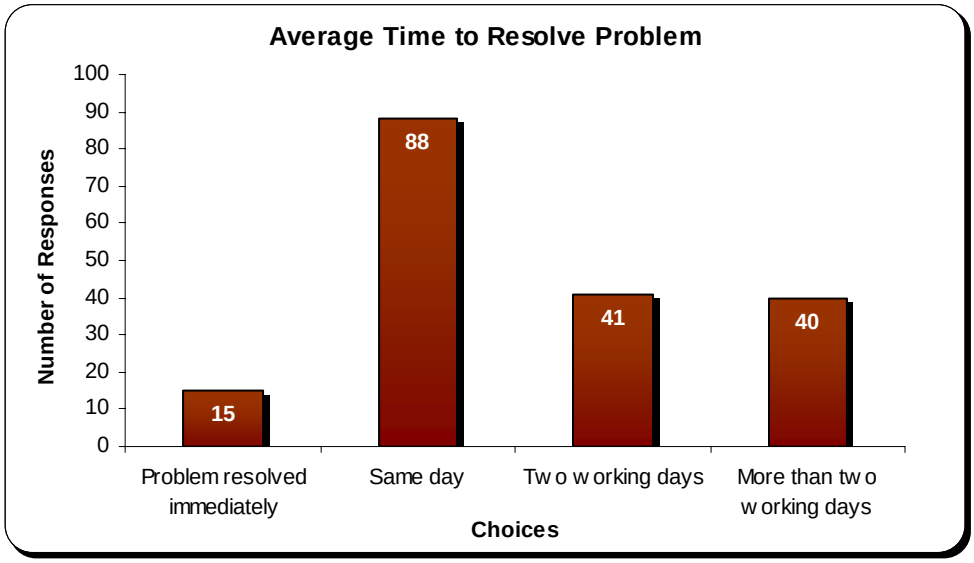
QUESTION 14C = IN A FRIENDLY MANNER
AVERAGE SATISFACTION RATING 4.55
TOTAL RESPONSES 188 OUT OF 194



15. How often do you use this help desk? TOTAL RESPONSES 189 OUT OF 194



16. Think about the problems for which you call the help desk. On average how long does it take to resolve the problem from the time you first call the help desk? TOTAL RESPONSES 184 OUT OF 194

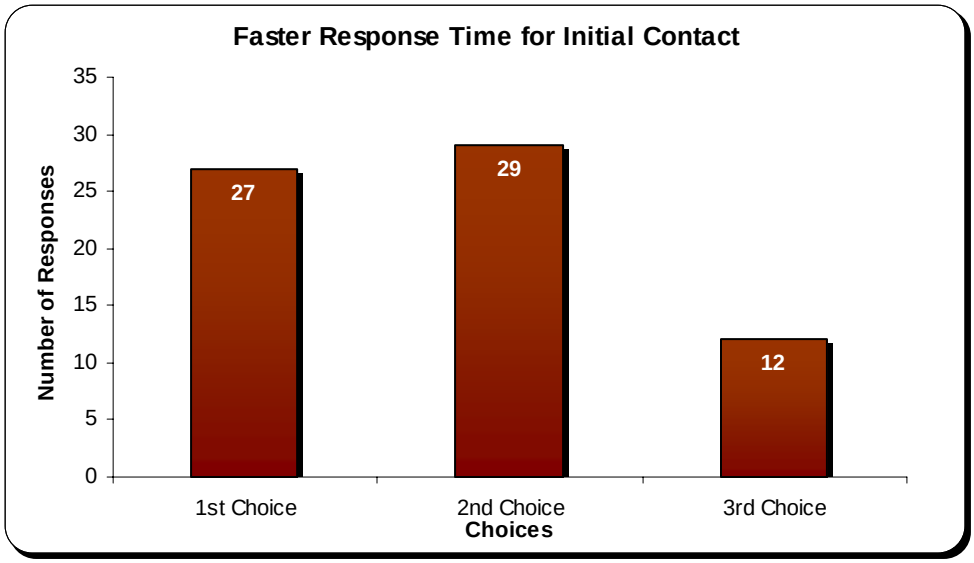


17. Please select in order of importance to you the top three (3) items from the following list that would appreciably increase your satisfaction with the Help Desk problem resolution. Rating: 1 = first choice 2 = second choice 3 = third choice). TOTAL RESPONSES 68 OUT OF 155

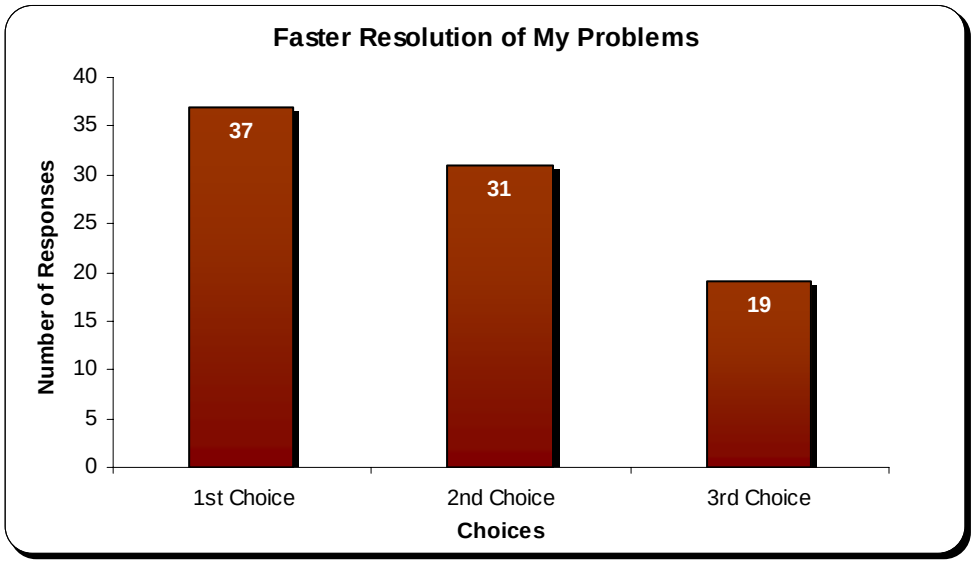
The top choices are as follows:

Category	1st Choice	2nd Choice	3rd Choice
Faster resolution of my problems	37 votes	31 votes	19 votes
Better communication about the status of my request	32 votes	30 votes	34 votes
Faster response time for initial contact	27 votes	29 votes	
Better web-based help information			17 votes

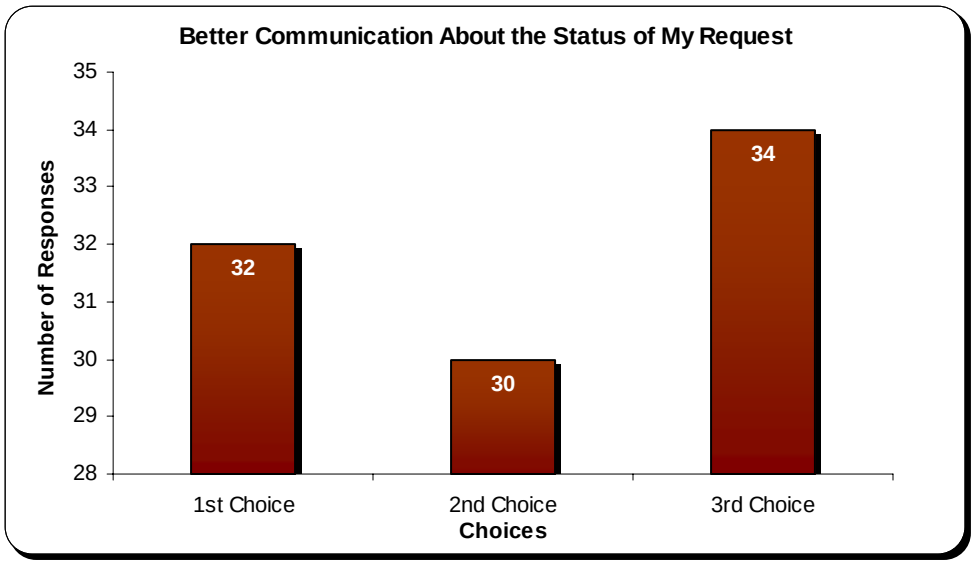
QUESTION 17A = FASTER RESPONSE TIME FOR INITIAL CONTACT
TOTAL RESPONSES 68 OUT OF 194



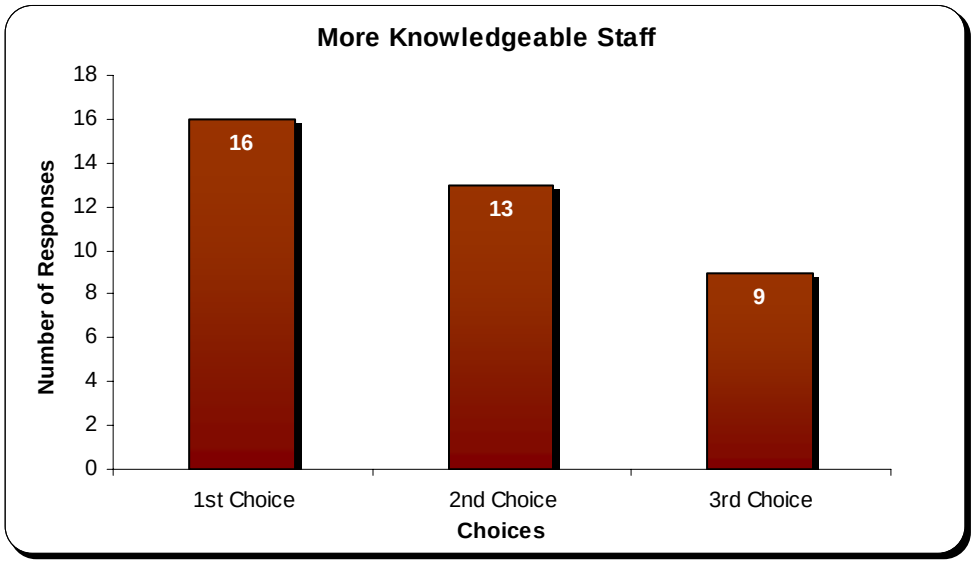
QUESTION 17B = FASTER RESOLUTION OF MY PROBLEMS
TOTAL RESPONSES 87 OUT OF 194



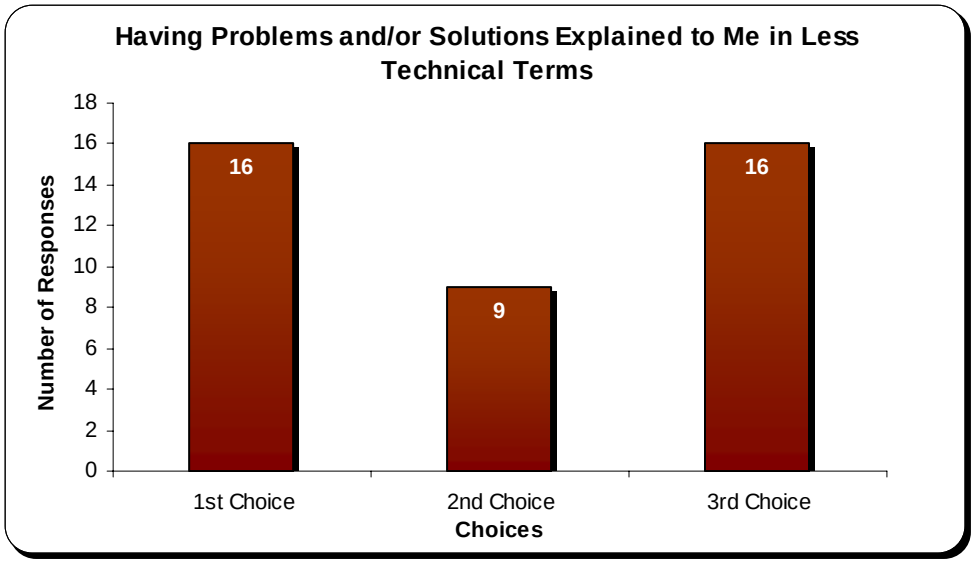
QUESTION 17C = BETTER COMMUNICATION ABOUT THE STATUS OF MY REQUEST
TOTAL RESPONSES 96 OUT OF 194



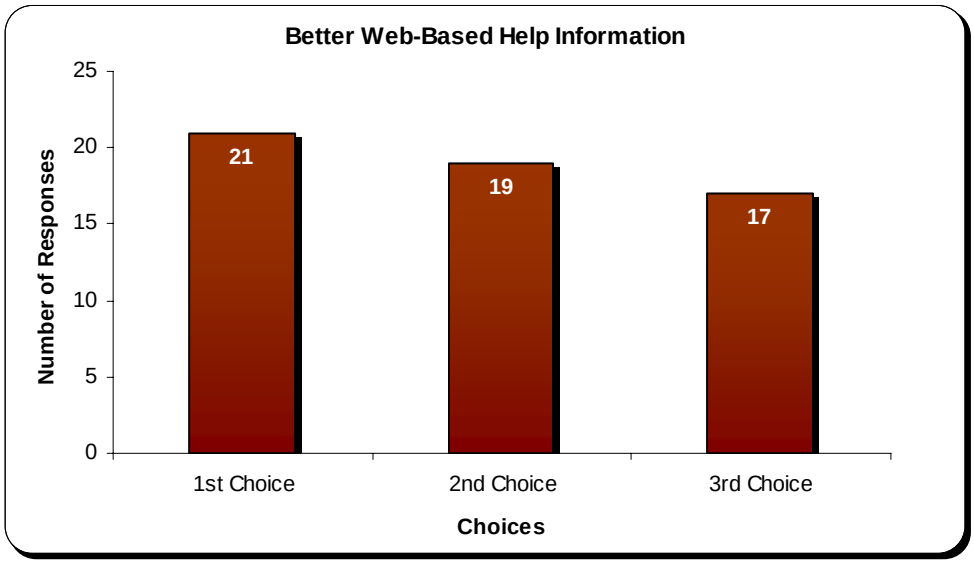
QUESTION 17D = MORE KNOWLEDGEABLE STAFF
TOTAL RESPONSES 38 OUT OF 194



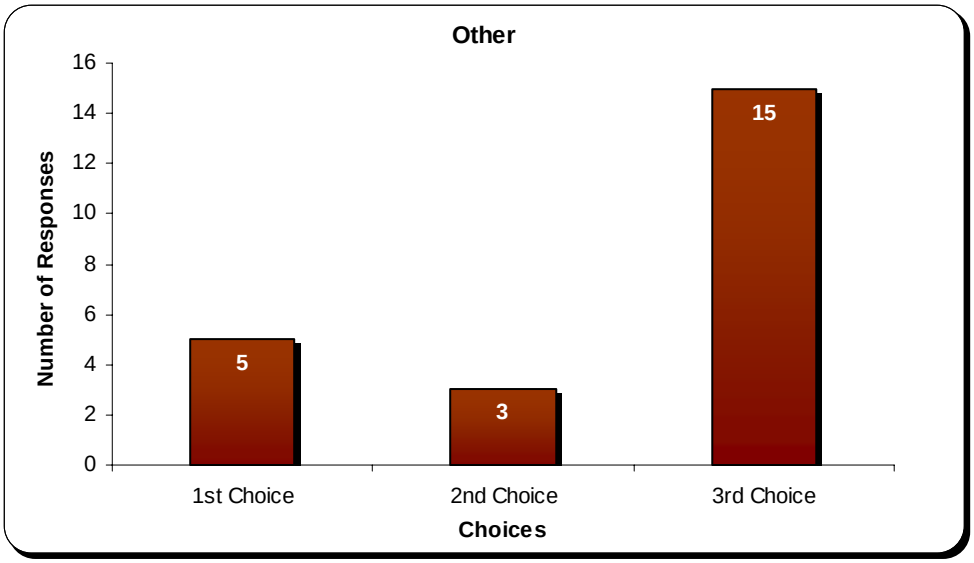
QUESTION 17E = HAVING PROBLEMS / SOLUTIONS EXPLAINED IN LESS TECH TERMS
TOTAL RESPONSES 41 OUT OF 194



QUESTION 17F = BETTER WEB-BASED HELP INFORMATION
TOTAL RESPONSES 51 OUT OF 194



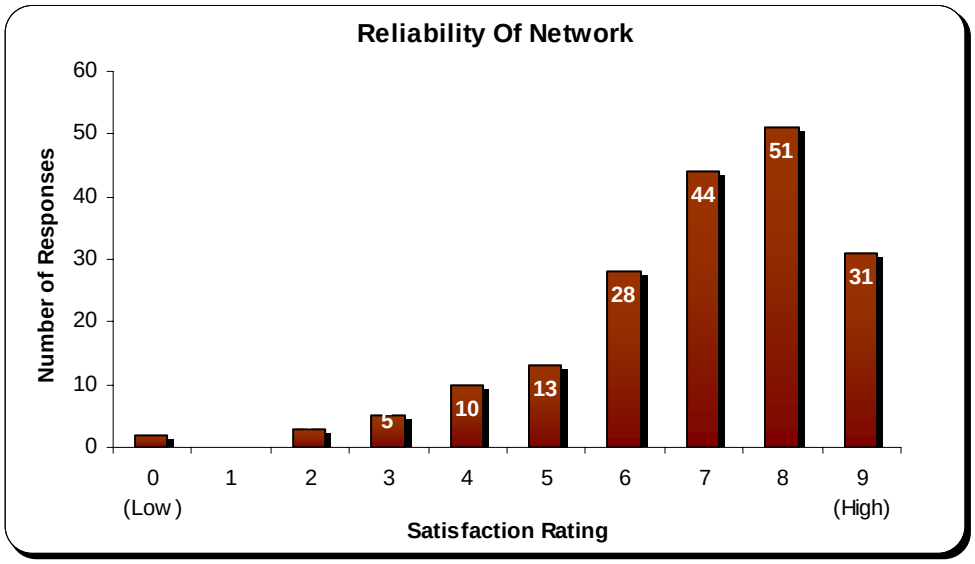
QUESTION 17G = OTHER
TOTAL RESPONSES 23 OUT OF 194



Network Services

18. How satisfied are you with the performance of the network?

QUESTION 18A = RELIABILITY OF NETWORK
AVERAGE SATISFACTION RATING 7.89
TOTAL RESPONSES 188 OUT OF 194



QUESTION 18B = PERFORMANCE (RESPONSE TIME – SLOW TO FAST)
AVERAGE SATISFACTION RATING 7.11
TOTAL RESPONSES 175 OUT OF 194

19. Please list any location where access needs to be added or improved. Include specific information such as college, building name, room number, etc. TOTAL RESPONSES 48 OUT OF 194

- The entire Fine Arts complex at BC is in bad shape. I've been told that this is a hardware problem. It sometimes takes 3 to 4 minutes for my office computer to log onto the network.
- I personally wired the rooms that I teach in because I found out at the last minute that my room was moved, and it was on the Friday before classes started, and there was no way IT was going to do the job in time for the start of my classes.
- There are two kiosks in the library lobby that have not worked for years. They should either be functional or removed.
- I don't think it is the server that is the problem to access. I believe it is the relatively low memory in the computers that are purchased. For future purposes, please keep that in mind.
- Student Computer for Registration at each site.
- hook printer to pc in Porterville College Maintenance conference room for maintenance workers.

- Students need some access to printing and the internet in the information area (A&R). When the library is closed during breaks, I usually have at least three students come to my office to use the computer to print transcripts or get other information.
- Teaching online-never know if the computer problem is with the server or personal ISP provider. Front Page difficult to set up where stdents can understand. Moodle variability with instructors confuses students.
- my computer in particular needs improvement, it locks up, freezes up and throws me out launched programs
- Wireless capability in the main building at Cerro Coso for students
- Wireless access at points around campus.
- More student computer access is needed in PC's Academic Center lobby area. As we encourage students to handle more transacations online, this will give those students who may not have computers at home or elsewhere another place to obtain computer access and help they need
- Delano.....I am sure because my computer is old, but often it takes too long to switch from one page of banner to another...and gets stuck, and I have to shut down program and start again
- Help desk personnel training needs to be better. Students are sometimes given the wrong information in order to print.
- Slower in lab [H52]
- Mammoth, room 225
- Banner is sometimes very slow.
- from home
- Dead zones in the LRC make it impossible for students to use wireless labtops in group study rooms.
- Boot-up and log-on time in Bakersfield College Agriculture Room #9 has increased to about 10 minutes. Something's wrong!
- Some of the computers in the PC FA/Foundation offices have periodic problems with network access characterized by programs freezing and having to restart for access. However, if I understand correctly, this may be a problem with the Banner software and not our PCs. It is only this problem that leaves me less satisfied with the network than I ordinarily will be and our IT staff has addressed it.
- Allow Portable lab carts in the Horticulture lab

- Some of the computers are old and run more slowly than others. In the Learning Center there are a few. There are 2 in the work area of the Math Lab and the Student Success Lab's main computer has very little memory space.
- there is no wiring for access in many rooms at the gymnamsium. Is there a way to create a wireless network down here so we can it in more places?
- I don't think network access is the problem so much as the lack of adequate RAM to run programs. For over a year I only had 128 and recently RAM was taken from another computer to up mine to 356. I'm used to the 1G on my home laptop, so RAM is the problem here, NOT the network access.
- My computer in Industrial Tech has a very low amount of RAM and is super slow. It is unfair that in order to bump up the RAM on my computer I need to purchase more memory out of my budget.
- Delano College Center, Admissions & Records Station
- None.
- PC-Gym, sometimes we have outreach activities in there.
- Student Services Bldg. computers for students use are always having problems and we sometimes have to just shut them down. Near office SS-184,193,194
- Cashiering computers at Bakersfield College Business Services windows are about 6 years old and very slow. Hard to service students who are trying to get back to class when each transaction takes so long to ring in.
- If we had wireless connections, this wouldn't be an issue!!!
- Connectivity needs to be in all classrooms.
- PC SM114 is very slow much of the time. I believe this is because the computer is so old not so much the network -- same with my office computer.
- Accessing e-mail off campus should be improved so that e-mail can be deleted easily. Trying to e-mail students off-campus through Banner can't be done without filling out a POP menu. This should be easier. Overall, the start-up time to get the computer going and access Outlook on campus (or Explorer) seems slower than my wireless cable connection at home.
- I believe my problem is that my PC is slow. It is scheduled to be replaced soon.
- Student Services Building Learning Center Tutoring Center
- Porterville College, AC 112-On registration days and first week of school our computers run too slow. We have lines of students that need to get to class.

It helps us do our job more efficiently.

- No comment because of the extensive remodeling that had started at the college
- Cerro Coso IWV Learning Resource Center 1st floor NW corner. Wireless access is problematic.
- We have requested WiFi access in SE 40. The request seems to be in limbo?? I would also recommend WiFi at several public locations on campus. (Cafeteria, library, Student lounge areas)
- Wireless (preferably) or wired access for the classrooms in the Humanities building.
- I would like to see projectors and lap tops in more of the conference rooms with videoconference room capability. Its currently limited to only one room.
- It's a pretty slow network
- My computer in H-17 could use a look to see if it can be made a bit faster. I sit in the northeast corner of this four-desk office
- Delano computers, more specifically the office comps. and Room 6 can run very slow.
- Assessment Center building needs to be identified as such. I am frequently showing incoming students where it is. The only identification is on one door, and it is easy to not see.
- Network in Fine Arts area is very slow Labs in FA9, FA10 and offices.

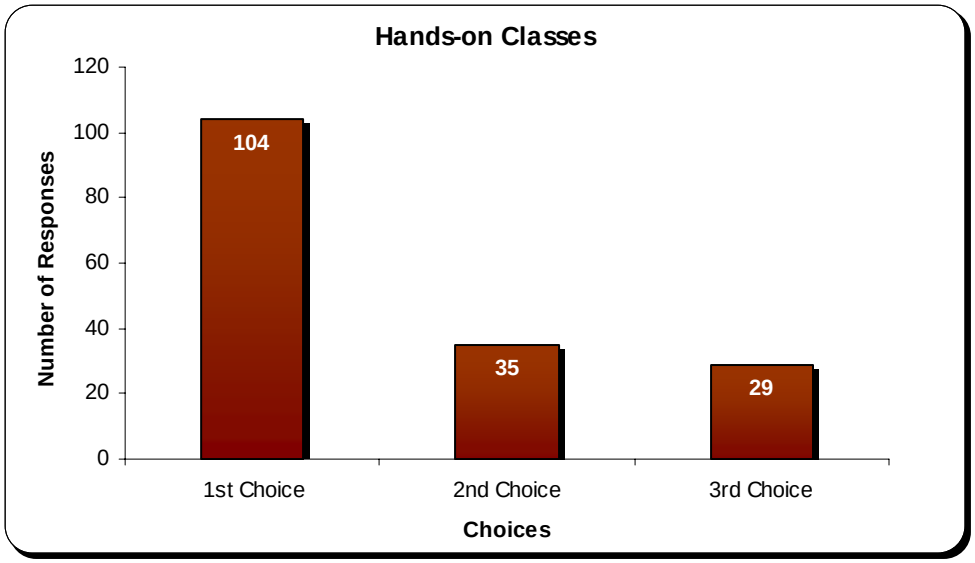
Training Services

20. Please select in order of importance to you your top three training methods for learning additional computer-related knowledge and skills (Rating 1 = first choice 2 = second choice 3 = third choice etc.)

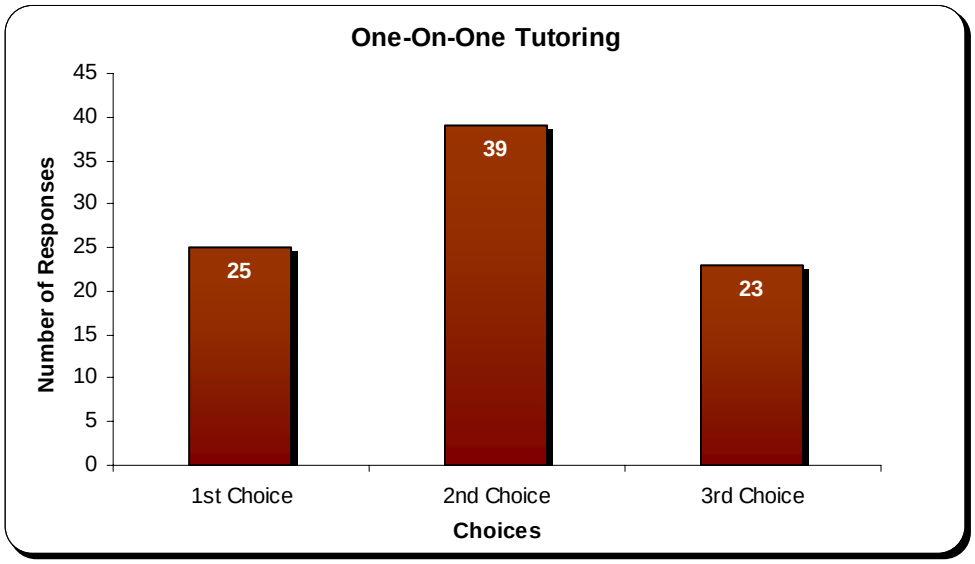
The top choices are as follows:

Category	1st Choice	2nd Choice	3rd Choice
Hands-on classes	104 votes		
Self-paced computer-based training	31 votes	44 votes	46 votes
One-on-one training	25 votes	39 votes	
Lecture / Demonstration		40 votes	45 votes
Online courses			31 votes

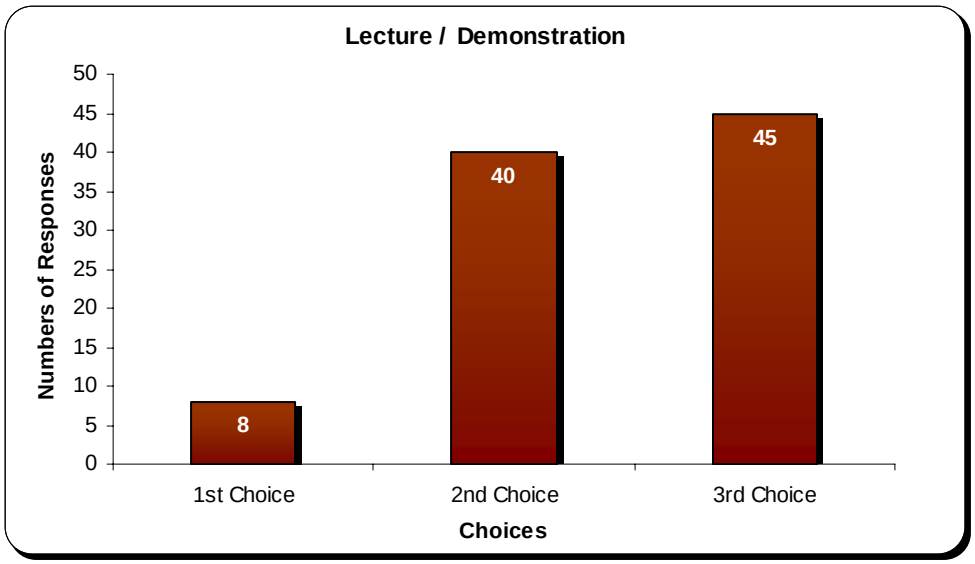
QUESTION 20A = HANDS ON CLASSES
TOTAL RESPONSES 168 OUT OF 194



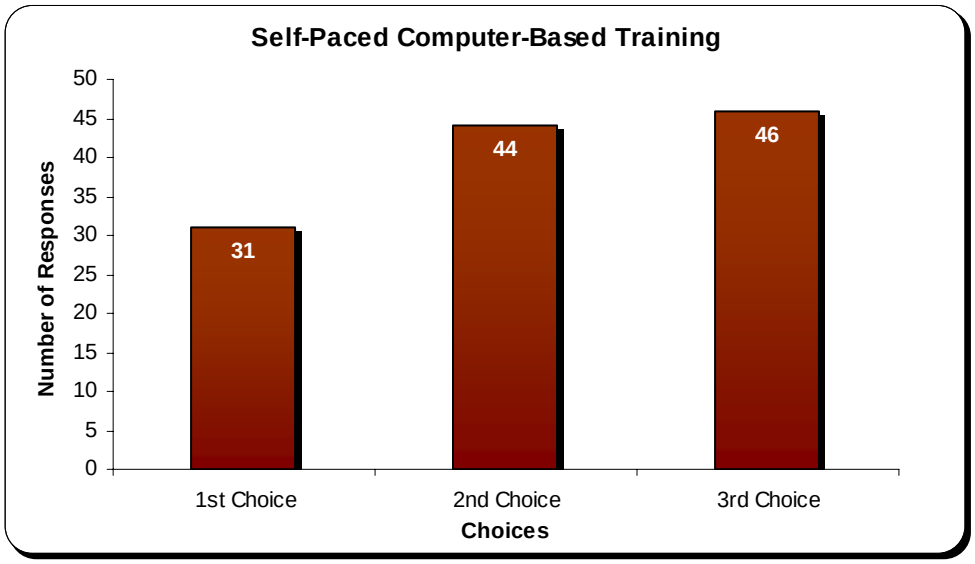
QUESTION 20B = ONE-ON-ONE TUTORING
TOTAL RESPONSES 87 OUT OF 194



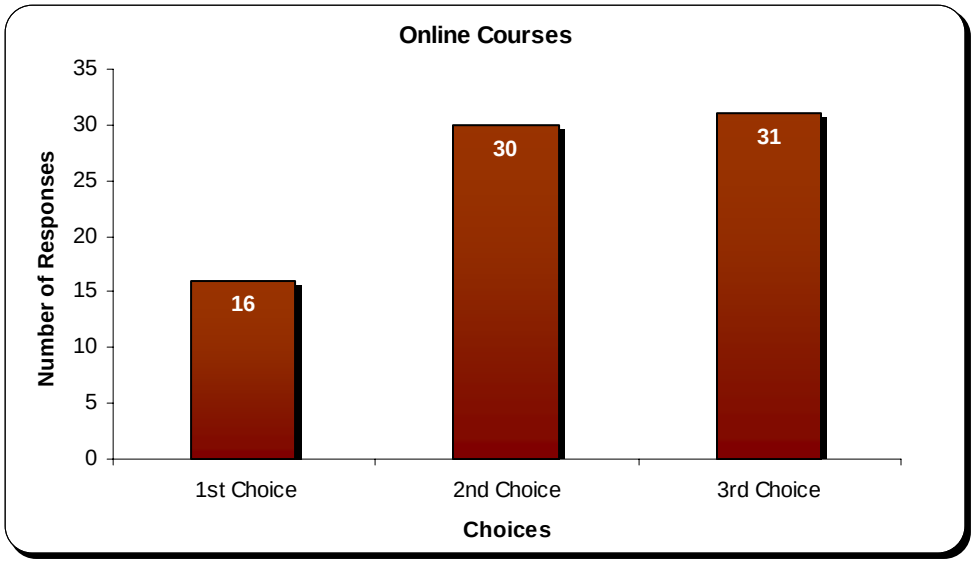
QUESTION 20C = LECTURE / DEMONSTRATION
TOTAL RESPONSES 93 OUT OF 194



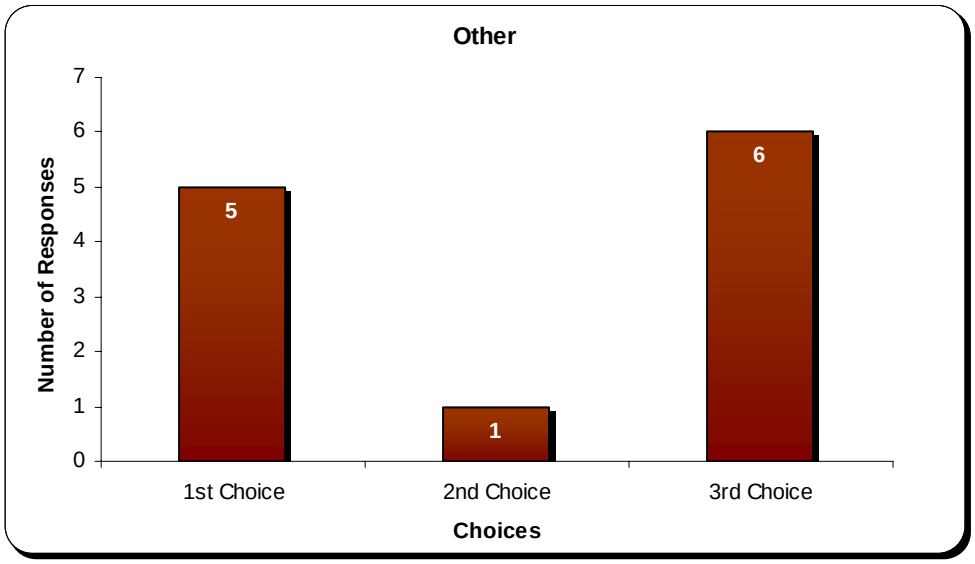
QUESTION 20D = SELF-PACED COMPUTER-BASED TRAINING
TOTAL RESPONSES 121 OUT OF 194



QUESTION 20E = ONLINE COURSES
TOTAL RESPONSES 77 OUT OF 194



QUESTION 20F = OTHER
TOTAL RESPONSES 12 OUT OF 194

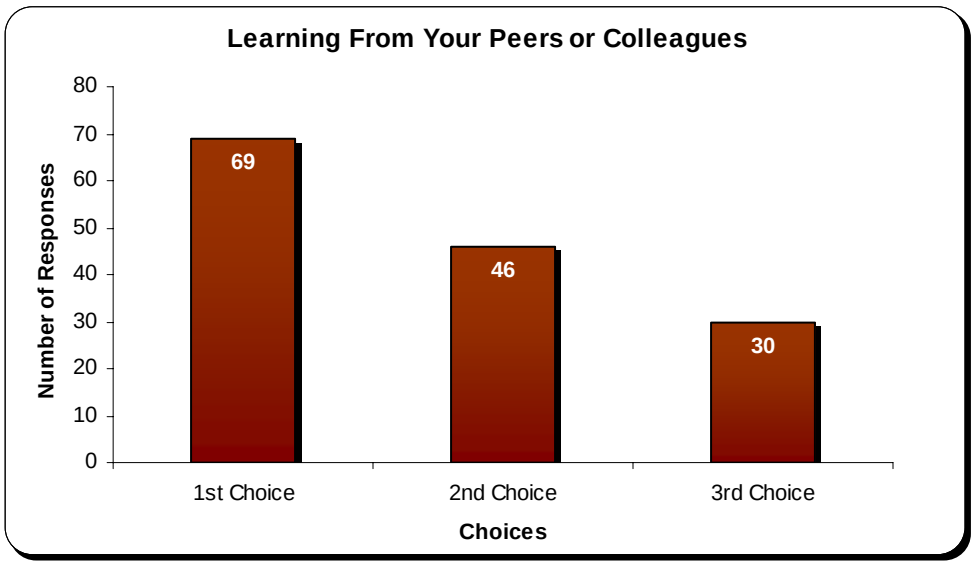


21. Please select in order of importance to you the top three sources for learning additional computer-related knowledge or skills. (Rating: 1 = first choice 2 = second choice 3 = third choice etc.)

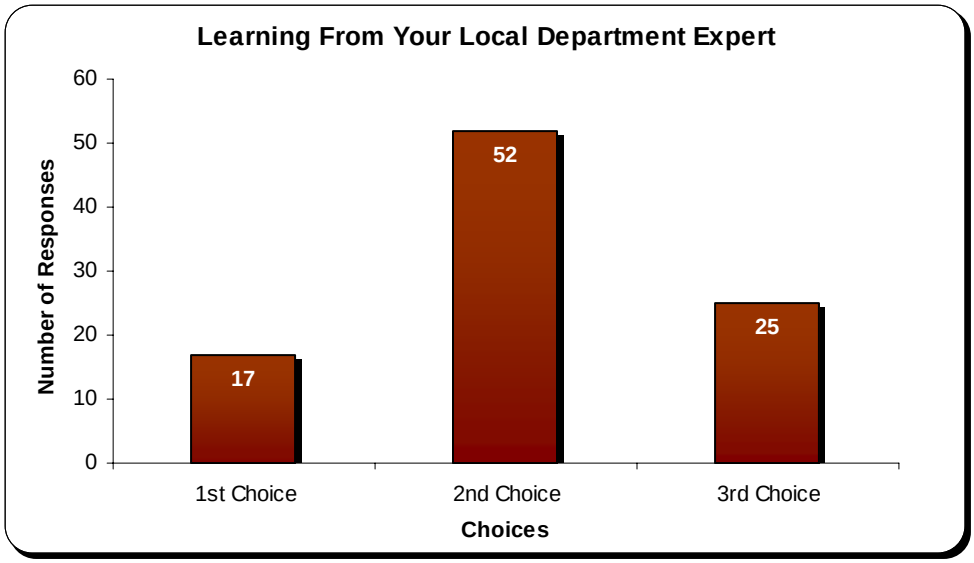
The top choices are as follows:

Category	1st Choice	2nd Choice	3rd Choice
Your peers or colleagues	69 votes	46 votes	30 votes
Your college IT/ IS department	59 votes	38 votes	40 votes
Information outside of KCCD	22 votes		
Your local department expert		52 votes	25 votes

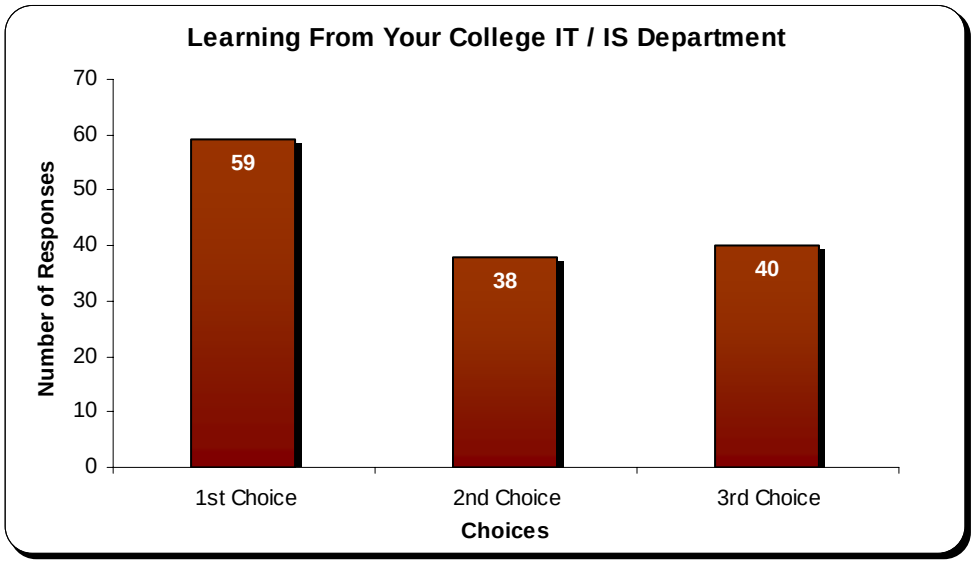
QUESTION 21A = LEARNING FROM YOUR PEERS OR COLLEAGUES
TOTAL RESPONSES 145 OUT OF 194



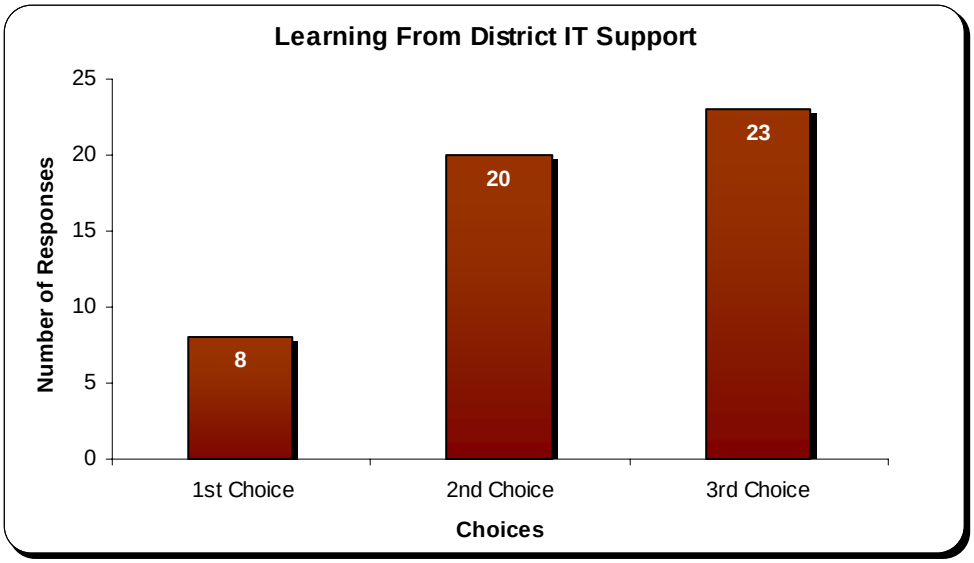
QUESTION 21B = LEARNING FROM YOUR LOCAL DEPARTMENT EXPERT
TOTAL RESPONSES 94 OUT OF 194



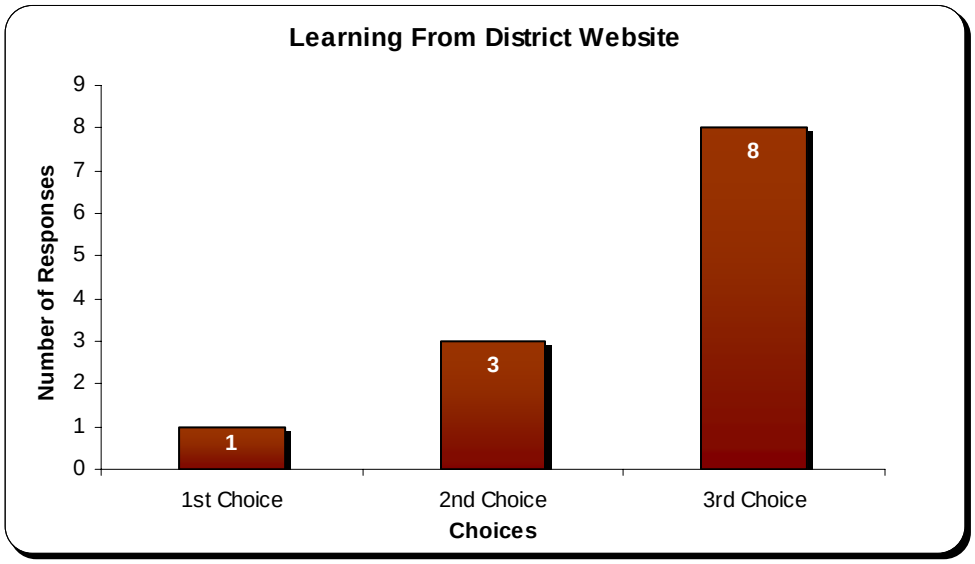
QUESTION 21C = LEARNING FROM YOUR COLLEGE IT / IS DEPARTMENT
TOTAL RESPONSES 137 OUT OF 194



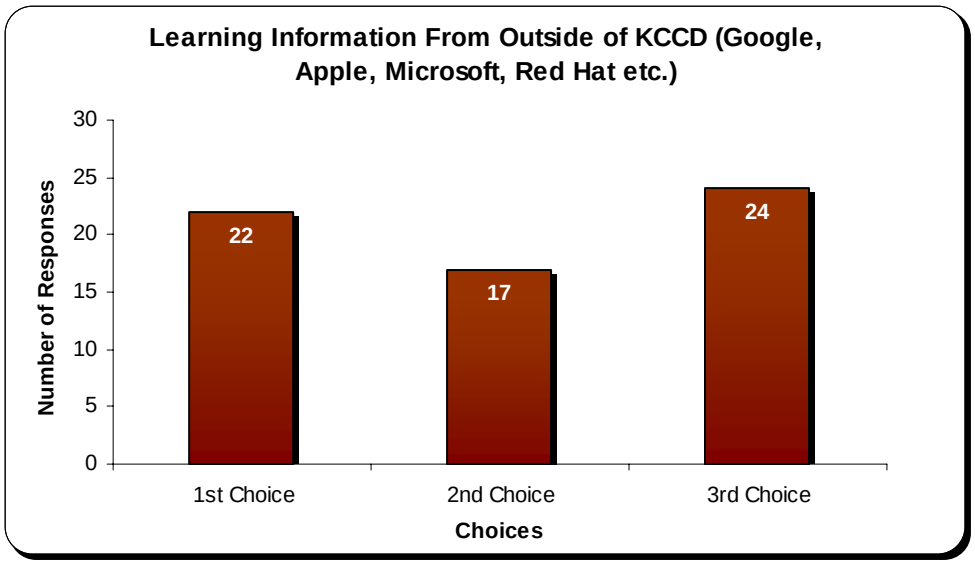
QUESTION 21D = LEARNING FROM DISTRICT IT SUPPORT
TOTAL RESPONSES 51 OUT OF 194



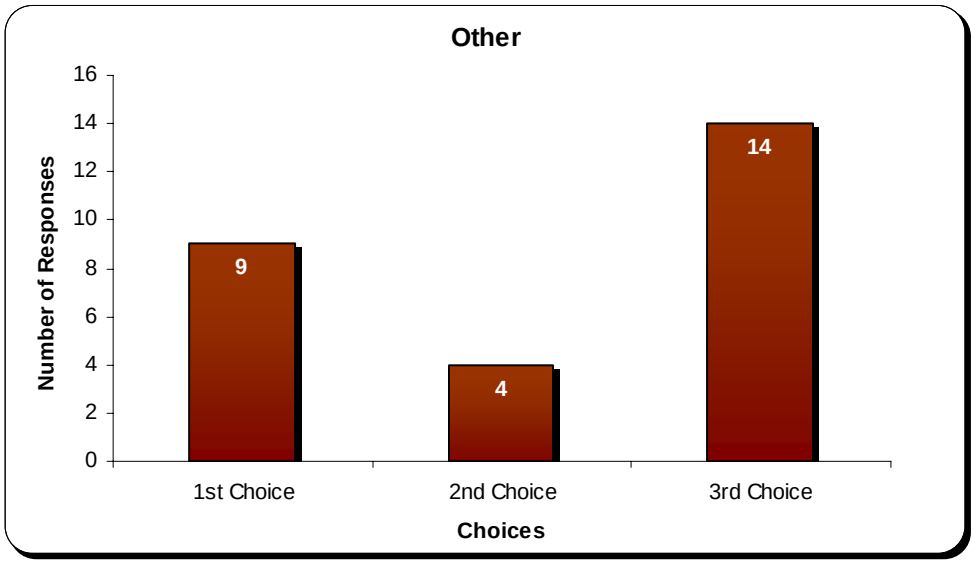
QUESTION 21E = LEARNING FROM DISTRICT WEBSITE
TOTAL RESPONSES 12 OUT OF 194



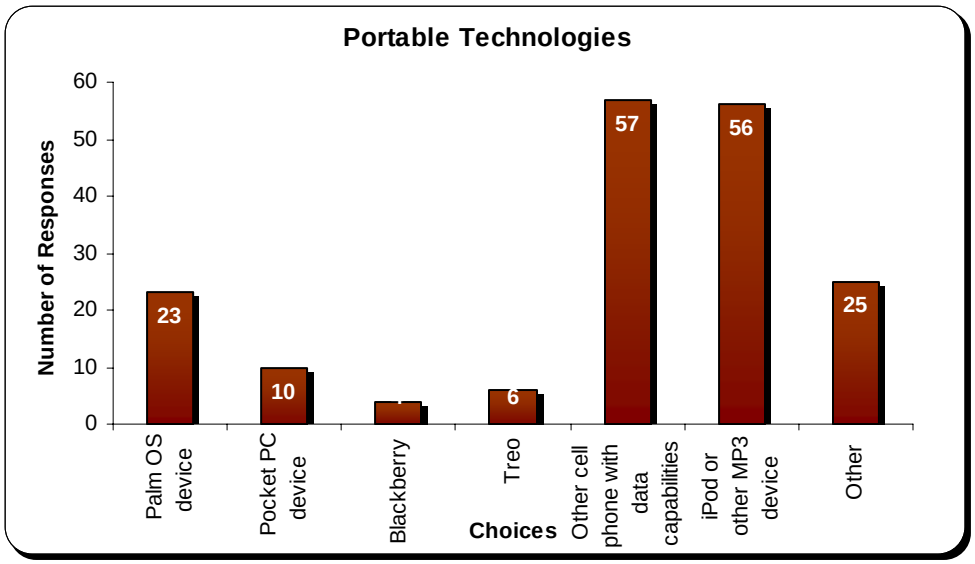
QUESTION 21F = LEARNING INFORMATION FROM OUTSIDE OF KCCD
TOTAL RESPONSES 63 OUT OF 194



QUESTION 21G = OTHER
TOTAL RESPONSES 27 OUT OF 194



22. Which of the following portable technologies do you use? Check all that apply. TOTAL RESPONSES 118 OUT OF 194



Other:

- Laptop
- I'm not that lucky.
- Voice recorder hand-held; voice recognition software;
- None
- None
- wireless mic remote PPT changer
- None
- I wouldn't mind learning how these applieances worked outside of the classroom if there was a demonstration available.
- Laptop
- none of the above
- laptop
- Bluetooth (cell phone to car and motorcycle com. systems). GPS systems.
- N/A

- portable computer
- none
- Laptop
- Wireless laptop
- I don't use any of these.
- Laptop
- Laptop
- don't use
- Just a cell phone for talking. Sorry, I'm not a very technical person!
- USB Drives
- Phone, PSP, NDS, Laptop

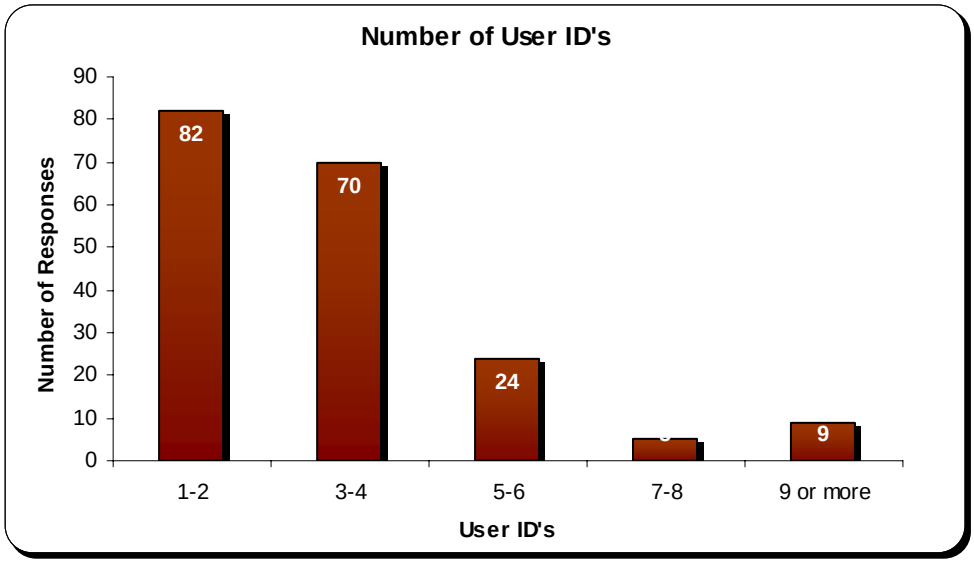
23. What software or services would you like to be able to access via portable devices? TOTAL RESPONSES 32 OUT OF 194

- Attendance and grading software
- none... ipod is for running with... I don't use it for work!!!
- Internet
- If I had a portable device, I would want to be able to access the New Student Orientation located on the server used for my storage.
- Outlook calendar
- laptop if needed
- I would the ability to load my Palm OS on my computer so I can actually use the Palm in the manner that would be helpful.
- Gradebooks
- I am satisfied with what I have via my Treo.
- n/a
- None

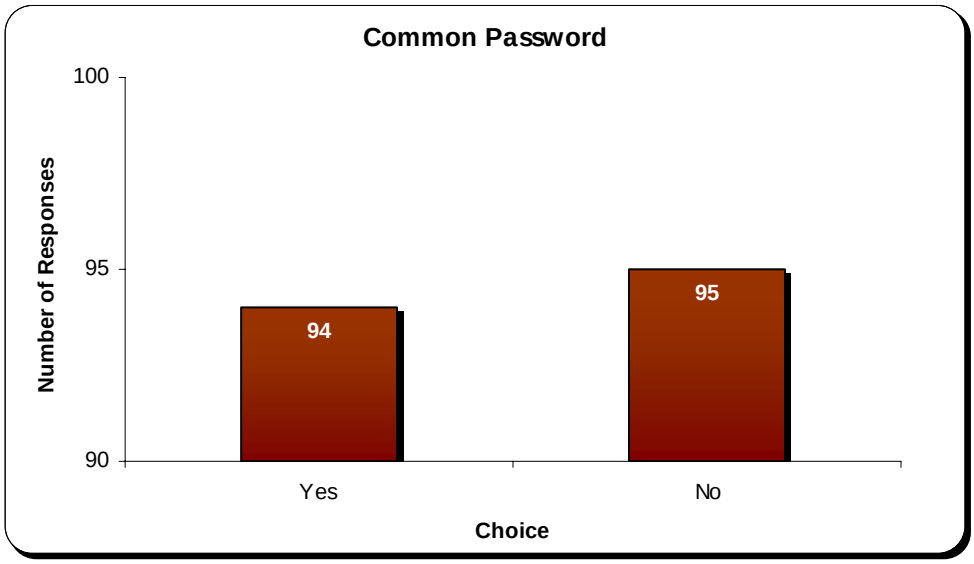
- Student database
- Not sure
- Banner access services
- Outlook, Banner
- None
- Banner
- Outlook calendar
- None
- n/a
- None
- None
- Banner
- Palms
- I'd like to be able to print from my wireless laptop easily, and access it in a lab easily.
- I have not had the opportunity to use any of these or shown how these work. So I am not sure what the purpose or function are for each of these or how it would benefit me. I would love to learn more.
- What I have is fine.
- No comment
- Faculty would like to begin podcasting
- On days I work from home, it would be great to be able to access documents on my work computer through the internet/network.
- wireless networking
- everything

User ID, Passwords and Privacy

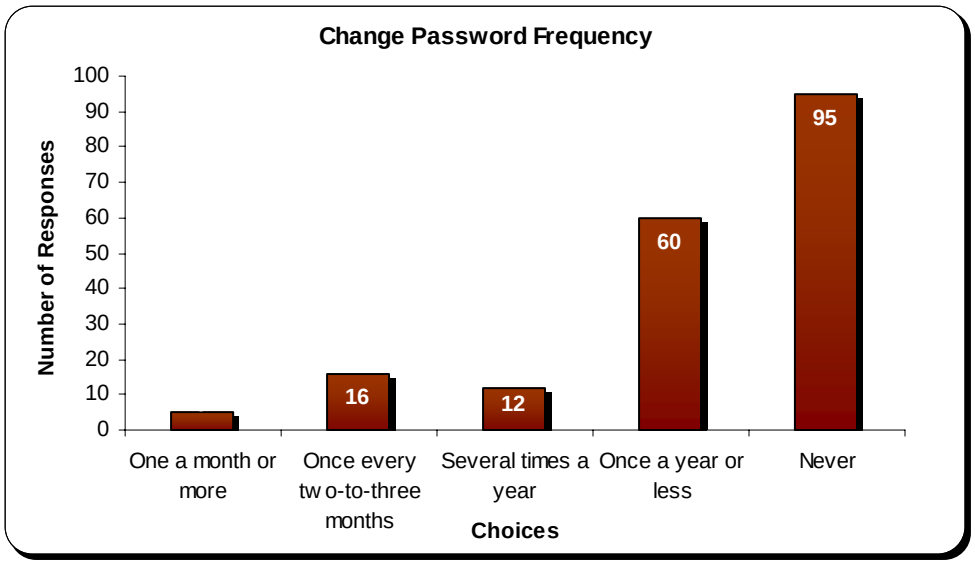
24. How many different User ID's do you use and remember as a part of your work? (e.g., Banner eMail Hershey system network login etc.) TOTAL RESPONSES 190 OUT OF 194



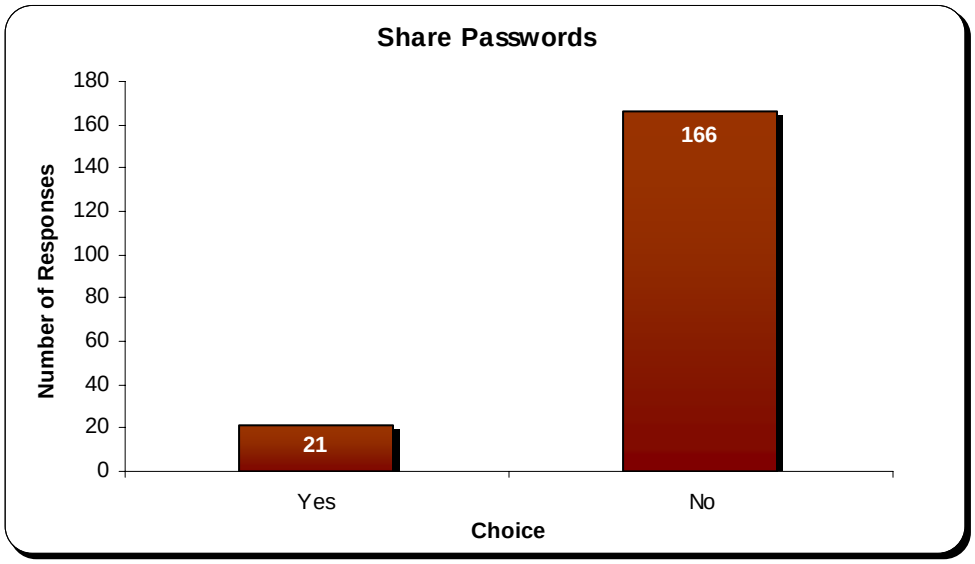
25. Do you use a common password for different login applications? (e.g., Banner eMail Hershey system network login etc.) TOTAL RESPONSES 189 OUT OF 194



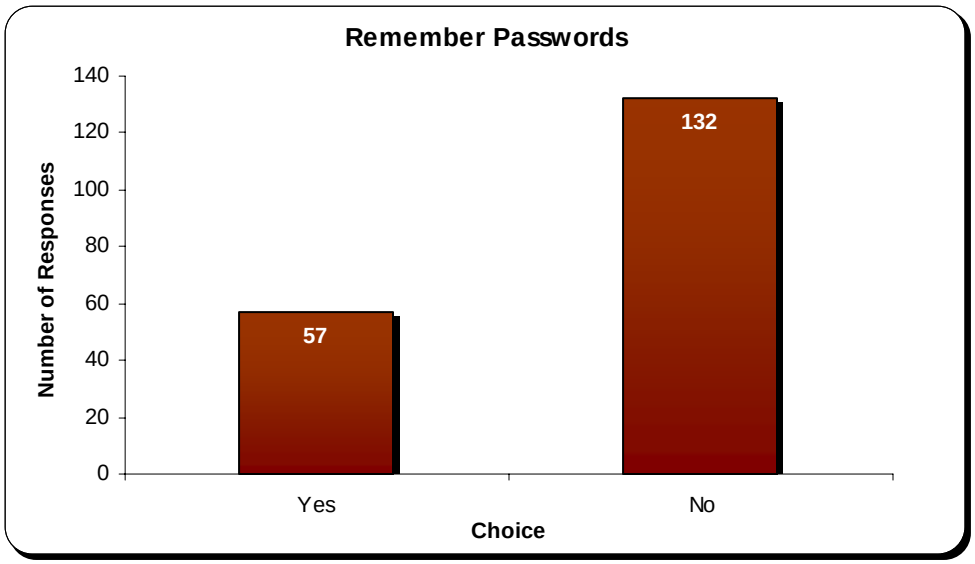
26. On average how often do you change your login passwords? TOTAL RESPONSES 188 OUT OF 194



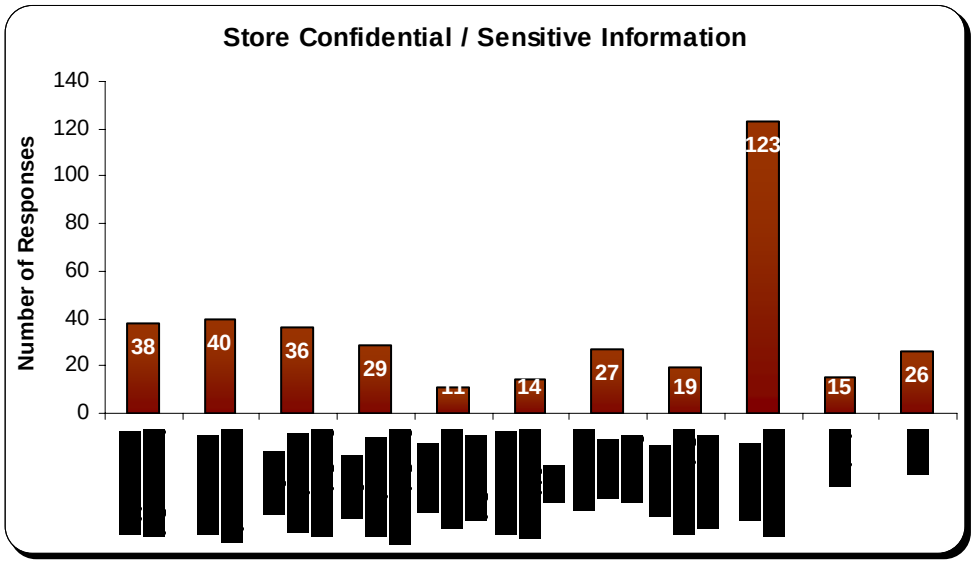
27. Have you shared your password with others? (excluding IT staff such as help desk) TOTAL RESPONSES 187 OUT OF 194



28. Do you write down your passwords in order to remember them? TOTAL RESPONSES 189 OUT OF 194



29. Where do you store confidential / sensitive information (e.g., social security numbers citizen visa code citizenship home phone numbers health records etc.)? Check all that apply. TOTAL RESPONSES 177 OUT OF 194



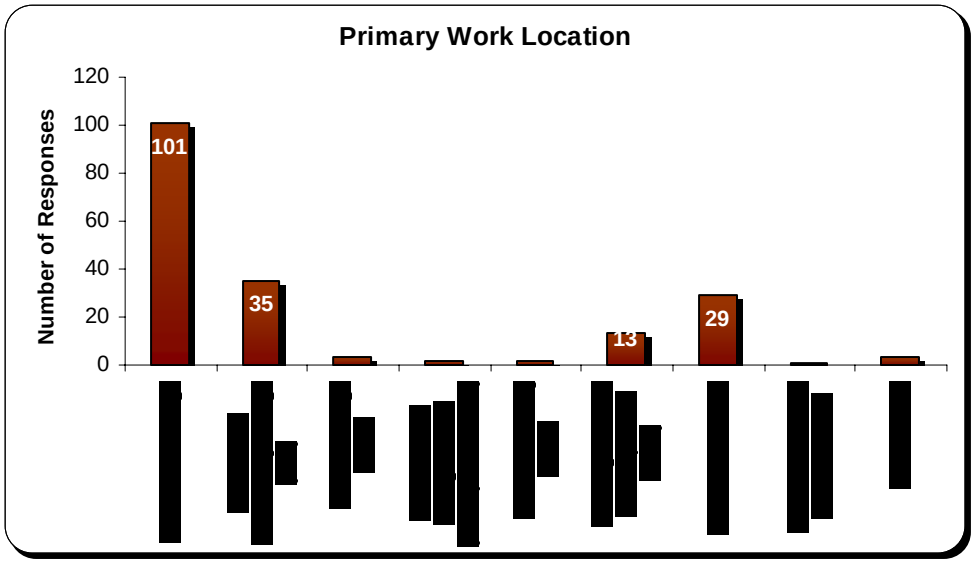
Other:

- I don't store sensitive information on my computer, but I know that the district has all my personal information in banner/banweb.
- They are kept in a separate hard copy file
- I use little sticky notes all over the place. No one else can find the information I save because there are so many notes.
- I keep senstive data in locked cabinets and encrypted, password protected spreadsheets. I do not keep work related content at home.
- safe deposit box at bank in home neighborhood
- Email messages to self
- memory,safe
- I may have some at work but it has been awhile
- Outlook Notes
- I don't store such information, aside from grades. I do access such information via Banner.
- I keep my personal information in a notebook. I won't keep information that important in an electric device. I don't have or keep confidential/sensitive info on co-workers or student workers.
- Microsoft Outlook
- address book
- in my head
- Gave a list to my boss in case I die or leave (work relate logins).
- Do not work with any of these files!
- Only 'sensitive' info I store would be student grades, work phone numbers,and work e-mail addresses, not SS numbers or any home numbers or addresses.
- Memorize them. I don't believe in storing passwords beyond the time it takes to learn them. That is why I marked paper. I write them down initially and then destroy them when I have the information memorized.
- Nowhere
- My head

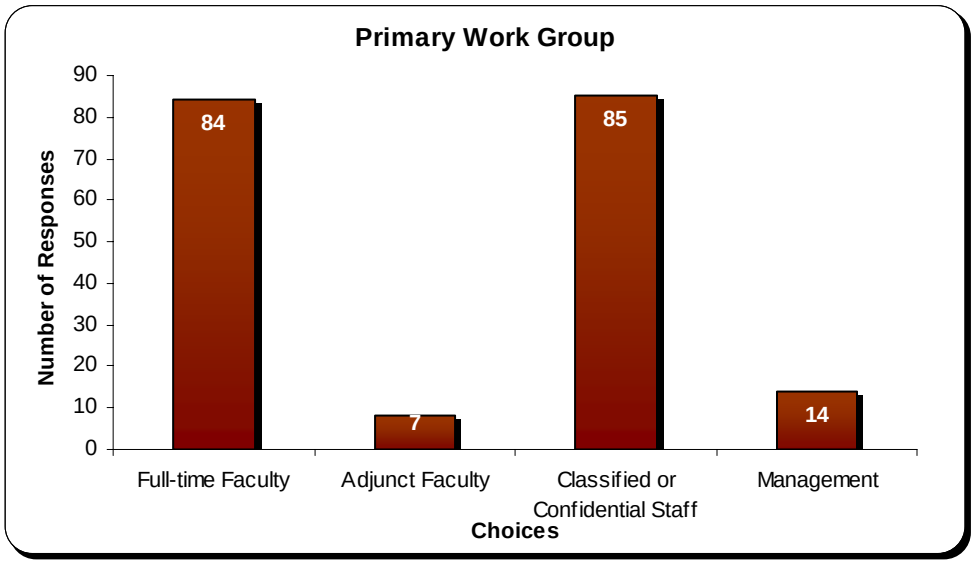
- safe at home
- Do not store phone numbers or any other personal information except within the contacts section of Outlook.
- Post-it note stuck to my computers
- I carry on my person a pocket calendar with my info.
- If I tell you then it won't be confidential :-0
- My Brain

Tell Us About Yourself

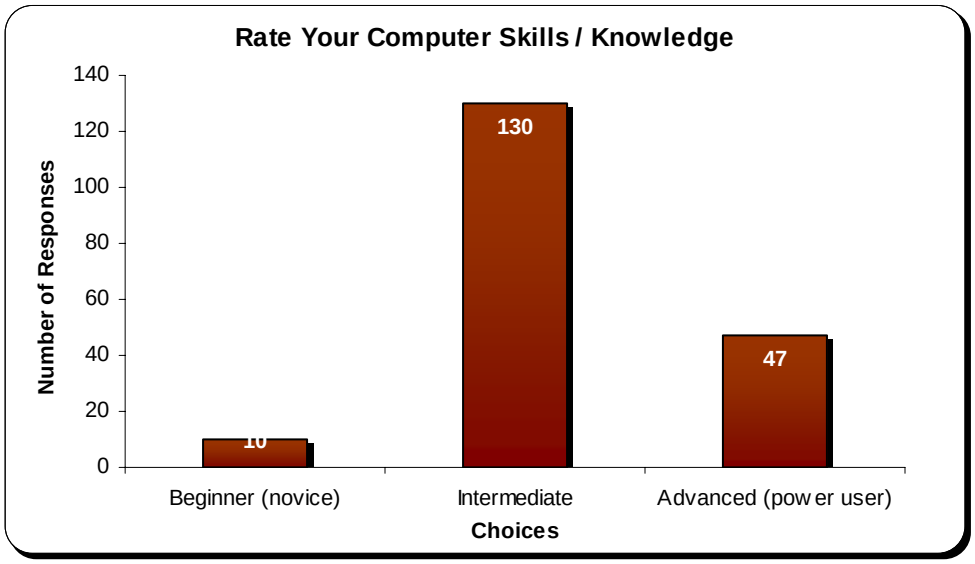
30. What is your primary work location? TOTAL RESPONSES 189 OUT OF 194



31. What is your primary group? TOTAL RESPONSES 190 OUT OF 194



32. How would you rate your computer skills and knowledge? TOTAL RESPONSES 187 OUT OF 194



Next Steps

Porterville College

An Interim IT Assessment presentation and discussion was conducted with the DWITC on Friday, March 9, 2007. During this meeting, SunGard Higher Education reviewed and elaborated on the best practices already in use within the district as well as the key gaps identified during the IT Assessment. The purpose of the preliminary review was to begin the process of identification and understanding of the issues by all stakeholders; address and eliminate any possible disagreements or dissention; and to begin thoughts on the next steps and final presentation.

It is important to begin to focus on the immediate next steps that should be taken at the conclusion of the assessment. After a reasonable review and discussion on findings and recommendations, it is imperative to select from the suggested top priorities and began with an action plan.

As an added value, there is a rich selection of tools that can be used to navigate the roadmaps – or recommendations – that have been made in this report. These navigational tools represent best practices that can be immediately considered and tailored for use within KCCD. It is usually easier to critique and modify an existing best practice to address the unique needs of an institution than to create something new from scratch. Obviously, the degree of required tailoring will vary for each navigational tool.

The obvious difficulties are the lack of available and appropriate resources to implement many of these recommendations. The majority of existing staff are preoccupied with current operations or projects. In many cases the required talents or backgrounds necessary to implement these recommendations may be missing within KCCD. As such, KCCD should consider the temporary use of facilitators, contractors or consultants to act as the catalysts for change. Any use of such temporary staff should offer ideal mentoring, coaching, professional development, or cross-training of existing staff during their engagements. After such temporary staff have completed their engagements and cross-training then the existing KCCD staff will be able to continue to manage, operate and maintain any changes that have been put into place.

Throughout the implementation of the IT assessment next steps, and particularly at the beginning, it is important that KCCD use the proposed IT governance structure to monitor and control this implementation project. The governance structure should assign the required resources and then hold them accountable for successful completion of the next steps. This drive for stronger governance and requisite accountability will be key to the empowerment of KCCD's user community in improving the deployment and use of IT.

A large part of the value of an assessment report must be measured on the positive impact it makes on its subject area in the future. The consensus and understanding of the issues that must be addressed have been placed in their prioritized order within a proposed Short-Term Improvement Program (STIP) named the "KCCD IT Assessment Implementation Program". It is recommended that KCCD consider and adopt a selection of the high priority activities identified within the program immediately to begin making progress.

A list of suggested project resources for the STIP is presented in the final navigational tool. A suggested schedule of activities is also presented. This largely mirrors the suggested priorities assigned and suggests working time, durations, and resource assignments for each. Finally, the detailed list of activities and schedules are itemized for each of the participants.

It is suggested that KCCD consider and adopt this STIP immediately to begin making the recommended improvements to the IT Assessment Implementation program. The agreed upon prioritized activities of the proposed project schedule should be tracked and controlled in “digestible pieces”. Discussions on specific priorities, realistic deadlines, and expected deliverables have begun with the project schedule as a guideline. Tasks of high priority should be the focus of activities between now and the beginning of the next academic year.

Roadmap Navigational Toolkit

Cerro Coso Community College

Each of the findings in the previous sections has a roadmap that KCCD can follow to avoid the impacts and to move into the Next Steps section. It is appropriate to make use of best practices as your navigational tools to follow the roadmap. The development of the following navigational tools is intended to specifically jump start KCCD in their journey towards a service-oriented, unified digital campus. The duration of the journey to the desired destination can be obtained by the effective, combined use of the roadmap and navigational tools.

- Contingency & Recovery Planning: Checklist for Information Systems Academic and Administrative Departments (PAGE 199)
- Disaster Recovery Plan: Activating the Plan (PAGE 204)
- KCCD IT Security Plan to Protect Private Data on Computers (PAGE 205)
- Site Proprietary IT Policy & Procedures Guide – Change Management (PAGE 205)
- Change Management Responsibilities (PAGE 209)
- Change Request Form (PAGE 210)
- Change Management Request Form Instructions (PAGE 211)
- IT 2007 Annual Work Plan (PAGE 213)
- Help Desk Professional Development Plan (PAGE 214)
- MS Access Database Self Assessment (PAGE 216)
- Banner Student – Role Based Assessment (PAGE 217)
- Information Technology Project Request Form (PAGE 218)
- Information Technology Project Scorecard (PAGE 219)
- Information Technology Survey Instrument (PAGE 221)
- IT Security for Higher Education: A Legal Perspective (PAGE 228)
- IT Assessment Implementation Program Plan (PAGE 245)

Contingency & Recovery Planning

CHECKLIST FOR INFORMATION SYSTEMS
ACADEMIC AND ADMINISTRATIVE DEPARTMENTS

This checklist is designed to help organize and put in place an emergency recovery plan for information systems and computing groups in college and district departments. The purpose is to create a planning tool that would serve to guide college / district IT groups when they embark on the emergency planning process. A series of priorities, task definitions, instructions, flow charts, agreements and reference materials result from following the checklist. When organized into a document these materials become core elements of an information systems contingency and recovery plan. This information systems emergency plan should adjoin the overall department emergency plans for responding to and recovering from a disaster.

Completed	Description
	Section I: Getting Ready
❒	A. Obtain a written commitment from senior management of support for contingency planning objectives.
❒	B. Assemble the contingency planning team to include one or more permanent members from: • College / District IT / IS department staff • Operational unit managers • Facilities management
❒	C. Provide for the planning committee to include participation on an "as needed" basis from the following departments: • Internal audit compliance (Business Services at District Office) • Purchasing / contracts (Business Services at College / District Office) • Health and safety coordination (Human Resources at District Office) • Public safety coordination (Department of Public Safety at Bakersfield & District Office; Maintenance and Operations at Cerro Coso and Porterville) • Office of emergency preparedness coordination (Chancellor's Office) • Insurance / liability (Business Services at District Office) • Real estate services / relocation (Business Services at District Office) • Information Technology including administrative systems and student information systems • Others as required
❒	D. Define the responsibility of planning committee members. Appoint… • Group moderator to facilitate planning meetings • Group scribe to take and prepare meeting notes and agenda's • Group administrator to aggregate meeting materials
	Section II: Gathering Necessary Information – Risk Assessment
❒	A. Prepare a written description of the mission-critical functions of the departments and units.
❒	B. Identify the areas impacted by an emergency: • Functional operation of the department • Service to students / staff • Obligations to vendors / suppliers / funding agencies • Relations with other college departments • Department credibility • Other departmental impacts

Completed	Description
❒	C. Define and establish estimated potential losses and liability to the department due to lost or delayed functions, in order of severity of the emergency:

Severity	$ Amount or Range	Duration
Catastrophic		
Major		
Serious		
Limited		

❒ D. Determine which critical department functions depend on information systems. List critical functions with the associated information system(s). Contingency planning for critical functions beyond their information systems components should be referred to the department recovery planning effort.

❒ E. Establish the vulnerability of information systems by examining possible consequences and frequency of specific emergencies.

Specific Emergencies	Possible Consequences
Earthquake	Prohibited Access
Fire	Disrupted Power
Flood	Mildew or Mold Damage
Hurricane / Tropical Storm	Power Outage
Landslide	Water Damage
Volcano	Smoke Damage
Wildfire	Chemical Damage
Urban Fire	Structural Damage
Severe Winter Storm	Communication Loss
Hazardous Material Incident	Ruptured Gas Mains
Civil Disorder	Other
Nuclear Attack	
Power Failure / Surge	
Sabotage	
Bomb / Explosion	
Other	

❒ F. Using the information in A through E make a prioritized list of mission critical information systems functions for restoration in an emergency.

❒ **Section IIa: Gathering Necessary Information – Resource Assessment**

A. Survey the systems and data which are critical to the department's functions. Develop flow charts of the results. Verify flow diagrams with appropriate system administrator. The survey should ascertain…

- Source of all data used in the system
- Nature of information or report
- Frequency of need for data
- How the data is obtained – e.g., paper, email, remote access download, tape or disk
- Who in the department receives or retrieves data
- Who at the college do you speak to about access to the data, will they be available in an emergency
- What is the impact if this data is not available
- Hardware / Operating system software
- Network
- Application

Completed	Description
❒	B. Identify the areas where the department's responsibility for disaster recovery begins and that of the KCCD Information Technology.
❒	C. Determine if the current backup plan is adequate for the completed risk assessment and includes the following features: • Routine periodic backups • Clear backup strategy (full vs. incremental backups, frequency, etc.) • Off-site storage and retrieval procedures • Alternate processing site (hot, warm or cold site)
❒	D. Complete a resource inventory in each of the following areas (items that may need to be replaced): • Equipment (computer hardware, network hardware or other equipment) • Documentation (procedure manuals / handbooks, software, accounting procedures, communication documentation) • Supplies (current inventory, outstanding orders, special items – e.g., toxic or hazardous materials
❒	E. Define the responsibilities of emergency response team(s).
❒	F. Complete staff responsibility chart for emergency response: • Disaster evaluation team (management level) • Interim operations team • Recovery team
	Section III: Integration with Department Response and Recovery Planning
❒	A. Specify who is authorized to declare a disaster and activate the information systems emergency plan.
❒	B. Define the department's immediate response actions by referring to the Public Safety at Bakersfield College and District Office or Maintenance and Operations at Cerro Coso and Porterville College for evacuation and notification of staff. • Accounting for staff and others in the building • Meeting location of disaster evaluation team • Reaching staff needed for emergency response (list of home telephone numbers, cellular phone or radio contact)
❒	C. The department recovery plan should define "manual" processes that can be used until computer resources are recovered. This need for parallel paper process is beyond the planning scope of KCCD IT. It needs to be defined by a department administrative recovery team and should include: • Stock the required forms • Pre-assign job numbers, PO numbers, work order numbers, service request numbers, etc. • Document procedures to merge the manually tracked data with the information on the system once it is restored • Document all manual procedures • Prescribe how the impact of changes in procedures will be clear to customers, suppliers or vendors
	Section IV: Interim Operation Plan – Prearranged Agreements for Resource Replacement
❒	A. Possible other alternative sites: • Other company with similar facilities • Other company in the immediate geographical areas • Computer manufacturer's facilities (or other suggestions from them) • Service bureaus in the immediate area

Completed	Description
❒	B. Considerations for alternate site selection: • Building type • Floor capacity – space and load • Raised flooring • Electric circuits / capacity / special connectors • Air conditioning and humidity control • Chilled water • Fire protection and suppression • Security – personnel • Security – physical • Security – data • Staff accommodations • Communications (telephones, network between departmental systems and access to other data, physical access to systems with critical data which are not accessible remotely)
❒	C. Back-up agreements • Written guarantee or contract with other companies • Reciprocal agreements • Service bureau commitments • Vendor commitments
❒	D. Alternate hardware • Computer and components (CPU model, memory, operating system, options, peripherals) • Network equipment and wiring • Terminals • Off-line equipment • Furniture • Office machines (phones, faxes, etc.)
❒	E. Supplies • Paper • Forms • Disks • Tapes (reel, cartridge (type))
❒	F. Off-site moving plan • Transportation of staff • Transportation of data and supplies • Staff phone list • Other
	Section V: Test, Evaluate and Update the Plan
❒	A. Specify periodic testing of the contingency plan to assure processing compatibility: • Frequency • Scope • Test data • Test evaluation team
❒	B. Periodically review and update of emergency response documentation • Staff responsibility charts • Staff telephone numbers • Vendors • Software license agreements • Alternate site agreements

Completed	Description
	• Inventory of computer hardware and software • Interim operations procedures
❒	C. Periodically review and drill emergency response and recovery teams: • Tabletop exercise to test documentation and communication in controlled environment • Functional exercise to test documentation, communication and procedures in controlled environment • Field exercise to test documentation, communication, procedures and logistics in a simulated "real" environment
	Section VI: Recovery and Restoration
❒	A. Permanent site preparation: • Building • Floor capacity – space and load • Raised flooring • Electric circuits / capacity / special connectors • Air conditioning and humidity control • Chilled water • Fire protection and suppression • Security – staff • Security – physical • Security – data • Communications (telephones, network between departmental systems and access to other data, physical access to systems with critical data which are not accessible remotely)
❒	B. Procurement of hardware • Acquisition (purchase, lease, donation, loan) • Computer and components (CPU model, memory, operating system, options, peripherals) • Network equipment and wiring • Terminals • Off-line equipment • Furniture • Office machines (phones, faxes, etc.)
❒	C. Supplies • Paper • Forms • Disks • Tapes (reel, cartridge (type))
❒	D. Parallel operations plans
❒	E. Migration plan
❒	F. Procedures to close down the interim operation

Disaster Recovery Plan: Activating the Plan

Last update: January 31, 2007

Determine Personnel Status

One of the Incident Manager's important early duties is to determine the status and availability of personnel.

Equipment / Media Protection and Salvage

A primary goal of the recovery process is to restore all computer operations without the loss of any data. It is important the TBD coordinator immediately set about the task of protecting and salvaging any magnetic media on which data may be stored.

Establish the Recovery Control Center

The Recovery Control Center is the location from which the disaster recovery process is coordinated. The Incident Manager should designate where the Recovery Control Center is to be established.

Activating the Disaster Recovery Plan

The Incident Manager sets the plan into motion. Early steps to take are as follows:

a. The Incident Manager should obtain an up-to-date copy of the Disaster Recovery Plan (online if accessible or diskette, thumb/flash drive, CD-ROM, etc.). Copies of the plan should be made and handed out at the first meeting of the Incident Management Team.

b. The Incident Manager is to call a meeting of the Incident Management Team at the Recovery Control Center or a designated alternate site. The following agenda is suggested for this meeting:
   - Each member of the team is to review the status of their respective areas of responsibilities.
   - After this review, the Incident Manager makes the final decision about where to do the recovery.
   - The Incident Manager briefly reviews the Disaster Recovery Plan with the team.
   - Any adjustments to the Disaster Recovery Plan to accommodate special circumstances are to be discussed and decided upon.
   - Each member of the team is charged with fulfilling his/her respective role in the recovery and to begin work as scheduled in the Plan.
   - Each member of the team is to review the makeup of their respective recovery teams. If individual's key to one of the recovery teams is unavailable, the Incident Manager is to assist in locating others who have the skills and experience necessary, including locating outside help from other are computer centers or vendors.
   - The next meeting of the Incident Management Team is scheduled. It is suggested that the team meet at least once each day for the first week of the recovery process.

3. The Incident Management Team members are to immediately start the process of contacting the people who will sit on their respective recovery teams and call meetings to set in motion their part of the recovery.

4. The Administrative Coordinator should begin locating baseline facilities for the recovery room: Office desks and chairs, telephones, PCs, printers, fax machine, and copier.

5. Mobile communications will be important during the early phases of the recovery process. This need can be satisfied through the use of cellular telephones and/or two way radios. KCCD has an existing contract with TBD, and Maintenance & Operations and Public Safety have two-way radio units that may be available upon request.

IT Security Plan to Protect Private Data on Computers

The local data owner(s) and the technical support person or group should complete this form for each computer that stores Private Data. Department head should review and sign this form. Completed forms should be filed in the department office and reviewed and updated annually.

General Information

Department: Computer Name: Computer Location (Building and Room #):

Type of Private Data Stored:

- ❒ Health information on individuals other than students or employees
- ❒ Non-public student data
- ❒ Non-public employee data
- ❒ Other legally protected, contractually protected or non-public data

Describe:

Volume: ❒ High (> 1,000 records) ❒ Medium (100 – 1,000 records) ❒ Low (< 100 records)

Description of System (include the operating system, what applications will be accessing the data, other kinds of applications allowed on the same computer):

Contacts

Local Data Owner(s):	Phone: _ _ _-_ _ _ - _ _ _ _
Local Tech Support:	Phone: _ _ _-_ _ _ - _ _ _ _
Security Contact:	Phone: _ _ _-_ _ _ - _ _ _ _
Alternate Security Contact:	Phone: _ _ _-_ _ _ - _ _ _ _

System meets the following baseline technical requirements to protect private data (Y/N):

1. ( ) Configuration and maintenance: Computer is maintained in accordance with applicable security guidelines.
2. ( ) Authentication and encryption: Access to private data is authenticated – e.g., with a strong password). If sent across the Internet both the authentication data – e.g., user ID and password) and the data itself are encrypted with strong encryption.
3. ( ) Anti-Virus Technology: Anti-virus or filtering software is installed and updated automatically daily.
4. ( ) Firewall or Filtering: A firewall or other communication filtering (e.g., port or IP address filtering) technology is used to limit network access to the device.
5. ( ) Access: Local access to computer is restricted when not in use.
6. ( ) Security event logging: Security log files are configured and reviewed regularly for anomalies – e.g. large # of login attempts at odd times.
7. ( ) Vulnerability scans: Computer is scanned at least quarterly by college / district IT and corrective actions taken as appropriate.
8. ( ) Backups and physical security: Periodic backup copies of software and data are made, tested and stored securely. The physical security of the hardware and removable media are maintained and plans made to allow recovery from unexpected problems. Use a "secure deletion" program to erase data from hard disks and media after done using and also prior to transfer or disposal of hardware.

If you answered No, describe why. Identify any risk mitigation plans, including target dates, if necessary.

Security Plan

Describe the risks, measures to mitigate the risks and the actions to be taken and by whom.

Risk:

Measures to Mitigate Risks and who is responsible:

Signatures

Created By: Date: _ _ / _ _ / _ _ Last Reviewed By: Date: _ _ / _ _ / _ _

Site Proprietary: IT Policy and Procedures Guide

DATE	SUBJECT	NUMBER
04/01/2006	Change Management	I.1

I. Need for Policy

As part of the support and delivery of all applications and network systems, it is necessary to define the change management structure, the reporting responsibilities, the roles of individuals and groups throughout IT.

II. Definitions

A. **User Requested Changes** - Changes to production systems or hardware requested by the end user of the product.

B. **Staff Requested Changes** - Changes to software or hardware requested by IT staff.

C. **Vendor Changes** - Any changes caused by the vendor, either software or hardware, for which the vendor is ultimately responsible.

D. **Production Systems** - The application software currently being used by IT in support of its business operations.

E. **Protocol** - The chain of authority with respect to change review and approval.

III. Statement of Policy

The purpose of this policy is to provide a framework for managing change across all college and district IT departments.

IV. Procedures

A. Definition:

1. **Change Coordinator (CC) –** The individual responsible for administering and coordinating the IT Change Management System. Evaluates the effectiveness of the Change Management process.

2. **Requester –** IT personnel requesting the implementation of a change.

3. **Change Advisory Board (CAB)**
Attendees are but not limited to:

Bakersfield College
- Director of Information Services
- Network Manager
- IS Technical Coordinator
- Network Technician
- Other departments as needed

Cerro Coso Community College
- Dean / Director of Information Technology

- Network Manager / Administrator
- Other departments as needed

Portersville College
- Dean / Director of Information Technology
- Network Manager / Administrator
- Other departments as needed

District IT
- Director of Information Technology
- Assistant Director of Information Technology
- Telecommunications Manager
- Systems Manager
- Network Manager
- Security Manager
- Database Administrator Team Leader
- Systems Analyst / Programmer Team Leader
- Help Desk Technician
- Other areas as needed

4. **Types of Changes**
   - Hardware (servers, routers, firewalls, etc.)
   - Application & Systems software
   - Patches
   - Procedures
   - Environment
   - Documentation

B. Requirements:

1. All requested changes will be documented using the Change Request Form and will be submitted to the CC as explained below.

2. If a change to be implemented has a high impact on end users, systems they use, or the network system as a whole the CAB and CC will determine if additional support is required.

3. If an emergency change is to be implemented untested, the CAB and CC will determine if additional support is required.

4. Only the Director of Information Technology (District Office) (or in their absence a director of equivalent status) has the authority to override scheduled implementation.

5. The Change Request Form must be submitted to the CC as follows:

LEVEL	SUBMITTAL
Major Change (**High Risk**)	At least **30 days before** target implementation date
Minor Change (**Medium Risk**)	At least **7 days before** target implementation date
Routine Change (**Low Risk**)	At least **1 day before** target implementation date
Emergency Change	**As soon as possible**

6. All changes must have a back out plan in writing, are well documented and the procedures are clear.

7. CAB and CC will meet weekly to review requests and make recommendations.

8. Testing must be performed in an appropriate testing area and not on the production network. Changes will then be staged for acceptance. Changes will only be implemented into the production environment upon the Director of Information Technology (District Office) signature that QA testing was conducted.

9. Change is authorized by the Director of Information Technology (District Office) based upon the risk assessments, service levels and provided there is a business justification for the change.

10. Upon approval of the change, the CC will return the original form to the Requester as follows:

LEVEL	SUBMITTAL
Major Change (**High Risk**)	At least **30 days before** target implementation date
Minor Change (**Medium Risk**)	At least **7 days before** target implementation date
Routine Change (**Low Risk**)	At least **1 day before** target implementation date
Emergency Change	**As soon as possible**

11. In an effort to evaluate the effectiveness of the change management process, the CC will present monthly report to the CAB, Director of Information Technology (District Office) and / or IT Governance summarizing changes in the environment. Topical areas include:

- Change category (major, minor, low, emergency)
- Change requests per status (entered, in review, assigned, completed, rejected)
- Time spent on tasks
- Lost time
- Reason for Change (performance, solve problem, new function, maintenance)

12. Post mortems will be convened on an “as needed” basis. Post mortems will be held for changes resulting in significant problems to determine, what, if anything went wrong and how any such problems can be prevented in the future.

V. Exceptions

None.

VI. Interpretation Contact

Director of Information Technology (District Office)

VII. Attachments

Change Management Responsibilities, Change Request Form and Change Request Form Instructions.

VIII. Approvals

Originated by: _____ Originator

Approved by: _____ Standards Committee

Approved by: _____ Director of Information Technology (District Office)

Change Management Responsibilities

Individual	Activities
Requester 	• Completes the appropriate fields on the Change Request Form. See the Change Request Form Instructions. • Acquires Manager sign-off. • Submits detailed implementation and back out plan to the Change Coordinator. • If the change is tested and a target user has been designated, forward a copy of the tested output with the implementation plan for the user approval.
Requester's Manager 	• Indicates approval of change request by signing at top of the form. • Submits Change Request Form to the Change Coordinator.
Change Coordinator (CC) 	• Evaluates change request for completeness of information and determines if requested implementation date is to be accepted. • Notifies Requester if information is incomplete. • Assigns change number. • Logs change request in appropriate logs and schedules change. • Writes date for approved and scheduled request; signs the form. • Obtains approval and signature of the Director of Information Technology (District Office). • Forwards copy of form to Requester. Notifies Requester change approved and scheduled. • Determines success of change. Writes date of change installed. Writes "Y" (yes) for successful and signs initials to indicate verification of success. Writes "N" (no) for unsuccessful and contacts the Change Advisory Board to reschedule a second installation of change. • Fills out final sections of Change Request Form, signs his/her approval, updates the change log and files final form. • Compiles and presents volume statistics to CAB, Director of Information Technology and / or IT Governance.
Change Advisory Board (CAB) 	• Evaluates change request for completeness of information and determines if requested implementation date is to be accepted. • If an emergency change is untested, additional support for the implementation and initial executions may be scheduled. • If the change has high impact on end-users, systems they use, or network system as a whole additional support may be scheduled.
Director of Information Technology 	• Ensures QA testing is conducted. • Authorizes change.

Change Request Form

Requester _____ Change Number_____

Manager _____ Date Submitted_____

Change Category: 1-(MAJOR) 2-(MINOR) 3-(ROUTINE) 4-(EMERGENCY)

Change Has Been Tested: ❒ Yes ❒ No

Change Type: ❒ New Requirement ❒ Requirement Change ❒ Design Change ❒ Other: _____

Change Reason: Solve Problem # _____ ❒ Performance ❒ New Function ❒ Legal ❒ Defect ❒ Maintenance
Other _____

User Areas Affected by Change_____

Components of Change - (Affected Modules, Job streams, Files, Procs, Schedules, etc.) _____
_____

Change Benefit _____
_____

Implication of Not Making Change _____
_____

Planned Installation Date _____ Revised Date _____ Reason _____

Revised Date _____ Reason _____

Amount of Time Required _____

Prerequisites/Special Considerations _____

Resources Required _____

Responsible for Installation _____

Detailed Installation Plan Submitted Date _____ Accepted _____

(Must be submitted 30 days before Major Change; 7 days – Minor Change; 1 day – Routine Change; ASAP – Emergency Change)

Back Out Procedure (Source location, job to run to restore previous status, does not change requester need to be notified before back out.)

_____

Back Out Time Required: _____

Change Control Decision
❑ Approved ❑ Deferred ❑ Rejected _____
CC / Director of Information Technology Signature

Scheduled Implementation _____
Date

Change Installed _____ Successful: ❒ Yes ❒ No
Date

Change Backed Out _____ Reason Code _____
Date

Lost Time (CPU Time) _____ cc:_____
Date

Change Reviewed _____
Date

Change Request Form Instructions

This form is used as a means to communicate change request plans to the Change Coordinator. The Requester will complete all fields in BLUE prior to submitting the form to the Change Coordinator. The Change Coordinator will complete fields in RED. Any additional information is coordinated and obtained by the Change Coordinator.

DETAILED INSTRUCTIONS		
Field Name	**Field Definition**	**Completed By**
Requester	Print the name of the individual making the change.	REQUESTER
Date	Date the Change Request Form is submitted to the Change Coordinator.	REQUESTER
Change Category	The category in which the change is classified. Can be one of the following: Major Change • High risk • Potential to disrupt critical business and/or student activities for many users • Will Affect all users if not implemented successfully • Affects multiple systems or elements of the infrastructure • Complex or lengthy implementation and back out Minor Change • Medium risk • Minor visibility to users and minimal business and/or student impact • Impact limited to specific portions of infrastructure • Quick and fairly simple back out Routine Change • Low risk • No visibility to users and no business and/or student impact • Has been implemented in many other areas with no errors • Routinely done without any failures on the 1st attempt Emergency Change • Critical service is down or severely impaired with disruption to business and/or student activities • Fix first, and document change after the fact	REQUESTER
Change Tested	A response of Yes or No prior to implementation?	REQUESTER
Change Type	Check appropriate type or write a brief description in the "Other" category.	REQUESTER
Change Reason	The appropriate reason for the change or write a brief description in the "Other" category.	REQUESTER
Description	A brief, non-technical explanation of what you are expecting to accomplish by this change.	REQUESTER
User Areas Affected By Change	List all areas, departments, or individuals that will be affected. This will assist the Change Coordinator in determining the schedule of all changes.	REQUESTER
Components of Change	Identify all components, programs, copy books, subroutines, maps, schedules, and documentation which you are changing.	REQUESTER

DETAILED INSTRUCTIONS		
Field Name	**Field Definition**	**Completed By**
Planned Installation Date	Date you expect to install the change.	REQUESTER
Amount of Time	Numbers of minutes of stand-alone system time required to accomplish change.	REQUESTER
Prerequisites Special Consideration	List any special concerns such as requires a specific application to be running or not scheduled, requires on-line files closed, etc. If no special considerations are necessary, indicate this by writing “None” on the line.	REQUESTER
Resources Required	List any special resource requirements such as tape drives, a specific printer, etc.	REQUESTER
Responsible for Installation	Usually this the Requester but may be someone else such as a 3rd party vendor.	REQUESTER
Detailed Installation Plan	Attach plan with Change Request Form.	REQUESTER
Back Out Procedure	Explanation of how to restore previous status of system. This may require that the Requester be contacted before back out procedures begin. This section is mandatory. Attach with Change Request Form.	REQUESTER
Back Out Time Required	Amount of time required to restore old version of program or time required to reformat and / or restore files or system downtime required.	REQUESTER
Manager	Signature of Manager.	REQUESTER
Change Number	An identification number assigned to each change request submitted.	CHANGE COORDINATOR
Request Approved	The date entered indicates when the change implementation request was approved by the Change Advisory Board and Change Coordinator.	CHANGE COORDINATOR
Scheduled Implementation	The date in which the change will be implemented as designated by the Change Coordinator.	CHANGE COORDINATOR
CC	Signature by Change Coordinator indicating that the change has been approved and scheduled.	CHANGE COORDINATOR
Change Installed	The date the change was implemented. Indicate whether or not the change was successful (Y or N). Includes initials and date.	CHANGE COORDINATOR
Change Backed Out	Date the change is backed out.	CHANGE COORDINATOR
Reason Code	The code which indicates why the change was backed out. One of the following four (4) codes is used: B1 – Insufficient testing B2 – User request B3 – Insufficient time to complete implementation B4 – Other	CHANGE COORDINATOR

IT 2007 Annual Work Plan

Status Legend:
New, Scheduled, In Progress, Waiting on Department Approval (WDA), Waiting on Budget Approval (WBA), Resource Not Available (RNA), Test, Completed, Ongoing, Closed, Denied

Project	Description	Projected Start Date	Projected End Date	Status	% Complete	Planned Hours	Actual Hours	Project Lead
Expand Wireless network								
Desktop Refresh Program								
Printer Refresh Program								
MAC Refresh Program								
Network Infrastructure Refresh Program								
Server Refresh Program								
Classroom Projection Systems Refresh Program								
New Staff, Programs or Labs Refresh Program								
Disaster Recovery Plan								
Business Continuity Plan								
Change Management Program								
IT Security Awareness Program								
Communication Plan / Strategy								
Standard Operating Policies & Procedures								
Student Support Help Desk								
Telephone System Upgrade								
Exchange Upgrade								
Help Desk Problem Management System								

Help Desk Professional Development Plan

This Help Desk Professional Development Plan is a collection of technical and professional curriculum intended for staff in the Help Desk area. It was developed based on identified knowledge and skill requirements required based upon current strategic goals, competencies lists, job descriptions, job analysis and task analysis for team members. Taken from a collection of sources it is considered to be a specific plan for {Employee Name}.

Job Title: Help Desk Professional	Today's Date:	_ _ / _ _ / _ _	Requested Completion Date:	_ _ / _ _ / _ _
LAST		FIRST		
Employee Name:	**Doe**	**Jane**		
Department:		Position:		
Phone #:	_ _ _-_ _ _ - _ _ _ _	Hire Date:	_ _ / _ _ / _ _	
Manager's Name: (please print)		Manager's Approval / Signature:		

Week 1	**Estimated Time to Complete**	**Date Scheduled**	**Date Completed**
Attend New Hire Orientation		_ _ / _ _ / _ _	_ _ / _ _ / _ _
Help Desk Orientation and training		_ _ / _ _ / _ _	_ _ / _ _ / _ _
Overview of services		_ _ / _ _ / _ _	_ _ / _ _ / _ _
Help Desk schedule		_ _ / _ _ / _ _	_ _ / _ _ / _ _
Help Desk problem handling procedures & training		_ _ / _ _ / _ _	_ _ / _ _ / _ _
Help Desk software training		_ _ / _ _ / _ _	_ _ / _ _ / _ _
Knowledge base training		_ _ / _ _ / _ _	_ _ / _ _ / _ _
Self Study: 2007 Office Suite, Windows Vista, network fundamentals		_ _ / _ _ / _ _	_ _ / _ _ / _ _
Review detailed job responsibilities description		_ _ / _ _ / _ _	_ _ / _ _ / _ _
Review performance expectations and evaluation methods with Manager		_ _ / _ _ / _ _	_ _ / _ _ / _ _
Details of operations, applications supported, customer base, typical support issues		_ _ / _ _ / _ _	_ _ / _ _ / _ _
Certified Help Desk professional training class		_ _ / _ _ / _ _	_ _ / _ _ / _ _

Subscribe to the following publications: www.callcentermagazine.com, www.cio.com www.ccmreview.com, www.computerworld.com www.customersupportmgmt.com, www.zavata.com		__/__/__	__/__/__
WEEK 1: TOTAL HOURS			

Week 2	Estimated Time to Complete	Date Scheduled	Date Completed
Testing on 2007 Office Suite, Windows Vista, network fundamentals		__/__/__	__/__/__
Self study: Proprietary applications		__/__/__	__/__/__
Self study: Shrink-wrapped applications		__/__/__	__/__/__
Self study: Banner Suite		__/__/__	__/__/__
Help Desk problem-handling training		__/__/__	__/__/__
Recording problems in problem tracking database		__/__/__	__/__/__
Institution proprietary application skills evaluation		__/__/__	__/__/__
WEEK 2: TOTAL HOURS			

Week 3	Estimated Time to Complete	Date Scheduled	Date Completed
Live problem-handling with team member monitoring		__/__/__	__/__/__
Skills testing for proprietary applications		__/__/__	__/__/__
Skills testing for shrink-wrapped applications		__/__/__	__/__/__
Skills testing for Banner Suite		__/__/__	__/__/__
Call-handling evaluation/coaching with team member		__/__/__	__/__/__
WEEK 3: TOTAL HOURS			

Week 4	Estimated Time to Complete	Date Scheduled	Date Completed
Self study: Certified Help Desk Professional exam		__/__/__	__/__/__
Live-call handling with team member monitoring		__/__/__	__/__/__
Certified Help Desk Professional exam		__/__/__	__/__/__
Performance and skills assessment; plan for next evaluation period		__/__/__	__/__/__
WEEK 4: TOTAL HOURS			

MS Access Database Self-Assessment

This assessment is designed to measure your current knowledge of DATABASES. Please answer the following by placing a ✓ in the appropriate box and return to your manager.

Job Title:	Today's Date:	_ _ / _ _ / _ _	Requested Completion Date:	_ _ / _ _ / _ _
	LAST	FIRST		
Employee Name:	**Doe**	**Jane**		
Department:		Position:		
Phone #:	_ _ _-_ _ _ - _ _ _ _	Hire Date:	_ _ / _ _ / _ _	

I Know How	I Need Help	I Cannot	Skill
❒	❒	❒	Calculate totals
❒	❒	❒	Change data alignment
❒	❒	❒	Copy and move records
❒	❒	❒	Copy and move tables
❒	❒	❒	Create a combo box
❒	❒	❒	Create and edit levels
❒	❒	❒	Create bound and unbound controls
❒	❒	❒	Create crosstab queries
❒	❒	❒	Create custom forms
❒	❒	❒	Create filters
❒	❒	❒	Create forms
❒	❒	❒	Create reports
❒	❒	❒	Create select queries
❒	❒	❒	Create tables
❒	❒	❒	Create update queries
❒	❒	❒	Define relational database terminology & concepts
❒	❒	❒	Define relationships between tables
❒	❒	❒	Design data tables
❒	❒	❒	Edit and replace data
❒	❒	❒	Embed bound objects
❒	❒	❒	Identify database components
❒	❒	❒	Import database tables
❒	❒	❒	Import spreadsheet data
❒	❒	❒	Modify defined relationships
❒	❒	❒	Modify table designs
❒	❒	❒	Move and size controls
❒	❒	❒	Print reports
❒	❒	❒	Print selected table columns
❒	❒	❒	Print table records
❒	❒	❒	Save and close tables
❒	❒	❒	Set control properties
❒	❒	❒	Set default values
❒	❒	❒	Set format and other field properties

Banner Student – Role Based Assessment

General Person Training 7.1		1 Admissions & Records - 100	2 Registrar - 5	3 Student Worker - 4	4 Athletics - 8	5 Bookstore - 15	6 Business Office - 20	7 Campus Security - 10	8 Career Center/Job Placement - 9	9 Women's Center - 5	10 Continuing Education- 12	11 Counseling - 60	12 Dean of Students - 6	13 Recruiting - 15	14 Distance Education - 20	15 Library - 6	16 Faculty - 2000	17 Catalog - Curriculum - 3	18 Schedulers - 8	19 Maintenance & Operations - 13	20 IT - 10	21 Research - 10	22 International Students -10		# Required Training
1	Establishing a person/generating an ID	100	5		8				9			60		15		15								212
2	Assigning an address/multiple addresses to an ID	100	5		8				9			60		15		15								212
3	Making changes to a name - TBD																							0
4	Entering multiple telephone numbers	100	5		8				9			60		15		15								212
5	Capturing biographic information	100	5		8				9			60		15		15								212
6	Entering comments - TBD																							0
7	Entering medical information															15								15
8	Entering emergency contact information	100	5		8				9			60		15		15								212
9	Adding or updating appointments and contacts	100	5		8				9			60		15		15								212
10	Assigning and releasing holds	100	5				20	10		5			6											146
11	Produce a person directory report													15										15
12																								
13																								
14																								

This is a very small sample of the Banner Student Needs Assessment and Role Based Curriculum. The tool is used to help institutions plan their end user training providing information regarding who needs training on what tasks and how many total people require training on a given task. These numbers are useful for decisions regarding the delivery method chosen for training, class lists, and curriculum plans for a given role.

*The numbers provided above are hypothetical and subject to change based upon KCCD data.

Information Technology Project Request Form

Project Title:		Submission Date:	_ _ / _ _ / _ _	Request Number: (Assigned by IT)	
Requestor Name(s):					
Job Title(s):					
Phone #(s):	_ _ _-_ _ _ - _ _ _ _		Department:		
College / District:			*e*Mail Address(es):	@ .edu	

Requirements Analysis

+ **Problem Statement**
  - Summarize the problem you propose to address.
  - Write in terms of the problem discovered, not in terms of the solution.
+ **Solution Statement**
  - Summarize the solution.
  - What is / are the key value(s) – e.g., improved quality, reduced labor hours, improved service processes, conformance to regulation / legislation, cost saving, etc.
  - Write in business terms that are easy to understand (no jargon☺).
  - Solution describes what will be implemented, corrected, installed, replaced or otherwise addressed to solve the challenge / problems.
  - How does the solution align with the overall institution's vision, strategic, tactical and operational plans?
+ **Solution Success**
  - Provide business value / return on investment in terms of what will be improved, what problems will be reduced or what benefit will this be to the institution.
  - Address quantitative and tangible business benefits.
+ **Solution Deliverables**
  - Outline what will be accomplished.
  - Define boundaries (project scope).
+ **Resource Requirements**
  - People – Project staff, IT staff, participants and those impacted
  - Time – What is the time frame for this project? How long will it take?
  - Dollars – Direct and indirect costs – e.g., hardware, labor, etc.
  - Other – Software, training, expertise, consultant, contractor, procured items, travel, etc.
+ **Risks / Dependencies**
  - Identify internal risk factors – e.g., resource changes, assumption failures, sponsor availability, new, relatively unknown team members, misalignment of stakeholder's goals or expectations, lack of support staff, etc.
  - Identify external risk factors – e.g., change in technology direction, change in strategic direction, vendor goes out of business, etc.
  - Does this project conflict or compete for resources with any other project?
  - Does this project depend upon the success of any other project?
  - Does any other project depend upon this project?
+ **Methodology / Approach**
  - What is your strategy for completion?
  - How will the project team be organized?
  - What development and collaboration tools will be used? E.g., project website, project mailing list, problem management system, etc.
  - How will changes be controlled?
  - How will the project plan be updated?

Authorization

The Manager and Sponsor have reviewed this request. They concur that this document represents the details of the request and the justification for its submission.

Manager Signature:		Phone #(s):	_ _ _-_ _ _ - _ _ _ _
Project Sponsor Signature:		Phone #(s):	_ _ _-_ _ _ - _ _ _ _

Information Technology Project Scorecard

Project Name:	Request Number (Assigned by IT):	Review Date: _ _ / _ _ / _ _	Portfolio Rank:	
Requestor Name(s):		Phone #(s): _ _ _-_ _ _ - _ _ _ _		
College / District:		Department:		
Project Sponsor:				

PROJECT DESCRIPTION

+ Provide a brief overview of the project, the benefit / value, deliverables, etc.

SCORECARD MEASURES

Alignment :	❒ Institution's Vision	❒ College Vision/Goals	❒ College IT Goals	❒ District IT Goals
Posture:	❒ Very Defensive	❒ Defensive	❒ Neutral	❒ Bold / ❒ Very Bold
Planning:	❒ Strategic	❒ Tactical	❒ Operational	
Implementation Timeframe:	❒ Short-term < 12 months		❒ Long-term > 12 months	
Funds:	❒ Existing budget		❒ New funds	
Investment Costs: - One Time	❒ < $25,000	❒ < $50,000	❒ < $100,000	❒ > $100,001
- Ongoing	❒ < $25,000	❒ < $50,000	❒ < $100,000	❒ > $100,001
Capability Gap:	❒ Large gulf between current tools, skills and staff	❒ Will take 3 – 6 months to build adequate inventory of tools, skills & staff	❒ Can achieve necessary tools, skills and staff needed within 3 months	❒ Necessary tools, skills and staff are available
FTE Requirements:	Implementation		Ongoing	

Risk Factor:	Low (0)	Medium (1)	High (2-3)	Very High (3-4)
Complexity	❒ The project is well defined	❒ The project has identified problems	❒ Multiple approaches to the project exist	❒ The project is only vaguely defined
Political Impact	❒ Department	❒ Multiple Departments	❒ College	❒ Institution
Deployment Impact	❒ Department	❒ Multiple Departments	❒ College	❒ Institution
Technology/ Process	❒ Expert	❒ Familiar	❒ New to College / District	❒ Cutting Edge
Total Risk Score		**0 – 6 Manageable**	**7 – 12 Moderate**	**13 – 16 High**

IT Comments:

Legend:

Alignment	Measure maps the projects against the stated strategic objectives for college and district IT as well as the overall vision and goals of the Institution and College.
Posture	Measure identifies projects that are: - Defensive projects reduce costs or inefficiencies – e.g., spam control projects, security, IdM, etc. - Bold projects either create capacity or provide strategic advantage to KCCD

Planning	Measure identifies projects by their impact (strategic, tactical and operational).
Implementation Timeframe	Measure allows IT to balance projects between short-term and long-term.
Risk	Measure identifies and scores points of failure.
Funds	Measure identifies where funds for the project are coming from.
Investment Costs	Measure assesses direct and indirect project costs.
Capability Gap	Measure ascertains imbalance of required resources to deliver project.
FTE Requirements	Measure clarifies human effort to implement and maintain project.

Information Technology Survey Instrument

You have been randomly selected to participate in the Information Technology 2007 Customer Satisfaction survey. This survey is one part of the Information Technology Assessment being conducted by SunGard Higher Education on behalf of KCCD.

The results and findings of this survey will be incorporated into the IT Assessment Report and be used to measure and improve the quality and effectiveness of both College and District Office IT services over time.

The survey contains 32 questions and will take approximately 15 minutes to complete. The deadline for completing this survey is March 16, 2007. This survey is confidential, your name will never be associated with your responses and I would appreciate candid and honest feedback. Results will be released only in statistical and summary form.

To complete the survey, click on this link http://surveymonkey.com.

Thank you in advance for your time and consideration.

David Palinsky
Director, Information Technology

Instructions: The questionnaire uses a combination of methods to solicit your opinion. Many of the questions ask for your level of satisfaction for a given service based on a 5 or 9-point scale. The scale represents a spectrum where "0 or 1" indicates a low satisfaction with the service and a "5 or 9" indicates a high satisfaction. A few questions are open ended for you to make comments. Yet others will ask you to rank in order of preference your needs.

Please answer all questions to the best of your ability. Use your mouse to click on the circle that best represents your response. If you do not have an opinion, please skip the question.

Part I. College and District Information Technology Services

A. Using your impressions of College and District IT departments please rate the following.

	Low									High
Responsiveness (timeliness & completeness)	⓪	①	②	③	④	⑤	⑥	⑦	⑧	⑨
Customer Service	⓪	①	②	③	④	⑤	⑥	⑦	⑧	⑨
Clarity of communication	⓪	①	②	③	④	⑤	⑥	⑦	⑧	⑨
Alignment of IT services with organization's goals and initiatives	⓪	①	②	③	④	⑤	⑥	⑦	⑧	⑨
Security	⓪	①	②	③	④	⑤	⑥	⑦	⑧	⑨
Overall satisfaction with IT services	⓪	①	②	③	④	⑤	⑥	⑦	⑧	⑨

B. How satisfied are you with the following IT service offerings?

	Low	High

PC and Printer Support	①	②	③	④	⑤
Outlook eMail and Related Services	①	②	③	④	⑤
Telephone	①	②	③	④	⑤
Internet Access from Campus and District Office Facilities	①	②	③	④	⑤
Online Course Management Systems	①	②	③	④	⑤
Interactive TV	①	②	③	④	⑤
Library Technology	①	②	③	④	⑤
Banner	①	②	③	④	⑤
Banner Web	①	②	③	④	⑤
College Website Services	①	②	③	④	⑤
District Website	①	②	③	④	⑤
Video Conferencing for Conducting Meetings	①	②	③	④	⑤
Training	①	②	③	④	⑤
Hardware / Software Purchasing	①	②	③	④	⑤
IT Consulting for Instructional and Administrative Initiatives	①	②	③	④	⑤

C. Please describe what would increase your satisfaction with the IT service offerings?

D. Please select, in order of importance to you, the top three (3) items from the following list you believe that college or district IT should offer. **Rating:** 1 = first choice, 2 = second choice, 3 = third choice

- ○ Off-campus access to college and district technology resources
- ○ Provide network access for non-college / district issued laptops
- ○ Online ordering / purchasing of college products and services (e.g. books, tickets, etc.)
- ○ Blogging support
- ○ Podcast support
- ○ Expanded wireless access
- ○ Expanded document imaging and retrieval
- ○ Portal technology (e.g. Web-based personal gateway into college services and information)
- ○ Student email
- ○ Student support help desk
- ○ Student information kiosks
- ○ Other (Please explain) _____

E. Which of the following concern you regarding information technology? Select all that apply.

- ○ Inadequate access to printing
- ○ The age of my computer hardware / software
- ○ Frequent network outages during normal working hours
- ○ My technical skill level in troubleshooting my computer

- ○ Computer viruses, worms or Trojan horses
- ○ Spam
- ○ Inadequate technical assistance and help available to me
- ○ Other (Please explain) _____

Part II. College and District Instructional Technology Services

F. Do you provide instruction to students? (APPLY SKIP LOGIC IN SURVEY MONKEY)

- ○ Yes (continue to question G)
- ○ No (continue to question L)

G. How satisfied are you with the following aspects of audio-visual services?

	Low				High
Selection of A/V equipment	①	②	③	④	⑤
Equipment reliability	①	②	③	④	⑤
Response time for equipment-related help requests	①	②	③	④	⑤

H. How satisfied are you with audio-visual services overall?

Low				High
①	②	③	④	⑤

I. How satisfied are you with the following aspects of your college's Computer Labs?

	Low				High
Software availability	①	②	③	④	⑤
Computer work station availability	①	②	③	④	⑤
Printing	①	②	③	④	⑤

J. How satisfied are you with your college's Computer Labs overall?

Low				High
①	②	③	④	⑤

K. What additional software or services would you like to see in your college's Computer Labs? Please explain.

Part III. College and District Help Desk Services

L. Which Help Desk do you primarily call for assistance? Select one profile.

- ○ Bakersfield College IS Help Desk (661.395.4274)
- ○ Bakersfield College Distance Learning (661.395.4694)
- ○ Bakersfield College Media Services (661.395.4516)
- ○ Cerro Coso College IT Help Desk (760.384.6166)
- ○ Cerro Coso College Online (CC Online) Help Desk (760.934.2796 or 888.537.6932)
- ○ Porterville College Tech Services
- ○ Learning Services Center Help Desk (661.336.5197)
- ○ Other (Please explain) _____

M. Please rate your satisfaction with the following Help Desk areas.

	Low				High
Ability to get through to a person	①	②	③	④	⑤
Timeliness of response	①	②	③	④	⑤
Professionalism	①	②	③	④	⑤
Ability to solve your problem	①	②	③	④	⑤
Customer oriented	①	②	③	④	⑤

N. Thinking about all of your interactions with the Help Desk staff mentioned above, which rating on the scale below best describes the frequency with which you were treated?

	Never				Always
Courteously	①	②	③	④	⑤
Patiently	①	②	③	④	⑤
In a friendly manner	①	②	③	④	⑤

O. How often do you use the Help Desk? Select one profile.

- ○ Less than once a month
- ○ Once a month
- ○ More than once a month
- ○ Once a week
- ○ More than once a week
- ○ Daily
- ○ Never

P. Think about the problems for which you call the help desk. On average, how long does it take to resolve the problem from the time you first call the help desk? Select one profile.

- ○ Problem resolved immediately
- ○ Same day
- ○ Two working days
- ○ More than two working days

Q. Please select, in order of importance to you, the top three (3) items from the following list that would appreciably increase your satisfaction with the Help Desk problem resolution.
Rating: 1 = first choice, 2 = second choice, 3 = third choice)

- ○ Faster response time for initial contact
- ○ Faster resolution of my problems (the initial call is resolved and closed on contact)
- ○ Better communication about the status of my request
- ○ More knowledgeable staff
- ○ Having problems and/or solutions explained to me in less technical terms
- ○ Better web-based help information
- ○ Other (Please explain) _____

Part IV. College and District Network Services

A network ties things together. Computer networks connect all types of computers and non-computer devices — e.g. PC's, printers, servers, video conference equipment, etc. Local Area Networks (LANs) connect computer equipment within a building or campus. Wide Area Networks (WANS) connect computer equipment between colleges and sites. It is through these networks that students, faculty and staff access the Internet, email, Banner and other services.

R. How satisfied are you with the performance of the network?

	Low									High
Reliability (works when you need it to)	⓪	①	②	③	④	⑤	⑥	⑦	⑧	⑨
Performance (response time – slow to fast)	⓪	①	②	③	④	⑤	⑥	⑦	⑧	⑨

S. Please list any locations where access needs to be added or improved. Include specific information such as college, building name, room number, etc.

Part V. College and District Training Services

T. Please select, in order of importance to you, the top three training methods for learning additional computer-related knowledge and skills. Rating: 1 = first choice, 2 = second choice, 3 = third choice

- ○ Hands-on classes
- ○ One-on-one tutoring
- ○ Lecture / demonstration
- ○ Self-paced computer-based training
- ○ Online courses
- ○ Other (Please explain) _____

U. Please select, in order of importance to you, the top three sources for learning additional computer-related knowledge and skills. Rating: 1 = first choice, 2 = second choice, 3 = third choice

- ○ Your peers or colleagues
- ○ Your local department expert
- ○ Your college IT / IS department

- ○ District IT support
- ○ District website
- ○ Information outside of KCCD (Google, Apple, Microsoft, Red Hat, etc.)
- ○ Other (Please explain) _____

Part VI. Portable Technology

V. Which of the following portable technologies do you use? Select all that apply.

- ○ Palm OS device
- ○ Pocket PC device
- ○ Blackberry
- ○ Treo
- ○ Other cell phone with data capabilities
- ○ iPod or other MP3 device
- ○ Other (Please explain) _____

W. What software or services would you like to be able to access via portable devices? Please explain.

Part VII. User ID, Passwords and Privacy

X. How many different User ID's do you use and remember as part of your work? (e.g. Banner, *e*Mail, Hershey system, network login, etc.) Select one profile.

- ○ 1– 2
- ○ 3 – 4
- ○ 5 – 6
- ○ 7 – 8
- ○ More than 9

Y. Do you use a common password for different login applications? (e.g. Banner, *e*Mail, Hershey system, network login, etc.) Select one profile.

- ○ Yes
- ○ No

Z. On average, how often do you change your login passwords? Select one profile.

- ○ Once a month or more
- ○ Once every two to three months
- ○ Several times a year
- ○ Once a year or less
- ○ Never

AA. Have you shared your password with others? Select one profile.

- ○ Yes
- ○ No

BB. Do you write down your passwords in order to remember them? Select one profile.

- ○ Yes
- ○ No

CC. Where do you store confidential / sensitive information? (e.g. social security numbers, citizen visa code, citizenship, home phone numbers, health records, etc.) Select all that apply.

- ○ Applications (e.g. Banner)
- ○ Databases / Spreadsheets
- ○ On your computer at work (e.g. "My Documents" folder)
- ○ On your computer at home (e.g. "My documents" folder)
- ○ Network shared drive (e.g. home directory)
- ○ Downloaded to floppy disk / CD
- ○ USB flash drives / memory sticks / thumb drives
- ○ Portable devices (e.g. PDA, iPod, MP3, Blackberry, Treo, Cell phone, etc.)
- ○ Paper, file cabinets, etc.
- ○ Laptop
- ○ Other (Please explain) _____

Part VIII. Tell Us About Yourself

DD. What is your primary work location? Select one profile.

- ○ Bakersfield College
- ○ Cerro Coso Community College (IWV)
- ○ Delano College Center
- ○ Eastern Sierra College Center (Bishop/Mammoth)
- ○ Kern River Valley Center
- ○ Learning Services Center (District Office)
- ○ Porterville College
- ○ South Kern Center (Edwards AFB)
- ○ Weill Institute

EE. What is your primary group? Select one profile.

- ○ Full-time Faculty
- ○ Adjunct Faculty
- ○ Classified or Confidential Staff
- ○ Management

FF. How would you rate your computer skills and knowledge. Select one profile.

- ○ Beginner (novice)
- ○ Intermediate
- ○ Advanced (power user)

Thank you for taking the time to complete the survey. Your feedback is appreciated and will help to improve the quality of support and shared services college and district IT offers you and students.

IT Security for Higher Education: A Legal Perspective

Prepared for the
EDUCAUSE/Internet2 Computer and Network Security Task Force

Funded by a grant from the National Science Foundation

Kenneth D. Salomon
Peter C. Cassat
Briana E. Thibeau

Dow, Lohnes & Albertson, PLLC

March 20, 2003

I. Introduction

Federal and state laws relating to privacy and information technology security have become increasingly complex in nature, and the practical effect of these laws on colleges and universities is just beginning to unfold. Recent incidents relating to information security have brought these issues to the forefront and have highlighted the liabilities that can arise when security measures are compromised. In one story that made national headlines in 2002, Yale University discovered that a member of Princeton University's admissions staff used the birth dates and Social Security numbers of Princeton applicants who had also applied to Yale to gain access to a Yale web site set up for prospective students.[1] The Princeton administrator stated that he was testing network security procedures and was not trying to gain an advantage in recruiting the students. Yale filed a complaint with the Federal Bureau of Investigation (FBI), and Princeton launched an independent investigation. In another incident, the University of Texas at Austin acknowledged that the names, e-mail addresses and Social Security numbers of some 59,000 students, alumni and employees were obtained through a brute force attack on a University database. According to the University, the incident could have been prevented if additional security measures were taken.[2]

The University of Kansas also found itself in the media spotlight when it discovered that the computers in its international students office had been hacked on at least five occasions and personal information on more than 1,400 foreign students had been stolen.[3] The information included Social Security numbers, dates of birth, passport numbers, phone numbers and countries of birth. The University had collected the information for the Student and Exchange Visitor Information System (SEVIS), a database that is being developed by the Immigration and Naturalization Service (INS) to monitor and track foreign students. The INS is under a mandate to create the database pursuant to the USA PATRIOT Act, and colleges and universities that enroll international students must participate in the system or forfeit their right to enroll those students. University officials report that the temporary "hole" in their security system has been closed. However, this incident has prompted the FBI to investigate possible connections to terrorism, and has prompted affected students to worry about identity theft and the possibility of facing additional questions at U.S. ports of entry when entering or leaving the country. Recognizing the risk posed to its students, the University is trying to contact every student affected by the security compromise.

Each incident illustrates the unforeseen risks that can be associated with information technology assets. For educational institutions, the importance of such assets continues to grow as the 21st Century institution is both increasingly computerized and increasingly networked. Everything from transcripts to

[1] *See* Karen W. Arenson, *Princeton Pries Into Web Site for Yale Applicants*, the New York Times, July 26, 2002, *available at* http://www.nytimes.com/2002/07/26/education/26IVY.html; Diane Scarponi, *Yale Accuses Princeton of Hacking*, the Washington Post, July 25, 2002, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A2411-2002Jul25; Michael Barbaro, *Princeton Apologizes for Web Breach*, the Washington Post, July 30, 2002, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A18705-2002Jul29.

[2] *See* Ralph K. M. Haurwitz, *Hackers steal vital data about UT students, staff*, Austin American-Statesman, March 6, 2003, *available at* www.austin360.com/aas/metro/030603/0306uthack.html.

[3] *See* Michael Arnone, *Hacker Steals Personal Data on Foreign Students at U. of Kansas*, the Chronicle of Higher Education, Jan. 24, 2003, *available at* http://chronicle.com/free/2003/01/2003012403n.htm; Julie Mah, *Foreign-student database at KU hacked*, The Wichita Eagle, Jan. 24, 2003, *available at* www.kansas.com/mld/kansas/5019148.htm.

course syllabi to student financial aid records are stored in databases on servers that without the use of appropriate safeguards to protect against unauthorized use can be accessed from both within and outside the institution. Office hours are some times replaced by e-mail, and virtually every institution claims to offer at least some form of online learning. The increasing digitization and dissemination of content for online use and the sprawling growth and interconnectivity of campus networks have allowed professors, students, and other members of the educational community to exchange ideas and information in ways only imagined a few years ago. But this proliferation of access and interconnectivity brings with it increasing risks. Unlike private corporate networks, which, by their nature, are designed to be "walled gardens" of information, campus networks – due to the need to facilitate collaboration and provide access to information – generally are designed to be more open, and therefore more vulnerable to misuse.

Not only can an educational institution's computer systems be the target of unauthorized access from outside the institution, but individuals with access to those powerful systems can use them to launch unauthorized attacks on other computer systems and networks. Public access terminals located in college and university libraries, now a nearly universal phenomenon, are particularly vulnerable, both as a means to obtain access to institutional networks and to harass others anonymously. As a result of these trends, college and university administrators, IT professionals, and legal counsel should become familiar with the federal and state computer theft and privacy laws that may give rise to criminal prosecution or civil claims *against the institution* as well as its personnel and students.

Federal laws such as the Electronic Communications Privacy Act (ECPA),[4] the Computer Fraud and Abuse Act (CFAA),[5] and the Family Educational Rights and Privacy Act (FERPA),[6] as well as state computer crime laws and common law or statutory rights of privacy may be implicated in situations where improper access is gained to a supposedly secure computer system. In many ways, however, these laws have failed to keep pace with technological innovations. The result has been an atmosphere of uncertainty, placing further strain on already scarce institutional resources and leading in some cases to inaction as a result of concerns over legal exposure. The absence of a single set of standards further complicates the issue, leaving administrators and IT directors struggling to decide how best to protect their institutions while at the same time not interfering with their educational mission.

This white paper explores the current legal landscape and the factors contributing to this atmosphere of uncertainty. The following sections present an overview of existing federal and state privacy and security related laws affecting institutions of higher education. The paper then discusses several practical implications of such laws for institutions of higher education and suggests areas for further exploration.

II. The Current Legal Landscape

The legal atmosphere in which institutions of higher education operate reflects an overlapping system of state and federal regulation. Various institutional activities may be governed by a combination of federal and state regulations, as well as by accrediting organization standards. In addition to these promulgated

[4] 18 U.S.C. § 2701 *et seq.*

[5] 18 U.S.C. § 1030.

[6] 20 U.S.C. § 1232g; 34 C.F.R. Part 99.

standards, in many cases institutions remain subject to suits based on common law negligence theories. In fact, as distance education and information technology have enabled colleges and universities to spread their reaches even farther, institutions may be subject to suit in multiple states and even foreign jurisdictions.

The likelihood that multiple federal, state and foreign laws could apply is even greater when it comes to laws that relate to the use or misuse of information technology. While there is an increased likelihood that an institution could be faced with a suit brought in another jurisdiction, it also may provide the institution with the ability to bring claims locally against defendants that hack into its systems from other states. In fact, a federal district court recently ruled that the act by an out-of-state defendant of accessing a plaintiff's servers without authorization formed a sufficient basis for the exercise of personal jurisdiction over the defendant.[7]

Federal Law

There is no single, comprehensive set of federal laws mandating either specific privacy practices or information security measures of colleges and universities.[8] Instead, depending on the particular institution and the nature of the activity at issue, institutions may be required to comply with any number of potentially applicable federal laws and regulations. The list of relevant acronyms is daunting: FERPA, HIPAA, ECPA, and CFAA are just a few of the federal laws that include obligations applicable to educational institutions. Both the hastily-enacted USA PATRIOT Act and the recent TEACH Act also have electronic privacy and security implications. Navigating this maze of federal privacy statutes is made even more difficult due to the fact that many of the laws overlap or apply differently to different institutional activities.[9]

1. Family Education Rights and Privacy Act (FERPA)

FERPA is the keystone federal privacy law for educational institutions. FERPA generally imposes a cloak of confidentiality around student educational records, prohibiting institutions from disclosing

[7] *See D.C. Micro Development Inc. v. Lange,* Civil Action No. 3:02-CV-225(H) (W.D. Ky. Jan. 28, 2003).

[8] While the Federal Trade Commission (FTC) has aggressively pursued misleading customer data and privacy practices under its broad deceptive practices jurisdiction under Section 5 of the FTC Act, the FTC's Section 5 jurisdiction does not extend to the activities of non-profit organizations. As a result, while this white paper addresses the FTC's rules implementing the Gramm-Leach-Bliley Act, it does not address the FTC's deceptive practices enforcement initiatives. Interestingly, however, in 2002 the FTC settled two high-profile investigations into the cyber security and privacy practices of Microsoft and Eli Lilly. The consent orders in these cases may provide an indication of the security standards to which institutions can expect to be held. According to FTC Chairman, Timothy J. Muris, "When we issued those orders, we hoped and expected the business community would pay attention."

[9] It also is noteworthy that the current Congress, like Congresses past, is considering additional privacy-related laws that, if passed, will only add to the complexity in this area. Some, such as the Online Privacy Protection Act of 2003 (H.R. 69), are quite broad, while others address more specific privacy concerns. *See, e.g.*, H.R. 70 (proposing restrictions on the use of Social Security numbers (SSNs) by Internet Service Providers (ISPs)); H.R. 71 (proposing restrictions on the use of wireless call location information); H.R. 637 (proposing to limit the use of SSNs and impose criminal penalties for misuse); S. 153 (proposing criminal penalties for “aggravated identity theft”).

"personally identifiable education information," such as grades or financial aid information, without the student's written permission.[10] FERPA also grants to students the right to request and review their educational records and to make corrections to those records. The law applies with equal force to electronic records as it does to those stored in file drawers. While violations of FERPA do not give rise to private rights of action,[11] the U.S. Secretary of Education has established the Family Policy Compliance Office which has the power to investigate and adjudicate FERPA violations and to terminate federal funding to any school that fails to substantially comply with the law.[12]

One of the most significant, current risks under FERPA is that the number of electronic records created by or relating to students that are stored in college and university databases on servers has increased exponentially, increasing in turn the number of potential "educational records" that must be protected. Faculty want the convenience of submitting grades electronically; students want to retrieve grades and register for courses via a web-enabled student information system; financial aid offices want to electronically process applications for loans and grants. In addition, course materials are increasingly transmitted and stored electronically. Deciding what constitutes an educational record subject to FERPA, therefore, is increasingly complex in the current technological environment. This ambiguity, combined with the proliferation of electronic records and the need to protect against unauthorized disclosure, threatens to significantly increase the costs and risks of exposure for security breaches.

There also is an absence of precedent regarding whether FERPA should be interpreted to apply to disclosures of student records occasioned by unauthorized access to an institution's network or databases. This issue was touched upon in a 2001 court decision which declined to impose liability based upon the "defendants' alleged 'policy of inaction by failing to implement safeguards to prevent unauthorized disclosure of educational records . . . .'" [13] According to the court, ". . . the defendants [we]re entitled to immunity inasmuch as no precedent ha[d] ever held similar defendants liable for such conduct or inaction."[14] Thus, while an argument can be made that FERPA only should apply to

[10] 20 U.S.C. § 1232g(b).

[11] *See Gonzaga University v. Doe*, 122 S. Ct. 2268 (June 20, 2002) (holding that an individual does not have the right to sue a school on the basis of an alleged violation of FERPA).

[12] In *Gonzaga University v. Doe,* the Supreme Court clarified that FERPA's nondisclosure provisions have an "aggregate" focus and are not concerned with whether the needs of any particular person have been satisfied. *See* 122 S. Ct. 2268, 2278 (June 20, 2002). Therefore, a school can avoid losing its funding by "substantially complying" (*i.e.*, making it a custom to comply) with FERPA, and a single FERPA violation would not be grounds for denying federal funding. *See id.; see also Appelberg v. DeVilbiss*, No. Civ. A00-0202-BH-C (S.D. Ala. Jan. 30, 2001) (stating that an isolated incident is not enough to amount to a custom and concluding that there was no evidentiary basis for plaintiffs' contention that a custom or practice existed of releasing information from student records at the defendant school without the student's consent in violation of FERPA).

[13] *See Appelberg v. DeVilbiss*, No. Civ. A00-0202-BH-C (S.D. Ala. Jan. 30, 2001) (involving unauthorized access by a school secretary's daughter to the physical – *i.e.* non-electronic – records of the plaintiff's son).

[14] *See id.* at *4, n.5 (S.D. Ala. Jan. 30, 2001). The court stated that the plaintiffs presented "no legal authority, and none exists, which earlier defined, or even now defines, a 'release' under FERPA to mean the mere unauthorized access of a student's records by a fellow student without the knowledge of the school superintendent, principal or any other staff member or faculty member." *See id.* at *4. The court went on to say that "[n]o other case has ever, in factual terms, staked out a bright line establishing that the mere

affirmative disclosures of educational records, and while the courts have not yet dealt with this issue head-on, it is possible that FERPA could be read to impose liability where the steps taken by the institution fail to adequately protect against unauthorized access by third parties.

An institution may be particularly vulnerable to a FERPA violation if it can be shown that it was negligent in instituting procedures to protect against disclosure of electronic records. At the same time, however, continuous changes in the technology environment, combined with the often decentralized nature of institutions' networks, make it difficult to ensure that appropriate practices are in place. For example, the movement away from mainframe systems and toward distributed databases and servers has made it more difficult to have consistent and clear data access policies and procedures. It also is uncertain under what circumstances it is necessary to use technological measures to maintain the confidentiality of educational records. While institutions appear to be moving toward securing e-mail and electronically stored records through encryption, there is no consensus as to when it is necessary to protect data or the methods that should be employed.

2. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA was enacted to protect the rights of patients and participants in certain health plans. In 2000, the federal Department of Health and Human Services adopted copious regulations granting consumers the right to receive written notice of the information practices of entities subject to HIPAA. Colleges and universities that are affiliated with health care providers are considered covered entities and by April 14, 2003, those institutions must provide written notice of their affiliated health care provider's electronic information practices. Most employer-sponsored health plans also are considered to be "entities" subject HIPAA. As a result, various compliance obligations are imposed on colleges and universities that sponsor and administer such plans. The deadline for health plan compliance also is April 14, 2003 (except that health plans with annual receipts of $5 million or less have until April 14, 2004 to comply).[15]

HIPAA generally requires covered entities to (i) adopt written privacy procedures that describe, among other things, who has access to protected information, how such information will be used, and when the information may be disclosed; (ii) require their business associates to protect the privacy of health information; (iii) train their employees in their privacy policies and procedures; (iv) take steps to protect against unauthorized disclosure of personal health records; and (v) designate an individual to be responsible for ensuring the procedures are followed.[16] Educational institutions may be obligated to comply with HIPAA in connection with a broad range of activities. College and university attorneys and their clients have been forced to dedicate significant resources in attempting to comply with the complex language of HIPAA and in applying it to the distributed environment of a typical campus, particularly as to how its enforcement coincides with other institutional obligations.

3. Electronic Communications Privacy Act (ECPA)

unauthorized access to student records, whether or not resulting from some failure on the part of the defendants to provide a security system within some previously defined parameters which prevents such access, would constitute a violation of FERPA." *See id*.

[15] *See* Gerald W. Woods, *HIPAA Privacy Rule Primer for the College or University Administrator*, prepared for the American Council on Education, December 2002, *available at* http://www.acenet.edu/washington/policyanalysis/HIPAA.2.pdf.

[16] Pub. L. No. 104-191 (1996).

Unlike FERPA and HIPAA, which are specific to certain types of entities, the ECPA broadly prohibits the unauthorized use or interception by any person of the contents of any wire, oral or electronic communication.[17] Protection of the "contents" of such communications, however, extends only to information concerning the "substance, purport, or meaning" of the communications.[18] In other words, the ECPA likely would not protect from disclosure to third parties information such as the existence of the communication itself or the identity of the parties involved.[19] As a result, the monitoring by institutions of students' network use or of network usage patterns, generally, would not be prohibited by the ECPA.

The ECPA also prohibits unauthorized access to or disclosure of electronically stored wire and electronic communications.[20] More specifically, the ECPA imposes liability on any person who intentionally accesses without authorization a facility through which an electronic communication service is provided, or exceeds an authorization to access that facility, if that person thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage.[21] While the ECPA restricts providers of *public* electronic communication services (specifically, providers of public access terminals and other public services) from divulging the contents of stored electronic communications, it does not appear to place the same restrictions on providers of *private* electronic communication services. Institutional e-mail systems and networks most likely would constitute private electronic communication services that enjoy the relaxed restrictions of the latter category, thus allowing institutions to monitor and access student e-mail accounts. Nevertheless, college and university computer use policies often strike a balance between student privacy rights and network security concerns by authorizing inspection by the institution of student e-mails or other communications *only* when there is reasonable basis to suspect improper use of a computer or network. In addition, educational institutions' networks often serve multiple communities of users (for example, students, faculty, employees, alumni, and the general public) and the correct application of the ECPA may depend on the nature of the relationship between the institution and the user. Thus, an institution's right to monitor electronic communications, or its obligation or ability to comply with a law enforcement request, may vary depending on whether the user in question is a student, an employee, or a member of the public.

The ECPA also contains specific exceptions allowing disclosures to law enforcement agencies under certain circumstances. Certain provisions of the USA PATRIOT Act, discussed below, substantially broaden the authority of law enforcement officials to obtain information under the ECPA. Under Section 210 of the USA PATRIOT Act, the scope of information that the government can obtain by subpoena has been expanded to include electronic communications, and law enforcement officials now can obtain information such as means and sources of payment, records of session times and duration, length of service and type(s) of service utilized, and user number or identity, including any temporarily assigned network addresses. Also, Section 212 of the USA PATRIOT Act amended the ECPA to permit communications service providers to release both content and non-content

[17] *See* 18 U.S.C. § 2511.

[18] *See id.* at § 2510(8).

[19] *See id.*

[20] *See* 18 U.S.C. §§ 2510 – 2521, 2701 *et seq.*

[21] *Id.*

information about a wire or electronic communication to a law enforcement agency if the provider reasonably believes that the information must be provided without delay to avoid injury to any person. This provision of the ECPA was further amended, however, by the Cyber Security Enhancement Act of 2002, and it now permits communications service providers to divulge to a Federal, State, or local governmental entity the contents of a communication if the provider believes in "good faith" that "an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[22] In other words, in responding to an emergency situation, institutions are now allowed to release relevant information, including not just the existence but also the *content* of wire and electronic communications, to law enforcement officials if the institution in good faith determines that release of the information is necessary to avoid injury.
These changes have significance for institutions that essentially function in the role of Internet service provider, and the result has been to make it more complex and burdensome to respond appropriately to requests for information from law enforcement agencies. Service providers most likely can expect that, because the government now has easier access to warrants and other authority to intercept communications of all kinds, new demands will be placed on their systems and their information processing and retrieval capability.

The ECPA's reach is long: a University of Delaware student who in the summer of 2002 obtained unauthorized access to the University's computer system to give herself passing grades in three spring semester courses potentially violated the ECPA. In that case, the student allegedly called the University's human resources office and impersonated her instructors to obtain new passwords, which in turn enabled her to log into the system as though she were her own professors. [23] No federal charges were brought under the ECPA, but the student pleaded guilty to misdemeanor charges on counts of criminal impersonation, unauthorized access to a computer system, and misuse of computer system information. She was sentenced to three years probation and ordered to pay $12,000 in restitution. Three counts of felony identity theft were dropped. The University, meanwhile, began reviewing its computer security measures and charged the student with three counts of academic dishonesty and three counts of violating the school's "responsible computing" code.

4. Computer Fraud and Abuse Act (CFAA)

The CFAA criminalizes unauthorized access to a "protected computer" with the intent to obtain information, defraud, obtain anything of value or cause damage to the computer.[24] A "protected computer" is defined as a computer that is used in interstate or foreign commerce or communication or by or for a financial institution or the government of the United States.[25] In light of the "interstate or foreign commerce" criterion, the act of "hacking" into a secure web site from an out-of-state computer, which may have occurred when the Princeton admissions officer accessed Yale's "secure" web site, could be considered a CFAA violation (although both schools took pains to say that they were not

[22] *See* Homeland Security Act of 2002, H.R. 5005, 107th Congr. § 225 (2002). The Cyber Security Enhancement Act was approved by the House of Representatives as a stand-alone bill in July of 2002 but was incorporated into the Homeland Security Act (at § 225) just before the Homeland Security Act's passage.

[23] *See* Brock Read, *U. of Delaware Student Is Charged With Breaking Into Computer System and Changing Her Grades*, the Chronicle of Higher Education, July 17, 2002.

[24] 18 U.S.C. § 1030(a).

[25] *Id.* at § 1030(e)(2).

seeking any civil or criminal prosecutions). The fact that both ECPA and CFAA are *criminal* statutes considerably raises the ante.

5. USA PATRIOT Act

The USA PATRIOT Act,[26] passed six weeks after September 11, 2001, grants law enforcement increased access to electronic communications and, among other things, amends FERPA, ECPA and the Foreign Intelligence Surveillance Act of 1978 (FISA),[27] in each case making it easier for law enforcement personnel to gain access to otherwise confidential information. Perhaps most significant in the context of higher education is an amendment that potentially prohibits institutions from revealing the very existence of law enforcement investigations. Under Section 215 of the USA PATRIOT Act, which amends Sections 501 through 503 of FISA, the FBI can seize with a court order certain business records pursuant to an investigation of "international terrorism or other clandestine intelligence activities," and record-keepers are prohibited from disclosing the FBI's action to anyone "other than those persons necessary to produce the tangible [records] . . . ." The same goes for investigations into data banks storing information, such as information about who may have accessed certain library resources – thus, librarians may not even reveal that an inquiry has been made.

The USA PATRIOT Act also amends the portion of the National Education Statistics Act of 1994 (NESA)[28] that specified that data collected by the National Center for Education Statistics (NCES) may only be used for statistical purposes. The amended NESA now permits the attorney general to petition a judge for an ex parte order requiring the Secretary of the Department of Education to provide data from the NCES that are identified as relevant to an authorized investigation or prosecution concerning national or international terrorism. In other words, data collected by NCES may now be used with a judge's order for matters relevant to an offense concerning terrorism. Nonetheless, the attorney general is obligated to protect the confidentiality of any NCES data it obtains.[29]

Another significant impact of the USA PATRIOT Act is its mandate to the INS requiring the INS to develop and implement the Student and Exchange Visitor Information System or "SEVIS." SEVIS is an Internet-based system that will allow schools to transmit information on foreign students to the INS for purposes of tracking and monitoring. The system will compile students' personally identifiable information including admission at port of entry, academic information, and disciplinary information. FERPA's restrictions have been waived to allow schools to disclose this information, which must be maintained and updated for the duration of a student's stay in the United States.

---

[26] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, H.R. 3162, Title II Section 215 (Oct. 26, 2001).

[27] Pub. L. No. 95- 511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-1811, 1821-1829, 1841-1846, 1861-62).

[28] 20 U.S.C. § 9007, *et seq*.

[29] Following the enactment of the USA PATRIOT Act, the 107th Congress enacted the E-Government Act of 2002, H.R. 2458, 107th Congr. (2002). Sections 511 through 513 of the E-Government Act require that all individually identifiable information supplied by individuals or institutions to a federal agency for statistical purposes under the pledge of confidentiality must be kept confidential and may only be used for statistical purposes. *See* H.R. 2458, 107th Congr. §§ 511-513 (2002).

As noted in the Introduction, above, recent events at the University of Kansas illustrate that efforts to require the creation of records for national security purposes may have unintended consequences. A hacker gained access to the computers in the University of Kansas (KU) international students office and obtained the SEVIS records for approximately 1,450 international students. Ironically, the hacker apparently exploited a security "hole" created while KU officials were updating the security features on the computer that maintained these records. The information that the hacker accessed from KU included personally identifiable information which could be used, along with other materials, to create fake passports, visas, and other documentation, as well as for other forms of identity theft. This incident illustrates that the creation of SEVIS may have the unintended consequence of compromising student privacy in the interest of public safety. Speaking in January of 2003 at a regional education conference, Frank J. Cilluffo, executive director of the President's Homeland Security Advisory Council, suggested as much when he stated that "we'd like to know if someone from a certain country changed their major from English literature to nuclear physics, or something along those lines."[30]

6. TEACH Act

The TEACH Act, passed by Congress on October 3, and signed into law by the president on November 2, 2002, relaxes certain copyright restrictions to make it easier for accredited nonprofit colleges and universities to use materials in technology-mediated educational settings.[31] But the new law carries with it obligations that have privacy and security implications: institutions that want to take advantage of the relaxed copyright restrictions must limit "to the extent technologically feasible" the transmission of such content to students who actually are enrolled in a particular course, and they must use appropriate technological means to prohibit the unauthorized retransmission of such information.[32] In other words, the TEACH Act may require institutions to implement technical copy protection measures and to authenticate the identity of users of electronic course content.[33]

The implementation of digital rights management tools necessary to control access will create additional cost, complexity, and yet another set of electronic records. Enforcement of the required protections also will raise new issues about appropriate disciplinary measures, not to mention the privacy concerns arising from monitoring student usage of course materials for unauthorized use or dissemination. Among other things, institutions may be confronted with claims under the Digital Millennium Copyright Act (DMCA) if their users attempt to defeat the technological restrictions employed by digital rights management tools. The DMCA makes it unlawful to circumvent technological measures that effectively control access to protected works.

7. Gramm – Leach – Bliley Act (GLBA)

[30] *See* Florence Olsen, *Demands of Homeland Security Will Pressure Colleges, Campus Computing Experts Warn*, the Chronicle of Higher Education, January 17, 2003, *available at* http://chronicle.com/free/2003/01/2003011702t.htm.

[31] Technology Education and Copyright Harmonization (TEACH) Act of 2001, H.R. 2215, *codified at* 17 U.S.C. §§ 101(1), 112(f).

[32] *See id.*

[33] For guidance on the technological considerations of the TEACH Act, see *Technological Requirements of the TEACH Act*, American Library Association, EDUCAUSE and the Association for Computing Machinery (2003), *available at* http://www.educause.edu/asp/doclib/abstract.asp?ID=CSD2725.

The GLBA[34], enacted in 1999, is applicable to financial institutions, including colleges and universities, and creates obligations to protect customer financial information. The GLBA includes requirements to take steps to ensure the security of personally identifying information of financial institution customers, such as names, addresses, account and credit information, and Social Security numbers.[35] The GLBA also sets forth extensive privacy rules which, among other things, require covered financial institutions to provide customers with privacy statements describing their information privacy practices. However, the Federal Trade Commission's (FTC's) regulations implementing the GLBA specifically provide that colleges and universities will be deemed to be in compliance with the privacy provisions of the GLBA if they are in compliance with FERPA. Nevertheless, educational institutions likely remain subject to the security provisions under the GLBA and the FTC's implementing rules. The GLBA customer financial information security rules, with which institutions must come into compliance by May 23, 2003, will require colleges and universities to develop comprehensive security programs, assess the need for employee training, and include obligations in their agreements with third parties that have access to financial records covered by the rules.[36]

State Law

Institutions naturally tend to worry most about federal requirements that constrain their actions or increase their costs. But in addition to the variety of federal laws that are applicable to information security and privacy, there are numerous state laws relating to security and privacy. Many states have enacted computer crime laws that expressly criminalize tampering with computers or accessing certain computerized records without authorization. For example, under Connecticut law, it is unlawful for any person to use a computer or computer network without authority and with the intent to remove, halt or disable computer programs or software; cause a computer to malfunction, alter or erase any computer data or software; cause physical injury to the property of another; or make an unauthorized copy of computer data or software.[37] Virginia and Rhode Island have enacted laws that are nearly identical to Connecticut's,[38] and several other states have passed similar laws.[39] In addition, most states recognize a right to privacy, either by statute or by common law, which broadly

[34] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

[35] For guidance on the GLBA Safeguards Rule, see *Financial Institutions and Customer Data: Complying with the Safeguards Rule* (September 2002), *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm.

[36] For additional information concerning educational institutions obligations under the GLBA, see the National Association of College and University Business Officers January 13, 2003 Advisory Report, entitled *Colleges and Universities Subject to New FTC Rules Safeguarding Customer Information*, *available at* http://www.nacubo.org/public_policy/advisory_reports/2003/2003-01.pdf.

[37] Conn. Stat. Title 53, Chapter 949g, § 53-451(b).

[38] Va. Code § 18.2-152.4; R.I. Gen Laws § 11-52-4.1.

[39] *See, e.g.*, Ala. Code § 13A-8-10; Cal. Penal Code § 502; Del. Crim. Code §§ 931-939; Md. Code Ann. § 146.

speaking includes the right to be free from "unwanted intrusion upon seclusion or solitude" or the "public disclosure of private affairs."

Moreover, the absence of comprehensive federal privacy standards has led to a proliferation of state information privacy laws. For example, several states are considering or have enacted privacy legislation that deals with collection of information relating to children, disclosure of health care information, or collection of consumer information. Other laws have been developed to deal with very specific privacy concerns. Many states have laws that expressly provide for the confidentiality of library records, including patron information.[40] Other states have passed laws that restrict the use and/or disclosure of Social Security numbers (SSNs).[41] New York, for example, limits the use of SSNs in schools and colleges. The legislation specifically bars the display of a student's SSN in a posting or public listing of grades, on class rosters or other lists provided to teachers, on student identification cards, and in student directories or similar listings. As a result, many public and private schools in the State are opting instead to assign students identification numbers.[42] Arizona has a similar statute that specifically restricts the use of SSNs by educational institutions. The statute, which became effective June 30, 2002, prohibits any university under the jurisdiction of the Arizona board of regents from assigning an individual identification number to faculty, staff or students that is identical to the individual's SSN.[43] The statute also restricts, though does not prohibit, the use of SSNs by community colleges under the jurisdiction of the State Board of Directors for Community Colleges.[44] In California, businesses, health care providers and schools are barred from:

- Publicly posting SSNs or requiring them for access to products or services;
- Printing SSNs on cards required for accessing products or services;
- Requiring an individual to use his or her SSN to access a web site unless a password is also required to access the site; or
- Printing an individual's SSN on any materials that are mailed to the individual.[45]

While many state laws fall into discrete categories, others are creating new areas of potential liability by proscribing new types of conduct or imposing new obligations. California, for example, recently enacted a law that defines the specific crime of identity theft,[46] as well as a law that requires

[40] *See, e.g.*, Am. H.B. 389, 123d Gen. Assem., Reg. Sess. (Ohio 2000).

[41] Even absent the existence of state law restrictions on SSNs, it is important to note that SSNs, in whole or in part, may constitute "personally identifiable educational information" that is protected under FERPA. *See, e.g.*, *FERPA Advisory Letter: Disclosure of Social Security Numbers*, Family Policy Compliance Office, Dept. of Education (May 2001), *available at*, www.nacua.org/documents/Evangelos_Gizis_Letter.pdf (advising that the use of the last four digits of student SSNs for posting grades, without prior written consent of the students, constitutes an unlawful disclosure of personally identifiable information under FERPA).

[42] N.Y. Educ. Law § 2-b.

[43] Ariz. Rev. Stat. § 15-1823(A).

[44] Ariz. Rev. Stat. § 15-1823(C).

[45] Cal. Civ. Code §§ 1798.85 – 1798.86 and 1786.6.

[46] Cal. Penal Code §§ 530.5 – 530.8.

companies that do business in California to promptly disclose to affected individuals any breach of network security that results in the disclosure of unencrypted personal information.[47] This latter requirement appears to impose an affirmative obligation on institutions to notify those parties who may have a claim as a result of their information potentially having been obtained through unauthorized access to a computer system or network. Moreover, California's municipalities also have joined in the fray by adopting local privacy ordinances regulating the disclosure of certain confidential information by financial institutions.[48]

Another source of headaches for those responsible for information services at public institutions are state freedom of information (FOI) or "open records" laws. All 50 states have such laws, which generally provide citizens with access to public records. While many of these state laws model the form adopted by Congress in crafting the federal Freedom of Information Act,[49] others have developed unique FOI regulatory schemes shaped by state and local policies and special interest group intervention. Therefore, it is important for institutions and their legal advisors to remain up-to-date with the FOI decisions in their state(s). A recurring question is the definition of "public records." Not all state FOI laws define the term, and because most of these laws were created long before networked data systems existed, it is often unclear as to whether e-mail and extra-textual electronic material, such as cookies, log files, and the like should be considered part of the "public records" required to be disclosed. This uncertainty is illustrated by a recent incident involving West Virginia University, in which Sprysoft, a software retailer, filed a FOI request with the University, asking for e-mail directory information that the University makes publicly available. Armed with the results of its request, Sprysoft sent unsolicited e-mails to each West Virginia University student offering a "WVU Academic Software Special."[50] Aside from an interesting question regarding the use of the university name, the fact that the institution inadvertently contributed to the spamming of its students by responding to a FOI request again illustrates the complex issues and unintended consequences that can result when existing information laws are applied in a changing technological environment.

Compliance with state laws is even more challenging in the context of technology-mediated learning: an e-learning student residing in one state may be protected by a set of laws that are different from the ones that apply to the state where the institution he or she is "attending" is located, and vice versa. As a result, the student may become subject to laws very different from those of his or her home state. Where once an institution could be more content with an understanding of federal legal requirements and those of its state of domicile they are now finding it necessary to extend their knowledge base nationally and, indeed, globally. As education becomes increasingly borderless, keeping track of state laws can be an expensive proposition for institutions, and a compliance failure can bring with it the risk of criticism, reputational damage, and costly class action liability.

[47] Cal. Civ. Code §§ 1798.29, 1798.82 - .84.

[48] *See, e.g.*, Daly City Ordinance No. 1295; County of San Mateo Ordinance No. 04126; San Francisco City and County Ordinance File No. 021339.

[49] Pub. L. No. 89-487, 80 Stat. 250 (codified at 5 U.S.C. §552).

[50] *See* Justin Leonard, *SEJ investigates spam mail*, the Daily Athenaeum Interactive, Nov. 21, 2002, *available at* http://www.da.wvu.edu/archives/022111/news/022110,01,01.html; David McHugh, *TECHBITS: Emotions for e-mail, university spam, Linux in China, computer chess*, Foster's/Citizen Online, Nov. 21, 2002, *available at* http://www4.fosters.com/tech/articles/tech_1121_02e.asp.

IV. Practical Implications: What You Can Do

✓ Analyze Applicable State Laws and Municipal Ordinances

Colleges and universities would be remiss to focus only on federal legal requirements and ignore the possibility that states or municipalities may also impose constraints in the areas of information privacy and electronic security. Many laws relating to privacy and security already are on the books at the state level, and others loom in the form of pending legislation. In addition, local governments are getting into the act, passing privacy ordinances to protect consumer rights and the confidentiality of certain types of information. With state and local laws proliferating in this area, colleges and universities would be wise to coordinate with their legal advisors to properly assess and analyze applicable state laws and municipal ordinances. Where appropriate, institutional information security specialists should work with higher education associations and their legislative liaisons to influence the legislative process.

✓ Assess Information Security Vulnerabilities and Risks

The recent information security breaches highlighted above illustrate the increasingly complex challenges faced by institutions that may become subjected to computer attacks or that may face liability for the unauthorized disclosure of personal information. In the wake of these events, college and university IT administrators undoubtedly are already revisiting their network security measures and computer usage policies. At the same time, however, IT administrators should bear in mind that conducting an effective security audit is a complex process and that identifying potential weaknesses is only a part of the equation. In fact, by identifying an institution's vulnerability to unauthorized access to its electronic records, without then promptly instituting appropriate measures to remedy those vulnerabilities, the institution may only serve to heighten its potential liability should a compromise occur. A report documenting security weaknesses issued months or years before a system is compromised – and later obtained under a Freedom of Information or "open records" law request by an inquiring journalist – may in fact add to an institution's woes and result in potential liability, particularly if the weaknesses, once detected, are not remedied. The alternative is no more attractive: simply ignoring the possibility of weaknesses is no protection. Although arguably it is worse to affirmatively know of a problem and fail to act than to remain blissfully ignorant, neither is a desirable route.

✓ Review and Update Information Security Policies & Procedures

College and university administrators and their IT specialists should coordinate closely with each other and with their legal advisors in developing information technology and security policies. Security audits are an important component of creating and maintaining an effective security program. An institution should take care, however, to avoid simply creating a harmful paper trail, and it is important to act upon security findings within a reasonable and responsible time frame.

An institution's policies should be developed with this reaction time in mind. A good policy will be flexible enough to allow the institution to react quickly, and with some discretion, to a variety of situations. A good policy also will appropriately limit access to information based on an assessment of the threats posed to the institution's systems. In developing flexible policies, institutions will have to consider the nature and magnitude of such threats and respond with an amount of security that is commensurate with the associated vulnerability based on the sensitivity of the information that is

being protected. For example, it may be sufficient to provide students access to a web site at which course materials are made available using basic password protection, while at the same time it may be advisable to deploy more stringent authentication measures in allowing root access to the institution's critical systems and information databases.

✓ Review Personnel Policies and Procedures for Access to Sensitive Information

Institutions should focus in particular on their policies and procedures relating to the manner in which access to sensitive information is permitted and managed. A system for effectively managing network access and retiring authorization for former students and employees can greatly improve network security. A related issue is the use of criminal background checks and their role, if any, in higher education. Background checks may be required as a condition of receiving federal contracts or grant funds, and some state laws authorize background checks for certain job positions. But such checks can become a topic of hot debate. For example, when the University of Texas (UT) announced it was adopting a new policy requiring criminal background checks of all job finalists, some faculty leaders and administrators voiced concerns that the policy would inhibit the University's ability to recruit top-notch talent.[51] The outcry was so great that the University later announced that it is limiting the scope of its background check policy to only "security sensitive" positions. Three categories of positions are defined as "security sensitive" – senior-level administrators; child-care and patient-care positions; and employees with access to pharmaceuticals, select agents or controlled substances – but others can be defined as such by the various divisions of the UT system at their own discretion.[52]

No matter how complex a scheme of background checks and security policies an institution has in place, ultimately the information security of an institution hinges on the integrity and honesty of those who are given access. This fact is well illustrated by the recent events at Texas Tech. In mid-January, it was reported that 30 vials of a deadly bacteria were missing from a Texas Tech Health Sciences Center laboratory. Only one researcher had legal access to those vials, and after only a few days of intensive FBI investigation, that prominent researcher was arrested for allegedly making false statements about the vials, which he had previously destroyed.[53] This story had a happy ending because the vials were not in dangerous hands, as administrators and government officials first feared. But this researcher's apparent dishonesty raises questions and concerns about the safety and security of the remaining vials. In a time when fear of bioterrorism runs high, it is not surprising that these types of issues foster considerable debate. Whether background checks, password protection, or advanced measures like biometrics are the security method of choice, institutions would be wise to develop flexible policies that will allow quick action and wide institutional discretion in their administration. It may be difficult, if not impossible, to make an institution

[51] *See* Linda K. Wertheimer, Criminal checks incite UT outcry, the Dallas Morning News, Aug. 22, 2002, *available at* http://www.uh.edu/admin/media/topstories/2002/dmn/200208/20020822criminalck.html.

[52] *See* Chris Piper, *Background Checks Limited*, the Shorthorn Online, *available at* http://www.theshorthorn.com/archive/2002/fall/02-dec-03/n120302-02.html.

[53] *See* Betsy Blaney, *Missing vials of plague samples found in Texas after triggering bioterrorism fears*, Associated Press, Jan. 16, 2003, *available at* http://www.nlm.nih.gov/medlineplus/news/fullstory_11295.html; *Plague researcher held without bond*, Associated Press, Jan. 16, 2003, *available at* http://www.msnbc.com/news/859757.asp?0cv=CB10.

completely secure, but an inability to act, and act quickly, in the face of security threats could invite reputational damage and embarrassing and potentially costly legal proceedings.

✓ Scrutinize Relationships With Third-Party Vendors

All institutions rely, to varying degrees, on the use of third-party vendors and service providers in order to manage their information systems, provide and maintain critical software, and furnish the telecommunications capacity that connects their networks to the Internet or other institutions or applications. It is important to realize that, as is the case with any other link in the chain, vulnerabilities resulting from the procedures and systems relied upon by these third parties can create threats to the information security of an institution's network. Institutions should keep these threats in mind when negotiating or renewing their relationships with third-party service providers. Among other things, it is important to ensure that vendors with access to the institution's confidential information are subject to obligations of confidentiality that will enable the institution to comply with its own obligations of confidentiality under relevant privacy-related laws. In addition, vendors should be contractually obligated to implement data protection and security measures that are commensurate with the sensitivity of the information they are responsible for handling or transmitting. In certain cases, such as under the GLBA, institutions may be obligated by statute to include information security obligations in their third party vendor agreements.

Educational institutions should require vendors of mission critical applications to have in place contingency plans to provide for data back-up and disaster-recovery measures necessary to allow an institution to continue functioning even in the case of a catastrophic event. It also is important to ensure that the institution's vendors are obligated – through "service level agreements" – to timely respond to and escalate problems that may compromise the integrity of the institution's operations. Lawyers for institutions of higher education also should consider including in their IT vendor agreements representations and warranties to the effect that the software and services provided by such vendors will not result in the introduction of any "harmful code," such as Trojan horses, viruses, or backdoors. In negotiating and reviewing agreements with third-party service providers, college and university IT professionals and their lawyers also should bear in mind the potential differences among applicable state laws and seek to have their agreements governed by the laws of the state which will provide the most favorable treatment. This is particularly important in light of the recent developments in state laws described above, as well as the trend among states to enact or to consider enacting laws such as the Uniform Computer Information Transactions Act (UCITA), which to date has been adopted only in Maryland and Virginia.[54]

✓ Review the Institution's Insurance Policies

Educational institutions also can take proactive steps to manage their information security risks by reviewing and, where available, renewing their insurance policy coverage with an eye toward insuring against the risks of cyber security. Although the availability of cyber security coverage is a relatively new product, institutions should at a minimum review their existing insurance policies to consider the potential protections they may offer for the new types of risks they are encountering.

[54] *See* S.B. 142 (Md. 2000); S.B. 372 (Va. 2000); *see also* UCITA Online, http://www.ucitaonline.com/legalart.html.

✓ Develop a Rapid Response Plan and Incident Response Team

The worst time to prepare for a response to a security failure involving the unauthorized disclosure of educational records or other personal information is after it happens. Institutions should plan ahead and have in place a plan for responding to and escalating the decision-making associated with an information security crisis. Among other things, an institution should consider designating in advance an appropriate spokesperson, incident response team, and escalation path.[55]

✓ Work Together with Higher Education Associations and Coalitions to Develop Standards Relating to Information Security

As described above, many of the costs and potential liabilities associated with the increasingly complex challenges faced by educational institutions in the areas of information privacy and security result from the absence of uniform standards. For example, while FERPA may establish a duty on the part of educational institutions to guard against the unauthorized disclosure of educational records, there is virtually no guidance on how far an institution must go to safeguard its computer networks from unwanted intrusions. Absent such standards, institutions remain vulnerable to class action challenges in the event their information security policies and procedures fail to repel unauthorized intruders. Educational institutions at all levels would be far better served through the development and adoption of guidance in the form of recommended "best practices" or similar measures. Accordingly, institutions of higher learning should continue to work together through coalitions and the educational associations that represent them to develop sensible, national policies relating to the protection of their information assets.

FOR ADDITIONAL INFORMATION REGARDING IT SECURITY VISIT:

The EDUCAUSE/Internet2 Computer and Network Security Task Force web site at:
http://www.educause.edu/security

[55] For additional information on formulating incident response plans see Moira West-Brown, et al., *Handbook for Computer Security Incident Response Teams (CSIRTs)*, December 1998, a publication of the Carnegie-Mellon University Software Engineering Institute, *available at* http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf.

IT Assessment Implementation Program Plan

- Gantt Chart
- Resource Sheet
- Resource Usage

References

Porterville College

- McCredie, University of California, Berkeley, and ECAR. *Improving IT Governance in Higher Education.* ECAR Research Bulletin, Vol.2006, Issue 18, August 29, 2006.
- Shein, Esther. *Telepresence – Even Better Than The Real Thing.* CFO Magazine, January 2007.
- Katz, Richard N. and ECAR. *The ECAR Study of Undergraduate Students and Information Technology, 2006.* ECAR Key Findings, December 2006.
- Nichols, Brian. *A New CISO's To-Do List.* Campus Technology Magazine, September 2006.
- Arfman, J.M. and P. Roden. *Project Athena: Supporting distributed computing at MIT*. IBM Systems Journal, Vol.31, No.3
- Spransy, Derek, Emory University and ECAR. *Local IT Security for Colleges, Schools, and Departments: A Higher Education Perspective.* ECAR Research Bulletin, Vol.2006, Issue 24, December 5, 2006.
- Plante & Moran, L.L.P., Technology Support Models & Contrasting Education with Commercial Enterprise. [Online] http://techguide.merit.edu/plantemoran1.htm.
- Global Knowledge. *Microsoft Windows Vista: What To Expect.* [Online] http://www.globalknowledge.com.
- Brittain, K., Kirk, T. and Gartner. *Guidelines for Managing Consolidated Service Desk Technology Implementations.* Gartner Research Note, Decision Framework, DF-10-8704, May, 2000.
- Salomon, Kenneth D., Cassat, Peter C., Thibeau, Briana E., Dow, Lohnes & Albertson, PLLC. *IT Security for Higher Education: A Legal Perspective.* March 3, 2003.
- Gomolski, Barbara, Stanley, Craig, Morello, Diane and Gartner. *Benchmarks Can Help Determine Staff Sizes.* Gartner Research, ID# G00125495, February 11, 2005.
- Gulacheck, Bernard, University of Minnesota and ECAR. *Business Continuity Planning: Process, Impact and Implications.* ECAR Research Bulletin, Vol.2005, Issue 13.
- Dallas, Susan and Gartner. *The Myths and Realities of Workforce Forecasting.* Gartner Research Note, Decision Framework, ID # G00136483.
- Dewey, Tim, Zavata. *Business Metrics for Support Leaders.* White Paper, 2006.

- Antolovic, Laurie G., McRobbie, Michael A., Indiana University and Educause. *Implementing Life Cycle Funding*. [Online] http://www.educause.edu/ir/library/pdf/ERM0152.pdf

- Dell. *Why Windows Vista on Dell?*. [Online] http://www.dell.com/content/topics/global.aspx/solutions/en/winvista?c=us&cs=RC956904&l=en&s=hied

- Microsoft. *2007 Microsoft Office System Suites*. [Online] http://office.microsoft.com/en-us/suites/FX101635841033.aspx

- Ciber. *Questions from the July 18 CIBER Data Governance Webinar*. [Online] http://www.ciber.com/services/integration/pdf/CIBER_DataGov_Webinar_Questions.pdf?category=ei-datagov&title=Enterprise%20Integration%20

- B-Eye. *Data Quality and Data Governance: The Basics*. [Online] http://www.b-eye-network.com/print/630

- Accenture. *Enterprise Data: Opportunities and Threats*. [Online] http://www.accenture.com/Global/Services/By_Subject/Information_Mgmt/Information_Mgmt_Services/R_and_I/EnterpriseDataOpportThreats.htm

- Accenture. *A Framework for Building a Data Governance Strategy*. [Online] http://www.digitalforum.accenture.com/DigitalForum/Global/CurrentEdition/HotTechnologies/A+Framework+for+Building+a+Data+Governance+Strategy.htm

- Accenture. *Data Management and the Journey to High Performance*. [Online] http://www.accenture.com/Global/Services/By_Subject/Information_Mgmt/Data_Management_and_Architecture/R_and_I/DataJourney.htm

- Accenture. *Data Governance*. [Online] http://www.accenture.com/Global/Services/By_Subject/Information_Mgmt/Data_Management_and_Architecture/DataGovernance.htm

Glossary of Terms

Bakersfield College

ATHENA PROJECT FORMULA—an educational computing project at the Massachusetts Institute of Technology, undertaken with IBM Corporation and Digital Equipment Corporation from 1983 to 1991. The project created a model for networking a college or commercial campus, including staffing appropriate support for the model.

DATA GOVERNANCE: 7 LAYERS OF MATURITY (AS DEFINED BY MARTHA DEMBER WITH CIBER, INC.)—

- **Stage 1: *Strategy***
  The implementing institution starts by identifying data issues, their causes and effects, and methods to solve the issues. A charter is developed which states how the data governance team will develop and deploy integrated business and technical support policies, guidelines, and standards to manage the institution's data assets. The charter also describes the roles and organizational structure that responsively and proactively focus on ensuring data integrity.

  Stage 1: *Framework*
  The framework defines the roles and responsibilities of the data governance team. The framework also defines the relationships and dependencies between the data governance and the data architecture.

- **Stage 2: *Scenarios and Validation***
  Institutions will typically take an existing data issue and follow the reactive process to determine the cause and effect of the issue, and then propose a solution. The results of the exercise provide a means to:

  - Refine the data governance processes framework
  - Determine the communication steps involved
  - Identify how best to formulate those steps – e.g., via *e*mail or telephone
  - Identify the most appropriate individuals to play these roles moving forward

- **Stage 3: *Formalized Organization and Responsive Process Rollout***
  As the responsive process is being played out, the roles of data governance – e.g., data governance manager or steward – are formally defined in Human Resources. As appropriate, new positions within the institution are created and filled, preferably with internal resources having the required skills and aptitude to carry out the specified responsibilities.

- **Stage 4: *Proactive Process Rollout***
  As the governance team members become proficient in identifying the causes of data issues, they also become aware of the things that can be done to prevent data issues for occurring in the first place. At this stage, stewards take on the responsibility to identify business events or activities that trigger the process.

- **Stage 5: *Expanded Business Involvement***
  Reaching this stage is marked by the explicit buy-in from key stakeholders and executive management in the data governance program. Priorities have been established to aid in the difficult decisions often required in resolving data issues. Standards compliance monitoring is incorporated as a part of performance measurement; and data-specific technology, processes, and organizational components are aligned with the institutions vision and business objectives.

- **Stage 6: *Stewardship Culture***
  Governance protocols include procedures across divisions and departments that explicitly reconcile priorities, expedite conflict resolution, and build cooperation in support of data quality as a common objective shared at every level of the institution. Data quality education and awareness programs are an integral part of the institution's in-house on-going employee training programs.

- **Stage 7: *Strategic Governance***
  At this stage, the institution transforms data governance and compliance from time-based audits to real-time, change driven, on-demand business processes tat continually assess risks, update policies, and manage resources across the institution. Ultimately it is the institution's people, processes and technology working together organically and autonomically that result in an effective data governance program.

LEADING EDGE TECHNOLOGY USER—individuals who need to be at the forefront of technology including those who:

- Interface with other entities, governments where such interface requires the utilization of the latest technology
- Regularly use very large files or memory intensive applications in the execution of their job duties
- Maintain positions and related duties such as network/system administrators, application developers, graphics and publications development, institutional research, Computer-Aided Design (CAD), scientific or statistical modeling, etc.

LIFECYCLE—The period of time during which information technology hardware and software remains useful to the institution.

MICROSOFT WINDOWS VISTA AERO—Windows Vista will come with 2 user experiences. Windows Vista Basic, Windows Vista Aero. The new Aero experience is designed to show translucent windows, 3-dimnesional perspective, rich textures, advanced color mixes and animations.

REFRESH RATE—The planned rate of replacement for information technology hardware and software.

STANDARD TECHNOLOGY USER—individuals who require a standard level of technology for everyday office functions including those who:

- Have a standardized suite of applications on their desktops (e.g. MS Office Suite), customized applications beyond the standardized suite, Banner application
- Access to file and print servers
- Maintain positions such as classified or confidential staff, management staff, operational support, technical staff, and faculty