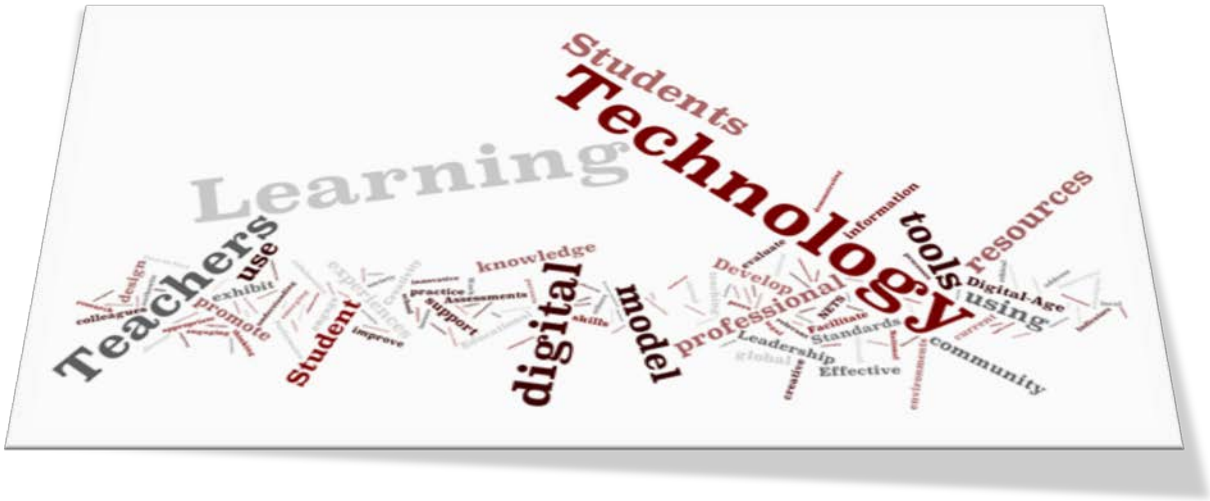
Imperial Community College District

Strategic Technology Plan

2011-2015



Committee Approved: Version April 14, 2011 – **Updated November 12, 2013**

Table of Contents

Vision Statement 3

Strategic Initiatives 3

Support Index 5

Five-Year Roadmap 5

2014 Action Plan 7

Appendix A: Framework for Technology implementation at IVC 9

Appendix B: Technology Support Index 10

Appendix C: Network Security Assessment 20

Vision Statement

Imperial Community College District is committed to empowering students, faculty, and staff to succeed in today's highly connected, collaborative environments. We strive to be an exemplar among California Community Colleges in our use and support of technology by implementing leading technologies, innovative strategies, and proven best practices.

Strategic Initiatives

This plan outlines the strategic initiatives related to the technology implementation at IVC. The *Framework for Technology Implementation at IVC* (Appendix A) is rooted in the identification, leveraging, and implementation of "best practices" in support of student, faculty, and staff success. The framework forms the basis for the strategic initiatives and drives the plan for technology at IVC.

There are four pillars to the framework, which include:

1. Ubiquitous Broadband and Technology Access
2. 21st Century Learning and Working Environments
3. Integrated Data Management Systems
4. User-centered Support Structures

These four strategic initiatives are linked to the institutional goals and objectives in the Educational Master Plan as follows:

1. Ubiquitous Broadband and Technology Access (EMP Goal 3)
2. 21st Century Learning and Working Environments (EMP Goal 2)
3. Integrated Data Management Systems (EMP Goal 1)
4. User-center Support Structures (EMP Goal 1)

Initiative One:
Ubiquitous Broadband and Technology Access

We shall provide students, faculty, and staff with access to a reliable infrastructure and computing systems to support anytime, anywhere teaching and learning. (EMP Goal 3)

Principles in Support of Initiative One
1. Robust, reliable network architecture
2. High-speed wired and wireless access in all classrooms and instructional areas
3. Wireless access throughout campus
4. Reliable, well-maintained technology and computing devices

Initiative Two:
21st Century Learning and Working Environments

We shall provide technology-rich learning and working environments that promote the acquisition and use of 21st Century Skills. (EMP Goal 2)

Principles in Support of Initiative Two
1. Appropriate technologies, tools, and content is readily available
2. Technology renewal and replacement is on predictable cycles
3. Faculty/staff-driven principles for selecting and deploying technologies
4. Actively embrace student technology use

Initiative Three:
Integrated Data Management Systems

We shall implement and support enterprise data systems that support effective decision-making and promote synergy, collaboration, and efficiencies throughout the organization. (EMP Goal 1)

Principles in Support of Initiative Three
1. Highly utilized enterprise-wide learning management systems
2. Best of breed student information and administrative systems
3. Leveraged cloud computing and data warehouse models
4. Secure authentication, authorization, and provisioning

Initiative Four:
User-centered Support Structures

We shall provide support structures that encourage confidence and success for all users. (EMP Goal 1)

Principles in Support of Initiative Four
1. Just-in-time support
2. Best of breed web support and documentation
3. Diverse learning options
4. Actively promote use of communities

Support Index

A Support Index was developed in support of the four strategic initiatives at IVC. The Support Index was modeled after the International Society for Technology in Education's (ISTE) Technology Support Index, which is a tool for districts to profile their technology support programs. It has been modified to support the *Framework for Technology Implementation at IVC* and serves the following purposes for this strategic plan:

1. It identifies a continuum of support capacity and efficiency levels, ranging from "Deficient" to "Exemplary".
2. It identifies the "targets" for IVC's technology implementation. These are represented as **Bold and GREEN Text** in the Index. These targets are identified as where we plan to be by 2015.
3. It identifies the current status (as of last document update) of IVC's technology implementation. This "self-study" forms our baseline for accountability. Our current status is shaded **RED** if not at target, **GREEN** if target is currently met.

From this identification of targets and the self evaluation of our current status, the Technology Planning Committee (TPC) developed an Action Plan for Year 1 of this Strategic Technology Plan. Each year, the TPC will evaluate progress, modify the Action Plan, and set priorities for the following year. This approach will permit the college to be responsive to emerging needs, as well as budget constraints and/or opportunities. The Strategic Initiatives and Support Index outlined in this Plan will drive this process each year.

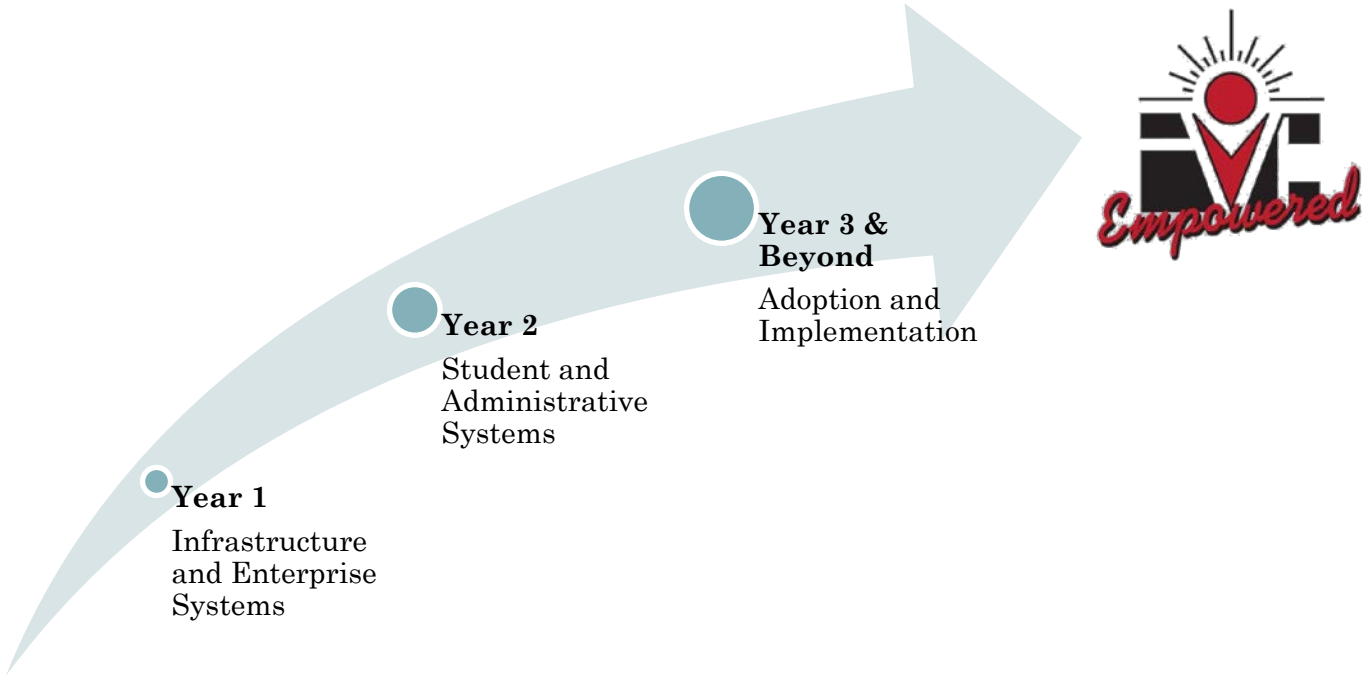
Five-Year Roadmap

Year 1 of this Strategic Plan is focused on improving the Enterprise Systems and core infrastructure to support the vision for IVC. In October 2010, a Network Security Assessment (Appendix C) was conducted to review the mission critical infrastructure and applications in the Data Center. This assessment revealed

several areas that require attention, identified as either critical, moderate, or suggested. Additionally, comprehensive plans for the virtualization of the Data Center, along with the upgrade and expansion of the network infrastructure across campus will be developed.

Year 2 of this Strategic Plan will be focused on the implementation and support of comprehensive student and administrative systems that support the efficient operation of the college. These include student cloud-based applications, improved information portals, and an Operational Data Store (ODS) and standardized reporting framework for our BANNER Enterprise Resource Planning (ERP) system. Additionally, faculty and staff development programs will be implemented to promote the effective use of technology across campus.

Years 3-5 will be focused on adoption and implementation of technology in the classroom and in essential business practices on campus. As mentioned earlier, each year the TPC will review progress and develop annual Action Plans to capture priorities and sequence activities outlined in this plan.



In October 2010, IVC was awarded a 5-year federal Title V grant focused on innovative approaches to teaching through technology. The *Access to Technology Leads to Advancement and Success* (ATLAS) program provides support resources toward the implementation of this strategic plan. This plan will incorporate the goals and objectives of the ATLAS grant each year.

In addition to the ATLAS grant, IVC is currently undertaking major modernization and facility improvements, which is supported by the passage of Measure J in November 2010. The modernization and construction of new facilities will span the next 7-10 years. It is imperative that this Strategic Technology Plan coordinate with these activities to maximize funding and provide for an integrated implementation of technology on campus.

2014 Action Plan

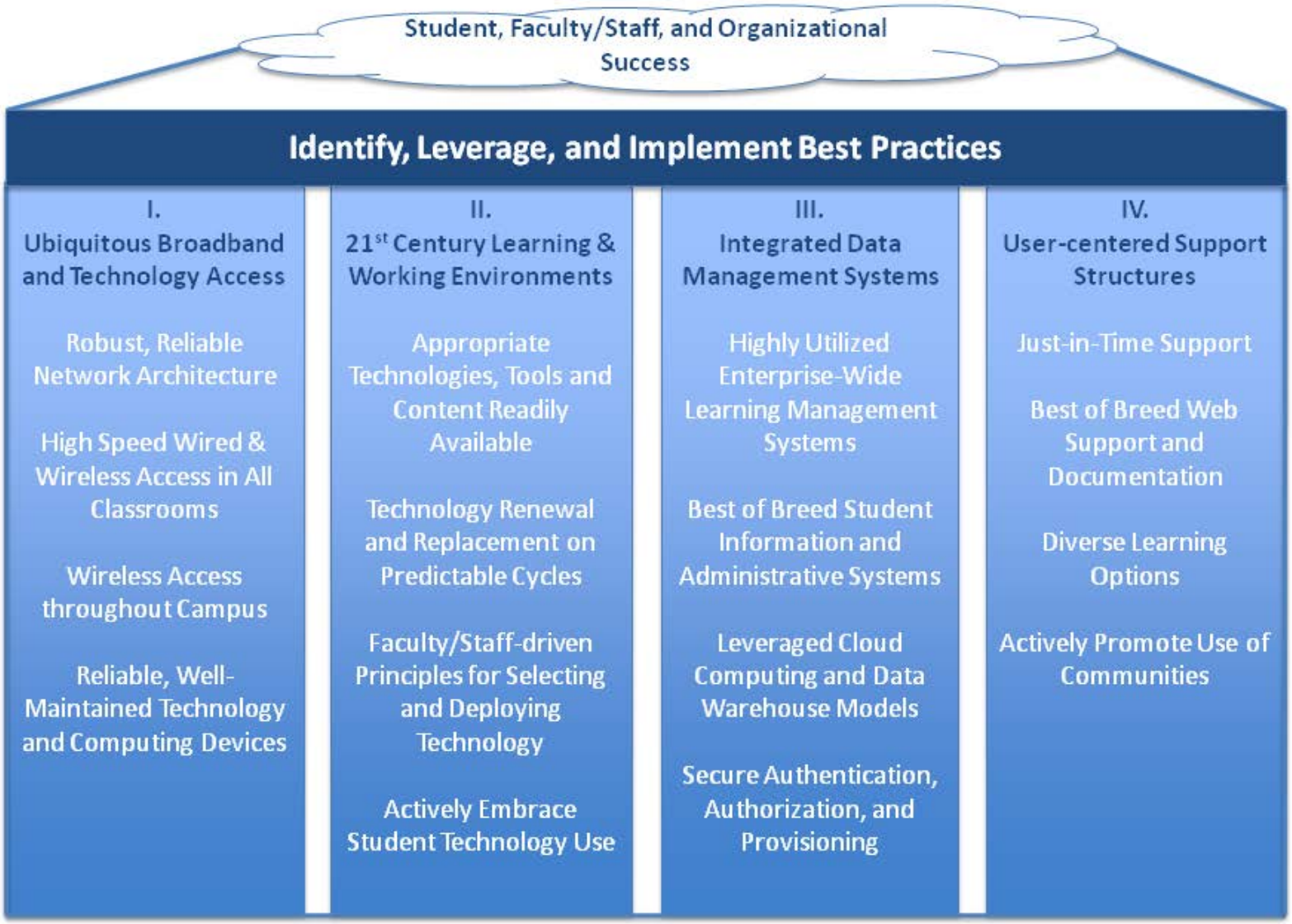
The following activities are outlined for calendar year 2014.
(Items 1-14 are carried over from the 2012 and 2013 Action Plan)

1. Complete the installation of and training for Position Control for Banner Integration
2. Evaluate and make recommendations for strengthening protection of confidential and personal information across systems and business practices
3. Conduct inventory of all instructional classrooms and make recommendations for improvements
4. Evaluate and make improvements to network design and architecture, and thoroughly document network
5. Fully implement System Center 2012 to manage, maintain, and support systems across campus
6. Complete testing and develop roll-out plan for Sharepoint
7. Evaluate Lync as a communications platform and develop recommendations for its use
8. Complete training and full implementation of the SonicWall Firewalls
9. Complete implementation of network performance monitoring and alerting
10. Integrate video surveillance systems on campus
11. Evaluate access control system for integration with Banner
12. Investigate and develop plan for migrating to Banner XE
13. Complete loading of electronic transcripts into Banner
14. Investigate and develop plan for migration to Open CCCApply

---

15. Investigate and implement strategy for Network Access Control and Problem mitigation (1.10)
16. Investigate providing multiple desktops, groups of applications, virtual computers to a single location (1.9)
17. Establish Software Standards for both Faculty, Staff and Lab computers (2.7)
18. Work on Policies and Procedures for authentication, authorization and provisioning and business practices (3.5)
19. Develop plan to refresh hardware for Banner, BDMS(including storage), and Degree Works.
20. Complete BDMS backup to EVault (Cloud Back-up Solution).
21. Improve business processes and new student ed planner for Degree Works.
22. Complete 2014 phase of MIS requirements for Student Success Act.
23. Complete 2013 phase of full year projected class schedule planning tool.

Framework for Technology Implementation at IVC



Appendix B

Domain I –Support for Ubiquitous Broadband and Technology Access

	Deficient Support Capacity and Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	Exemplary Support Capacity and Efficiency
1.1 Virus Protection	No virus software is used.	Virus software is used, but it is client-based and therefore often out of date.	Server-based virus software is used, but the parameters for its use are loosely defined and updates aren't consistent.	Server-based virus software is available, used, and automatically updated.
1.2 Network Infrastructure and Bandwidth	Network access is limited and isn't available in every location.	Network access is available to all locations, but doesn't impact all computers and is limited in bandwidth.	Network access is available to all locations but segments of the network are limited in bandwidth.	Robust broadband network access is available to all locations allowing for unlimited network control and tool use.
1.3 Desktop and Software Standardization Tools (Profiles)	No desktop standardization tools or practice are used.	Desktop standardization tools are in place, but are mostly ignored once the equipment is deployed.	Desktop standardization tools are in place, but changes users make aren't automatically corrected.	Desktop standardization tools are used to provide a common desktop for all users and access to common software. Changes to the desktop are automatically corrected.
1.4 Integrated and Systemic Electronic Communication	Electronic communication is limited and has little use for providing technical support.	Electronic communication is available to many staff but isn't integrated at all into the daily work of employees.	Electronic communication is available to everyone in the organization but isn't readily used for technical support.	Electronic communication is available to everyone in the organization and is integrated into daily work so that it can be used for technical support.
1.5 Remote Computer Management	No remote management is available.	Remote management is available for servers only.	Remote management is available for all computers but isn't used extensively.	Remote management is available for all computers and is used as a primary strategy of support.

	Deficient Support Capacity and Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	Exemplary Support Capacity and Efficiency
1.6 Imaging Software	Imaging Software isn't used.	Imaging software is used in the most primitive sense — only providing recovery services with the imaging software provided by the vendor.	An image is used for delivery of the machine but isn't used to clone all of the software on the machine. Only the basic OS and basic software is imaged. Imaging is used as a troubleshooting strategy.	Imaging software is used for delivery of new machines, and as a troubleshooting strategy. Software installed through the imaging process is comprehensive.
1.7 Metering and Application Push Technology	Metering and Push technology isn't used as a district tool.	Metering and Push technology is used for metering but isn't used for installation and updates, and its use is limited in scope.	Metering and Push technology is used for metering and some software updates, but major software installations are handled on the individual computer.	Metering and Push technology is used for all software distribution, technical updates, and for metering of software use on the district's computers.
1.8 Thin-client Computing	Thin-client computing isn't used.	Thin client is used but is limited to a small number of users for specific applications.	Thin client is used for most users of administrative systems and some productivity software.	All administrative and productivity software for staff is delivered through a thin-client model.
1.9 Vendor-specific Management Tools	Vendor tools aren't installed or considered when purchasing hardware.	Vendor tools are available and have been purchased but are mostly unused.	Vendor tools are used in a limited way for diagnosis and prevention.	Vendor tools are used extensively for diagnosis of issues, to streamline processes, and for preventive measures.
1.10 Network Sniffing Tools	No network sniffing tools are used.	Network sniffing tools are used for problem diagnosis only.	Network sniffing tools are used for problem diagnosis and limited preventative maintenance.	Network sniffing tools are used to both diagnose problems and establish performance matrices for preventative maintenance. The network is systematically monitored using these tools.

Domain II –Support for 21st Century Learning and Working Environments

	Deficient Support Capacity and Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	Exemplary Support Capacity and Efficiency
2.1 Cycling of Equipment	No replacement cycle has been defined.	Equipment is placed on a replacement cycle greater than 5 years.	Equipment is placed on a 4–5-year replacement cycle.	Equipment is placed on a 3-year replacement cycle.
2.2 Brand Selection (e.g., Compaq, Dell, Apple, IBM, etc.)	No brands are specified; purchasing is done by price only, and is site controlled.	A district brand is selected, but changes from year to year depending upon what vendor is providing the best selection at the time.	A district brand has been selected, but isn't strictly enforced allowing for purchasing of some equipment that is outside the standard.	A district brand has been specified, and all purchases are made within that brand over an extended period of time.
2.3 New Equipment Deployment	The campus and local staff are responsible for the deployment of new equipment.	The technical staff manages deployment of new equipment requiring a substantial reduction in regular service during deployment.	Additional help (internal or contracted) is utilized for imaging and tagging of equipment, but setup is the responsibility of the regular technical staff creating some delays in regular service.	Additional help (internal or contracted) is utilized for all deployment functions providing no delays or disruptions in regular technical service.
2.4 Model Selection	There are no limitations on model selection.	A model line has been selected, but many choices are given within that line.	A model line has been selected, and choices are limited to 3–5 models.	Model selection is limited to one or two, with few variations.
2.5 Platform (e.g., Apple, Windows, Sun)	The district supports two or more platforms, and platform choice is left to individuals in the district.	The district supports two or more platforms, but choices are made by departments at large and are generally uniform.	The district supports two platforms with one predominant platform for general use, and a second platform for specific programs and/or instructional applications.	One platform is selected for the district, with few exceptions for special projects only.
2.6 Standard Operating System (OS)	Four or more OS versions are used, and all are "supported" by the district.	Three OS versions are used, and the older OS computers are either migrated or receive limited support.	Two OS versions are used, with most equipment migrated to the most recent OS.	One OS version is used district-wide, with all computers migrated to that OS.

Domain II –Support for 21st Century Learning and Working Environments

	Deficient Support Capacity and Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	Exemplary Support Capacity and Efficiency
2.7 Application Software Standard	No software standards have been established.	Software standards are established. Nonstandard installations are permitted and some support is provided.	Software standards are established. Nonstandard installations are allowed but no support is provided.	Software standards are established and only those applications on the list are permitted on computers.
2.8 Donated Equipment	Donated equipment is accepted with no regard to whether it meets district equipment standards.	Donated equipment is accepted with minimum performance requirements with no regard to brand or age.	Donated equipment is accepted with minimum performance requirements and suggested brand. Equipment is less than 3 years old.	Donated equipment is accepted but only if it meets specific brand, model, performance, and system requirements. Equipment is less than 2 years old. Cash donations are encouraged so new standard equipment can be purchased.
2.9 Peripheral Standards (e.g., printers, scanners, digital cameras, projectors, video, etc.)	No peripheral standards are set.	Peripherals are standardized by brand but models within the brand aren't. The peripheral standards change frequently and are rated for consumer use.	Peripherals are standardized by brand and model, but the list contains many options with many consumer-rated items.	All peripherals are standardized, with specific models identified that are primarily rated for enterprise use. Brands and models are limited.
2.10 Surplus practice	Equipment isn't added to surplus until it is no longer usable and is supported as resources allow.	Surplus equipment is supported by district personnel but as a low priority.	Surplus equipment is no longer supported by district personnel but can be used by district until it breaks.	Surplus equipment is taken out of service when it reaches the replacement age even if it still works.

Domain II –Support for 21st Century Learning and Working Environments

	Deficient Support Capacity and Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	Exemplary Support Capacity and Efficiency
2.11 Contracted Support	Contracted support isn't used.	Contracted support is used for emergencies, but not as a part of the overall support strategy.	Contracted support is used as part of the overall support strategy, but has not been evaluated to determine the most strategic places and circumstances to use contractors.	Contracted support is strategically used as an effective part of the overall support strategy to solve complex problems and/or realize savings and efficiencies.
2.12 Warranties	No additional warranties are pursued beyond the standard warranty (1 year).	Extended warranties are purchased but don't cover the life of the equipment and doesn't include peripherals (3 year, computers only).	Extended warranties are purchased to extend the standard warranty on computers and peripherals but don't cover the equipment lifespan (3 year, all equipment).	Warranties are purchased to cover the life of the equipment (5 or more years).

Domain III – Support for Integrated Data Management Systems

	Deficient Support Capacity and Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	Exemplary Support Capacity and Efficiency
3.1 Server Farms and Centralized Services	Every site has its own server and, in some cases, multiple servers. Backup and server management takes place locally.	Each site has only one server with some services (e.g., e-mail, student information system [SIS]) provided centrally.	Many servers are consolidated into a few locations and most services are provided centrally.	All servers and services are centralized requiring minimal server management outside of one location.
3.2 Use of Application Service Providers (ASP)	No ASP services are utilized.	One or two ASP services are used, but it doesn't impact support due to the peripheral nature of the product.	A number of ASP services are used but is limited to one category of software (e.g., productivity, research, libraries, content, etc.).	ASP services are used for appropriate applications, including productivity, content, and research based applications.

Domain III – Support for Integrated Data Management Systems

	Deficient Support Capacity and Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	Exemplary Support Capacity and Efficiency
3.3 Enterprise Systems	Enterprise systems aren't in place.	Enterprise systems are partially in place, but aren't reliable or intuitive.	Enterprise systems are in place and are reliable, but don't integrate well with other systems and aren't intuitive.	Enterprise systems are in place, reliable, intuitive, and integrate nicely with other productivity tools.
3.4 Identity Management	No systemic processes exist to manage identities of faculty, staff, and students.	A basic system of identity management exists, but there is no authoritative source for identity records.	Authoritative sources for identity management exist supporting most critical systems.	A federated authoritative source for identity management exists supporting all critical systems.
3.5 Secure Authentication, Authorization, and Provisioning	No policies and procedures exist to address authentication, authorization, and provisioning, and business practices are inconsistent across campus.	Some policies and procedures exist, but business practices are not regularly audited and reviewed.	Policies and procedures are well-documented.	A consistent, well-documented method for providing and restricting access to resources is in place, is periodically audited, and is appropriately protected.
3.6 Cloud Computing	No cloud services are utilized.	Some systems are migrated to cloud services when being replaced or refreshed.	All systems are reviewed for suitability in the cloud environment. Systems are migrated as resources are available.	A structured process exists to evaluate each application for appropriateness of cloud delivery, which is widely adopted on campus.
3.7 Data Warehousing	No central repository for institutional data exists.	Multiple repositories exist and are not integrated together.	A central repository exists, but multiple reporting tools are used to support campus use.	A central repository for campus data is in place, and advanced reporting tools are provided to support data-driven decision making.
3.8 Data Governance and Security	No policies and procedures exist to address confidential information, and business practices are inconsistent across campus.	Some policies and procedures exist, but business practices are not regularly audited and reviewed.	Policies and procedures are well-documented.	A consistent, well-documented method for protecting confidential information is in place, is periodically audited, and is appropriately protected.

Domain III – Support for Integrated Data Management Systems

	Deficient Support Capacity and Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	Exemplary Support Capacity and Efficiency
3.9 Learning Management Systems	No Learning Management Systems exist to support instruction.	Multiple LMS's are available, and are not integrated with campus enterprise systems nor supported by IT.	A single LMS is provided, is somewhat integrated with campus systems, and is supported by IT.	An enterprise LMS is fully integrated with campus systems and is well supported for faculty and students.

Domain IV – Support for User-Centered Support Structures (Staffing, Training, and Professional Development)

	Deficient Support Capacity and Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	Exemplary Support Capacity and Efficiency
4.1 Organizational Structure	Direction comes from multiple points within the organization, and reporting isn't functionally logical. Cross-functional collaboration is difficult or non-existent.	The reporting structures are difficult to identify, and direction comes from multiple points of the organization. Cross-functional collaboration exists.	The technical support functions and instructional technology functions report differently, but each unit is cohesively organized and there is communication between units.	All of the technology functions report through the same unit in the organization, providing for a logical chain of command and communication structures with the unit clearly supporting the district mission.
4.2 Formula-driven Technology Staffing (e.g., X computers + X network drops + X applications divided by Y = # of technicians)	Staffing formulas aren't used or considered.	Formulas for staffing are considered but are limited in scope and aren't used to drive staffing.	Comprehensive formulas have been developed, considering multiple dimensions of the environment, but are only used as a guide and don't drive staffing.	Comprehensive formulas have been developed and drive staffing as a normal part of operations. Formulas include multiple dimensions of the environment.

Domain IV – Support for User-Centered Support Structures (Staffing, Training, and Professional Development)

	Deficient Support Capacity and Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	Exemplary Support Capacity and Efficiency
4.3 Escalation Process for Technical Issues	No escalation process is in place, and the path for resolution is unclear.	A clear path for resolution is in place, but no escalation process is recognized.	An escalation process is in place with two steps of escalation and significant crossover between levels.	A well-defined escalation process is in place, with three or more steps of escalation, and a clear path for resolution.
4.4 HelpDesk	No Help Desk support is provided.	A Help Desk is provided but isn't adequately staffed.	A district Help Desk is in place and staffed, but it is not used systemically as the first line of defense.	A district Help Desk is in place with trained staff, and the district culture embraces the Help Desk as the first line of defense.
4.5 Trouble Ticketing System	No trouble ticketing system exists.	A simple trouble ticketing system is in place, but isn't electronic and/or is simple in its implementation, not allowing for universal tracking of issues and establishing trends.	A trouble ticketing system is in place and is used extensively for responding to technical issues. Analysis of issues, response times, and possible trends isn't done effectively.	All technical issues are recorded and delegated to appropriate resources through an electronic trouble ticketing system. All technical issues are tracked and evaluated through this system.
4.6 Use of Online Knowledgebase for Technical Help	Staffs seek no help from online help both due to availability of resources and district culture.	Some staff seeks online help, but the behavior isn't pervasive and the resources are limited.	Many staff seeks online help and there are several broad resources available. Use is not organizationally pervasive.	Most staff seeks help from online knowledge bases as their first resource for help from diverse and comprehensive resources. This is a pervasive part of the culture.
4.7 Software Support Protocols and Standards	No list of supported software is provided for users.	A list of supported software is provided, but no differentiation is made for the kind of support a given category of software will receive.	A list of supported software is provided and differentiation is made for the kind of support a given category of software will receive; however, users don't follow the different processes closely.	A list of supported software is provided, with clear differentiated support processes for each set of software that are consistently used.

Domain IV – Support for User-Centered Support Structures (Staffing, Training, and Professional Development)

	Deficient Support Capacity and Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	Exemplary Support Capacity and Efficiency
4.8 Documented Procedures	Little or no documentation exists for technical tasks — requiring users and technical staff to invent their own solutions.	Some documentation exists for technical tasks but isn't widely shared or used. Most documentation is limited to few technical staff only.	Documentation exists for many technical tasks but is not well written and isn't systematically updated as procedures are developed.	Documentation exists for most technical tasks and is used by most user groups. Well-written documentation production is a normal part of operations.
4.9 Certification of Technical Staff	Certification isn't a priority in the organization and concerns are raised about time away from the job to pursue certification.	Appropriate technical staff is encouraged to become certified, but no support is provided towards certification.	Some technical staff is certified in appropriate areas, others are involved in district-supported programs towards certification.	Most technical staff is certified in appropriate areas (e.g., A+, Cisco, MCSE, etc.) and new certifications are strongly encouraged.
4.10 Differentiated Job Descriptions	Technical support employees do it all creating redundancies and inefficiencies.	Technical support employees do it all, but redundancies aren't created due to size and/or staffing levels.	Some differentiation in jobs has occurred, although assignments aren't provided based upon skill-set competencies.	Job descriptions are fully differentiated creating specialization and efficiencies, and a clear avenue for support.
4.11 Retention	Employee turnover is high primarily due to low employee satisfaction.	Employee turnover is high primarily due to other employment opportunities.	Employee turnover is moderate (excluding retirement), and employee satisfaction is good.	Employee turnover is low (excluding retirement), and employee satisfaction is high.
4.12 Competitive Compensation	Technical positions are poorly competitive, offering compensation in the bottom 50% of equivalent organizations in the area.	Technical positions are moderately competitive, offering compensation in the 50th to 75th percentile of equivalent organizations in the area.	Technical positions are competitive, offering compensation in the 75th to 90th percentile of equivalent organizations in the area, and offering competitive non-compensation benefits.	Technical positions are very competitive, offering compensation in the 90th percentile of equivalent organizations in the area, and in some cases, competing with private businesses for talent.

Domain IV – Support for User-Centered Support Structures (Staffing, Training, and Professional Development)

	Deficient Support Capacity and Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	Exemplary Support Capacity and Efficiency
4.13 Comprehensive Staff Development Programs – overall organizational capacity	There is no formal staff development program in place, and training is provided infrequently. The organization depends upon individuals' own motivation to build expertise.	A staff development program is in place but is limited, voluntary, and uses a single dimension in its delivery.	A staff development program is in place. It isn't comprehensive in nature in that it doesn't impact all staff and doesn't offer the depth required to change the organization.	A comprehensive staff development program is in place that impacts ALL staff. The program is progressive in nature and balances incentive, accountability, and diverse learning opportunities.
4.14 Online Training Opportunities	Online training opportunities don't exist.	Online training opportunities exist, but are limited in scope and are available to a limited population of employees.	Online training opportunities are available for staff onsite and remotely, but are limited in their offerings.	Online training opportunities are provided for staff both onsite and remotely, and represent a diversity of skill sets.
4.15 Just-in-time Training	No just-in-time training process or delivery system has been put into place.	Just-in-time training is used, but the process and delivery system hasn't been refined so that it can be used realistically within the organization.	A process and delivery for just-in-time training is in place, but hasn't been adopted by the organization as a mechanism for solving issues.	A process and delivery system has been established for just-in-time training organization-wide and is used consistently.
4.16 Expectations for All Staff	Expectations of staff aren't clearly defined and aren't part of the organizational culture.	Expectations of staff are articulated but are limited in scope.	Expectations of staff are articulated and are broad in scope, but have not been adopted as part of the organizational culture.	Expectations for all staff are clearly articulated and are broad in scope. Performance expectations are built into work functions and are part of the organizational culture.
4.17 Training for Technical Staff	Technical staff is only given training to take care of the immediate issues in the district. Advanced training isn't encouraged.	Technical staff receives consistent training around emergent issues. Advanced training isn't district sponsored but is encouraged.	Technical staff receives consistent training around emergent issues and have limited district-sponsored opportunities for advanced training.	Technical staff receives ample training as a normal part of their employment, including training towards certification.

Domain IV – Support for User-Centered Support Structures (Staffing, Training, and Professional Development)

	Deficient Support Capacity and Efficiency	Limited Support Capacity and Efficiency	Satisfactory Support Capacity and Efficiency	Exemplary Support Capacity and Efficiency
4.18 Quality Assurance (QA) and Customer Follow-up	Surveys are conducted generally as part of other departmental survey work within the organization or not at all.	QA surveys are conducted, but they aren't automated and are only done annually.	Surveys specific to technical support are conducted. However, they are done only periodically.	QA is measured by a random and automatic system that tracks customer satisfaction and closed tickets. Data is collected throughout the year. Questions asked are specific to technical support and the data is used to make adjustments.
4.19 Troubleshooting as Part of the Professional Development Program	Basic troubleshooting isn't considered part of professional development.	Troubleshooting is built into professional development, but is too technical in nature and isn't balanced with a technical support system.	Troubleshooting is built into the professional development program and is used as a major strategy for technical support.	Basic troubleshooting is built into the professional development program, and is used as a first line of defense in conjunction with technical support.

Executive Summary

Imperial Valley College (IVC) was evaluated on their overall Technology infrastructure to analyze possible flaws in the architecture and minimize the risk of a security breach. This assessment focuses primarily on data networks and enterprise systems such as servers and dedicated appliances.

Each segment of the assessment will have a severity level assigned. IVC should use these levels to prioritize the work that needs to be done after the completion of the assessment. The following levels will be used throughout the document:

- **Critical**: This priority suggests that these areas should be addressed first and represents a potential security concern.
- **Moderate**: This level of priority represents findings or configuration changes that will enhance the performance of existing systems, but they don't represent a significant security concern.
- **Suggested**: The areas marked with this priority are findings that should be addressed when resources are available.

Documentation

Severity Level = Critical

In general, system documentation is lacking and the existing records don't seem to be up-to-date. System documentation such as: network diagrams, master password lists, system configurations, wiring schematics and an overall catalog of systems and services needs to be developed in order to minimize disruption of services during outages.

Status: *Accurate documentation continues to be an area of high need. This past year has been spent collecting existing documentation from various sources. As areas of this plan are implemented, system documentation will be a priority.*

Network

Entry points

IVC has two locations that serve students in Imperial County. The main campus is large in size and houses the technology infrastructure. A remote campus located in Calexico is connected to the main campus through a T-1 circuit provisioned inside the network. Both locations are protected by one Cisco 5550 ASA firewall that serves as the perimeter for the IVC network.

IVC connects to the Internet through a direct connection to the CENIC network and another connection through the IVTA. This should provide IVC redundancy to the commodity Internet should one of the paths fail. All Internet traffic flows through the firewall and through the use of access lists; IVC can control the flow of traffic that enters the network.

IVC uses the Microsoft RAS to provide Virtual Private Network (VPN) servers to allow trusted users to access IVC network resources from any network location through an encrypted channel. This service is primarily used and limited to IT staff, IT consultants and high-level managers.

The largest entry point of the network is through the wireless network system. The college uses the Extricom wireless solution to provide access to mobile devices to faculty and students. Security control mechanisms are applied at the HP internal switches through access lists.

Calexico Campus

The Calexico IVC campus is comprised of a few faculty computers, a computer lab and several classrooms that connect via a T-1 to the main campus. Special attention to remote sites is required to ensure best practices are followed and that unauthorized devices are not connected to the network.

Network Perimeter

Firewall Assessment

Platform: Cisco Adaptive Security Appliance (ASA)

Model: 5550

Software Version: 7.2(2)

Firewall configuration

Severity level = Critical

After reviewing the firewall configuration, the following changes are recommended:

Recommendations redacted due to security concerns.

Status: *Edge security is always of the utmost concern. The firewall was replaced with two Sonic Wall next generation firewalls. These firewalls provide greater visibility and control of the traffic that traverse it. The configurations, including access lists, were reviewed along with the recommendations within this document when implementing the new equipment. The configurations will continue to be reviewed on an on-going basis.*

Hardware Redundancy

Severity Level = Moderate

IVC currently runs a single Cisco ASA 5550 firewall appliance. IVC should consider installing a second firewall for redundancy purposes. The firewalls can be installed in an active-standby configuration to provide hardware fault tolerance should one of the appliances fail. IVC should also ensure that this critical link in the network has premium support from the manufacturer for quick replacement.

Status: *We have replaced the single Cisco ASA with two Sonic Wall firewalls. This provides the recommended hardware redundancy at the firewall level that was recommended.*

Virtual Private Network (VPN) Access

IVC uses the Microsoft RAS/VPN services in Windows 2003 server. This provides remote access to network resources via an encrypted connection through this server. The server currently has two network interfaces,

one facing the internal network and another facing a DMZ on the firewall. Users authenticate using their Active Directory account, which need to be members of the "secVPN" group, which currently has 37 users (8 disabled) accounts.

Recommendations:

- The current physical server running the RAS services is probably about 6 to 7 years old and will need to be replaced soon. It is recommended to move this security function to the firewall and have all perimeter security handled by this device.
  Severity level = Moderate
- *Recommendations redacted due to security concerns.* (Severity level = Critical)
- Remove disabled accounts from the secVPN group.
  Severity level = Suggested

Status: *VPN access is now handled at the firewalls. The old secVPN group was replaced with the VPN ACCESS group and the members were reviewed and updated.*

Application Protection

Severity Level = Moderate

It is recommended that IVC consider moving server farms into a Demilitarized Zone (DMZ) connected to the firewall. *Recommendations redacted due to security concerns.*

The firewall is a dedicated appliance for this purpose and would centralized network security in one device. Moving servers into a DMZ has many implications and this process would need to be planned carefully to minimize down time to end users.

Status: *As noted within the recommendation, this process needs to be carefully planned to minimize the effect on the end users. With the many other projects that are currently under way we are still in the planning phase.*

Calexico Network

Severity Level = Moderate

The Calexico remote campus connects to the main campus via a T-1 line (1.54 Mbps). The capacity on this telecommunications circuit is not adequate for today's business requirements and it connects to very old equipment that is subject to failure soon. It is recommended that IVC explore other alternatives to connect the site with refreshed equipment that can provide more adequate bandwidth.

A thorough check of the campus should be done to ensure only authorized network devices are connected to the network.

Status: *The Calexico Campus no longer exists. If it is decided to re-open a dedicated campus in Calexico we will explore all options to provide sufficient telecommunications capacity.*

Network Authentication

Severity level = Critical

Recommendations redacted due to security concerns.

Due to the large amount of network devices on the network, it is highly recommended that IVC explore a solution to centralize authentication services to administer network devices. The solution should integrate with MS Active Directory to support single sign-on, which means that technical administrators would use their domain account to login to network devices.

A recommended solution is to explore the Network Policy Server embedded in the Windows 2008 server. This new built-in feature provides RADIUS authentication that uses Active Directory to authenticate users. Additional details can be obtained at: http://www.microsoft.com/windowsserver2008/en/us/security-policy.aspx.

Status: *We have moved all of our Network Administration to a single sign-on platform using Radius, via Windows 2008 Data Center.*

Network Segmentation

IVC's internal network has multiple VLANs created to isolate layer 2 broadcast domains. Connections between switches are trunked to allow multiple VLAN traffic to return to the core and out to the Internet. All switches appear to have the spanning-tree protocol turned on, which helps prevent network loops in the topology. Network ports where an IP phone is connected should also be configured as a trunked port to allow a computer to connect to the phone. The following are some low-level priority recommendations:

- Reduced the size of the IP subnet in most VLANs. Some VLAN's are configured with address spaces for 500 to 1000 nodes. It is unlikely to have this many nodes in one given VLAN and doing so would be problematic. A more reasonable size is the Class C size of 253 hosts per VLAN.
  Severity level = Suggested
- Update documentation to explain the different purposes of each VLAN. Severity level = Moderate
- Reserve the first 50 IP addresses in the available scope for static addresses. Severity level = Suggested
- When possible, use DHCP address reservation versus statically assigning the address to end nodes. This does not apply to servers.
  Severity level = Suggested
- Assign a unique PAT address on the firewall per internal VLAN. This will ease the identification of source traffic from the outside perspective.
  Severity level = Moderate
- Ensure a PTR DNS recorded is updated when a computer is leased a new IP address.
  Severity level = Moderate

Status: *The redesign of the Network is an on-going project that is being tackled as the different portions of the network are being upgraded. For example, when we replaced the wireless network we redesigned the wireless subnets as part of that project.*

Network Monitoring

IVC currently uses the Hewlett Packard (HP) Procurve Manager software to manage their network switch infrastructure. The software has access to all network devices in the campus. The system has the following management functions through the console:

- Configuration review and changes
- Hardware configurations
- SNMP trap collector
- Create, manage and track policies
- Real-time traffic

The IVC internal network provides switching and routing to support Internet Protocol (IP) through the main campus and Calexico. The HP switches support the OSPF routing protocol operating on the backbone switches across the campus. Virtual LANS or VLAN's are used to separate the broadcast/collision domains on the network and to provide a logical separation by building, departments or function on the network. For example, VoIP traffic (phones, gateways) is separated in a VLAN. All switches connect via trunked links in order to pass multiple VLAN traffic. All switches have the Simple Network Management Protocol (SNMP) turned on that allows the HP Procurve Manager to poll devices and extract relevant operational information. It can also be used to configure devices from one central platform. The following are a few suggestions:

- HP Procurve Manager does not seem to keep historical records on network performance. This information is useful to create baselines, understand traffic patterns and provide input for future growth needs.
  Severity Level = Suggested
- E-mail alerts should be configured so key IT staff is alerted if there is a problem on the network. This should assist in resolving problems in a more timely fashion and avoid unnecessary disruption of services.
  Severity Level = Moderated
- SNMP traps should be configured and collected by a syslog server to capture errors generated by network devices. This provides insight on issues occurring on the network and is a great resource for troubleshooting network problems.
  Severity level = Moderate
- A solution to complement the features of HP Procurve Manager and address the recommendations above is suggested. Two popular products on the market are WhatsUpGold or Orion from Solarwinds.
  Severity Level = Suggested

Status: *We have begun using HP Procurve Manager to maintain IOS images and to upgrade switches and routers. In addition, we using Orion from Solarwinds to manage the health of the network.*

Wireless Networking

IVC recently implemented a wireless solution from Extricom during the network refresh project. This solution consists of a controller per wiring closet where Access Points connect. There is a centralized management console to control all aspects of the wireless network to include SSID, encryption, VLANS, etc.

Available wireless networks are broadcasted and include encryption to secure traffic. Access control for wireless users is applied on the HP switches at the VLAN level. An open wireless network is available for

the public to connect with limited access to the internal campus but does provide Internet connectivity. The following are recommendations to take into consideration:

- IVC should explore the possibility of replacing the existing wireless solution. The Extricom solution does not scale well and staff has indicated that support for the product is lacking.
  Severity Level = Moderate
- IVC should move away from applying access lists on the internal switches to protect internal network resources from unauthorized users that are latched to the wireless network. One approach is to use the wireless controller to provide this level of security; a second approach would be to move the entire wireless network to the outside of the firewall and use it to apply access rules to inside resources.
  Severity Level = Moderate
- IVC should consider end-user authentication mechanisms to control users that are authorized to access the wireless network. If possible, authentication should be done against Active Directory via LDAP connectors.
  Severity Level = Critical

Status: *We have replaced the entire wireless infrastructure and extended the wireless reach to cover the entire campus with an AeroHive wireless solution. AeroHive is a "cloud" based controller solution. User authentication will be provided by integrating with our Radius server. Additionally, the solution manages security at the edge allowing for the removal of the access lists on internal switches.*

Cable plant

IVC recently modernized their data-cabling infrastructure and has a very solid, well design infrastructure that should last for many years. All cables are well organized, and are routed and identified inside proper enclosures. The only recommendation is to develop good documentation of cable paths, distribution facilities and manhole locations.

Status: *Even though the cable plant was found to be 'very solid,' we are working closely with Sanders Engineering and Neilson Construction to provide redundant connection between buildings and to make sure all on-going and future construction projects provide for the future growth of the Cable Plant.*

Server/Desktop Security

End-user passwords

End-user accounts and passwords are created and assigned by the technology department. This practice is very common for IT shops, although it does not scale well and has a potential for a security breach. Some end-users are aware that they have the capabilities to change their own password, while many others call the IT staff to have their password changed. IVC may want to follow these recommendations:

- Create policies and procedures around the use and maintenance of passwords. They should outline clear expectations around the use of passwords, change mechanisms, length and strength, resetting, age, etc.
  Severity level = Moderate

- End-user should be given a generic (but secure) password when the account is created and force them to change the password the first time they log in.
  Severity Level = Suggested
- Tech staff should use their own account to access staff computers for troubleshooting and maintenance.
  Severity level = Moderate
- Provide users with clear instructions on how to change passwords. The IT staff should promote good security practices to end-users and encourage them to change their passwords frequently.
  Severity level = Suggested
- IVC may adopt a policy to have passwords change every certain period. For example, users are forced to change passwords once a year.
  Severity level = Suggested
- Enforce password policies via Active Directory Group Policies.
  Severity level = Suggested
- IVC should determine the appropriate level of staff authorized to change user passwords.
  Severity level = Moderate

Status: *Security is always of the highest priority. We have begun drafting the policies and procedures to help drive these decisions. These changes will require significant man hours to implement. We are working on ways to implement these changes and still meet the needs of the campus.*

Remote Access to Servers

Severity Level = Critical

Most if not all the Windows servers in the IVC campus are accessible via the Microsoft's Remote Desktop protocol (RDP). This easy-to-use tool allows IT staff to access the server console to perform administrative tasks. Because the servers are located on the same internal network as faculty and staff, extra security measures need to be taken so that servers are not exposed to unauthorized access. In reviewing the Active Directory Users and Groups, it does appear that IVC has created a special security group that is used to control RDP access to the servers. IT staff need to ensure each server is configured so that only authorized access to servers occurs via RDP. This same philosophy should apply to the local server security roles; only the authorized groups should have administrative privileges over the server to minimize the potential of a security breach.

Status: *We recognize the critical nature of user access to servers and other computers. As such, we have been restructuring Active Directory with the intent to have better control over who has access to what resources on the network. We are beginning to implement security groups with specialized roles on the network, which will allow the technicians to complete the work that is necessary, but still restrict access to areas that require it.*

Centralized anti-virus solution

IVC uses the Sophos anti-virus solution to protect desktop and server computers. A handful of old servers continue to run the Symantec product, which appears to be the prior version of anti-virus software being used. During the discovery process, for the most part all servers and workstations had the Sophos agent installed and signature files up-to-date.

- IT staff should provide administrations with periodic reports from the anti-virus management platform. Examples of such reports are: (Severity Level = Suggested)

  - Compliance reports (protected systems, signature files)
  - Threats that have been mitigated
  - Top tens
  - Attack vectors (Trojans, e-mail, phishing, key loggers, etc.)
- Signature files should be updated regularly throughout the day and should balance between resources available and the acceptable risk. The larger the number of systems, the more network traffic and resources are needed to keep all systems with current signature files.
  Severity level = Moderate
- IVC should also build capacity to deploy an anti-virus solution that covers other operating systems other than Windows. A good example is the web server that runs a Linux operating system.
  Severity level = Suggested

Status: *We are currently using Microsoft Endpoint Protection with enterprise management. This allows the signature files to be updated on a scheduled time frame. We agree with the need to expand our virus coverage to operating systems other than Windows and will be working on that as time permits.*

Patch Management

IVC owns the KACE KBOX appliance that allows for the management of desktop lifecycle. This multi-function appliance provides technical staff with tools to effectively manage desktops and perform several tasks such as:

- Perform and maintain computer inventory (hardware and software)
- Software distribution
- Remote support tools
- Schedule and deploy security patches, system updates or new releases
- Ticket management
- Power management

During interviews with staff, it does not appear that IVC has embraced the tool to its full potential. Desktop and server patching is an ad-hoc approach and not very effective. The following could assist in the process:

- Assess the current functions the KBOX is currently doing and develop a plan to allow the appliance to bring additional efficiencies.
  Severity level = Moderate
- Develop a deployment strategy to include key staff and a realistic time frame for full implementation. The plan should progressively implement features of the KBOX appliance until they satisfy the needs of IVC.
  Severity Level = Moderate
- Provide adequate training for technical staff on the use of the appliance. Severity Level = Moderate

Status: *We have moved to Microsoft System Center. System Center is a "life-cycle" approach to computer management. It is designed to manage computers from the installation of the image to patch management and updating, to reporting on computer status, to end of life decision making.*

Back-end Services

Active Directory

IVC runs Microsoft Active Directory (AD) to run directory services for the campus. Two Windows 2008 servers are running AD in a clustered environment and replication seems to be working well. Internal DNS is currently integrated into the AD infrastructure although some issues were found with internal DNS replication. Both AD servers are running as Global Catalog servers (GC), which is a desired environment to provide resiliency. The following key recommendations need to be followed to correct existing issues and avoid potential problems in the future:

- Raise the AD Forest/Domain functional level to Windows 2008. It's currently running at Windows 2003 functional level.
  Severity Level = Moderate
- Have the operations master server (IVC1) synchronize its clock with a reliable NTP server. Since all client computers synchronize their time to this server, it is critical that this server's clock is as accurate as possible. Currently it shows a difference of approximately 2 minutes. The following link provides instructions on how to do this: (Severity Level = Critical)
  http://support.microsoft.com/kb/816042

Status: *Active Directory is the core component to any Microsoft domain and as such extremely important. We recognize the importance of raising the AD Domain functional level and synchronizing its clock with a reliable NTP source. Both the raising of the domain functional level and the NTP source and synchronization have been completed.*

Active Directory Administration

Severity Level = Critical

Recommendations redacted due to security concerns.

- Accessing servers via the console or remotely.
- Adding computers to the domain.
- Manage user accounts and groups.
- Server patching or updating.
- Manage network services such as DHCP and DNS.

Recommendations redacted due to security concerns.

Similar to the DA account, Active Directory contains Domain Administrators Group (DAG). This group shares the same administrative privileges to the DA account. Only high-level managers that require unrestricted access to manage the directory should be part of this group. The college should strongly consider the following suggestions:

- Change the DA account password as soon as possible. This account credentials should only be held by key personnel at IVC. This password should be changed on a regular basis (every year at minimum).
- *Recommendations redacted due to security concerns.*
- Review the members of the DAG group and remove anyone that doesn't have a need to manage the directory services. Special consideration should be given to consultants and ex-employees.
- It appears the college has created an IVC Admins group and is encouraged to implement and use such group to manage servers and day-to-day operations of the enterprise infrastructure. This group could have local administrative privileges on servers, allowing members full administration using their domain account.

- Implement delegation at the Organization Unit in AD. This allows a technician or employee to have certain administrative access over certain portions of Active Directory structure. This minimizes exposure to the enterprise infrastructure and provides the flexibility of having multiple staff managing the directory services in their respective political domain.

Status: *The DA account password has been changed to a random 64 bit password which is stored in a secure environment. The DAG group was reviewed and only those with a specific need remain part of the group*

DHCP Server

Severity Level = Moderate

IVC uses a Windows 2003 server to provide dynamic IP addresses to client computers. IVC should consider the following recommendations:

- Add the DHCP server to the domain. The server is currently a standalone server.
- Ensure scavenging is turned on. This feature will allow the DHCP database to purge old records, maintain consistency and avoid IP conflicts.
- The server uses the Domain Administrator (DA) account to be an authorized server for the imperial.edu domain. This should be corrected before the DA password is changed.

Status: *The DHCP server has been added to the domain and all other recommendations have been completed.*

Domain Name Services (DNS)

DNS services are critical for the proper operation of directory services and client access to resources, both internally and to the Internet. IVC currently has two DNS servers to respond to client requests. There are a couple of corrections that should be made for optimal functionality:

- Correct DNS replication problems between IVC1 and IVC2 for the imperial.edu forward lookup zone and all reverse lookup zones. Currently both servers are not synchronized with internal DNS records since the zones are not configured to transfer and notify their peer server when changes occur.
  Severity level = Critical
- Turn on the scavenging feature on the IVC1 internal DNS server. This feature allows the DNS server to purge old entries in the DNS table. In reviewing the table, some records have a time stamp of approximately a year ago or longer.
  Severity level = Moderate
- Ensure that all IP subnets (VLANs) have a reverse lookup zone in DNS. There were approximately 5 reverse lookup zones, which does not match the VLAN's currently documented.
  Severity level = Moderate

Status: *The replication problems between IVC1 and it903s-dc1 (IVC2 failed and was replaced) have been corrected. Additionally, the other issues have also been completed.*

Public DNS

Severity level = Moderate

IVC currently runs two public facing DNS servers that host the imperial.edu domain. This is standard industry practice and seems to work well for IVC. The servers sit on the public network with no firewall protection. It is recommended that IVC explore more cost effective solutions for hosting public DNS. One possible option is to host the zone files with the domain registrar or with the Imperial Valley Telecommunications Authority (IVTA). IVC should analyze the pros and cons to this approach.

Another possible approach is to convert the server over to a virtual server environment, which would allow the college to have local DNS control without having dedicated equipment for this purpose.

Status: *Through an agreement with IVTA (Imperial County Office of Education) the Public DNS has been moved to their public DNS servers.*

Files Services (NAS)

IVC has a dedicated file server that allows users to share and store files in a centralized location. One Windows 2008 server with ample storage (6 Terabytes) provides Windows files shares to IVC departments and users.

Status: *The file server has been moved into the SAN environment. It is being monitored and maintained on a regular basis.*

Printer Services

Severity level = Moderate

IVC currently runs a centralized print server where all printers are connected. Users then connect to this server and choose the appropriate printer on the network to use. The servers currently running this operation are 6 to 7 years old. IVC should consider replacing or virtualize the server to avoid potential downtime for all users.

Status: *Paper cut has been in place for almost two years. It manages and reports on all printing on campus. The print server has been moved into the new virtual environment.*

Data Backups

Severity level = Critical

IVC currently uses Backup Exec as their platform to perform data backups jobs. The IVCBK1 server is running Windows 2003 with the Symantec Backup Exec version 12.5. This enterprise platform does appear to have a Microsoft Exchange plug-in that allows the system to backup the message store while online. Another server named VM2 is used as a file server to store backups for the Banner system.

- Backup files are being stored in external storage attached to the backup server.
- There are four different backup jobs:

- Data and Infrastructure – Daily
  - Type: Incremental
  - Servers included: IVC2 and Fileserver
  - Retention Policy: None
- Data and Infrastructure – Weekly
  - Type: Full
  - Servers included: IVC2 and Fileserver
  - Retention Policy: None
- Daily Exchange - Daily
  - Type: Full
  - Servers included: Email.imperial.edu
  - Components: First and Second Storage Group
  - Retention Policy: None
- Quarterly Archive Data and Infrastructure
  - Type: Full
  - Servers included: IVC2 and Fileserver
  - Retention Policy: None

Backup Recommendations

- Backup jobs only include 3 of possibly 20 or more production servers in the environment. Exchange, User files and one domain controller (IVC2) are the only servers that are currently backed up. All critical servers need to have the Backup Exec agent installed and configured.
  Severity level = Critical
- The external storage on the IVCBK1 is currently out of space. This may prevent other backup jobs to complete successfully. Old backup files should be purged to make space for more recent backups.
  Severity level = Critical
- Retention policies should be configured in the backup system so it can automatically discard old backup files and eliminate the manual work.
  Severity level = Moderate
- IVC should explore a backup solution that can support multiple operating systems and use technologies such as de-duplication.
  Severity level = Moderate
- IVC should implement an off-site backup strategy to transport critical information outside the campus environment if possible.
  Severity level = Moderate
- The backup server appeared to have external USB drives connected for additional storage capacity. USB interfaces may not be adequate for fast data transfers or as reliable as SCSI or SAS interfaces. IVC may want to consider upgrading these storage devices.
  Severity level = Suggested

Status: *The backup system has been replaced with Microsoft System Center Data Protection Manager (SCDPM). SCDPM is backing up all Windows based servers with the data stored on its' own SAN environment. This will allow for data growth. The non-Windows machines are TARing their files and moving the data to a windows machine, which is being backed up. Additionally, the backup system was moved into another building in case something happens to the data room. This provides for separation of data in case of an emergency. In addition to this, all crucial Banner data is being stored off-site in case of disaster.*

E-mail System

IVC currently hosts Microsoft Exchange server as their electronic messaging and collaboration platform. Exchange 2007 currently serves approximately 500 mailboxes for staff and faculty that are primarily accessed via the Microsoft Outlook client.

End-users may also access the Exchange system via the Outlook Web Access (OWA) web interface, which allows users to check e-mail with a standard web browser. This also provides the framework for users to access their e-mail through mobile devices via Active Sync.

IVC uses the Barracuda Spam Firewall appliance to filter inbound and outbound mail for spam and viruses. End-users have the option to customize their filter settings to accommodate specific needs outside the general configuration settings of the filter.

System Configuration

The Microsoft Exchange 2007 server currently has all 4 roles installed within one server (Hub, Transport, Client, Mailbox). This setup is common and adequate for an organization the size of IVC. Exchange services run on a Dell PowerEdge 2950 running Windows 2003 server with 8 GB of RAM and 6 x 146 GB (15K) hard drives. The server was installed in 2007 and has 4-hour on-site premium warranty that expires in May of 2012.

Mailbox Storage Limits

Severity Level= Critical

IVC currently has no per-mailbox storage limitations configured in the system defaults settings. Space on the hard drive is currently at two-thirds capacity and IVC runs the risk of filling the hard drive space very quickly. IVC should do an assessment of space per mailbox and perform capacity planning to avoid running out of disk space.
The following command can be used in the Exchange Management Shell to provide a list of mailboxes sorted by size. Unfortunately, Exchange 2007 does not provide this feature via the GUI:

Get-MailboxStatistics | Sort-Object TotalItemSize -Descending | ft DisplayName,@{label="TotalItemSize(KB)";expression={$_.TotalItemSize.Value.ToKB()}},ItemCount

The first storage group where all the mailboxes reside is currently close to 200GB and most mailboxes are at approximately 1.5 GB of space, with a few well above 3 GB. One approach is to set a common storage limit for all mailboxes or set different tiers of storage limits and set criteria for how users would qualify for the different tiers.

Status: *The mail system has been upgraded to Exchange 2010 and is currently running on 4 separate virtual servers. We are in the process of moving mail services to the Office 365 cloud. This will allow for email access at all times. Storage limits are set by Microsoft at 50 Gigs.*

Hardware Redundancy

Severity level = Moderate

Exchange is running on a single server with redundant power supplies and multiple hard drives in a RAID configuration. The server is protected from the most common failures (power and hard drives) but IVC should consider strengthening other single point of failures on the server. Technologies such as virtualization or clustering should be considered to minimize communication downtime.

Status: *The Exchange server has been virtualized and moved into the new SAN and Server environment.*

E-mail System Recommendations

IVC should consider the following recommendations:

- Disable the Post Office Protocol v3 (POP3) on the Exchange server. This is an old protocol used to retrieve messages from the server via a POP3 client such as Outlook Express or others.
  Severity level = Suggested
- There is a large amount of distribution groups that should be reviewed for accuracy.
  Severity level = Suggested
- Set attachment size limits (10 – 20 Mbytes) to prevent large files entering the mail system. Transfer of large files should use a different mechanism of transport.
  Severity level = Suggested

Status: *All suggestions have been implemented as part of the virtualization, upgrade and move of the Exchange server.*

Spam and Viruses Protection

IVC uses the Barracuda Spam Firewall product line to scan inbound and outbound e-mail traffic using a physical appliance for each direction. A summary of the products:

Inbound Mail	Outbound Mail
Model: Barracuda 400 Hostname: spamcheck.imperial.edu IP address: 10.1.1.200 Firmware version: 3.5.12.012	Model: Barracuda 300 Hostname: oldspam.imperial.edu IP address: 10.1.1.201 Firmware version 3.5.12.025

The Barracuda product line has demonstrated over time to be very resilient and very good at blocking unwanted messages into the messaging infrastructure. After reviewing the configuration on the appliances, it is recommended the college do the following:

- Upgrade the firmware on both spam firewall appliances. The latest firmware update will consist on a major upgrade to Version 4.x which provides a new streamlined interface, new features and bug fixes.
  Severity level = Moderate
- Create a new DNS record for the outbound mail instead of oldspam.imperial.edu.
  Severity level = Moderate

- Configure the appliance for LDAP/Exchange user integration. This feature provides two important features (Severity level = Moderate):
    - Integrates users on the spam firewall with the Active Directory account. This way, users can login to the spam firewall (customize spam settings, review quarantine) with their e-mail address and domain password.
    - It provides a mechanism for the spam firewall to check the recipient list before accepting e-mail for a valid e-mail address. Without this feature, the spam firewall has no way to know if the recipients are valid and creates a quarantine account for invalid users as well. When reviewing the user list on the spam firewall, it currently has about 3,443 user quarantine accounts, when most likely only 500 of those accounts are valid. This creates unnecessary overhead and puts additional load on the appliances.
- Create an SPF record in DNS to identify authorized mail servers for the imperial.edu domain. This optional verification process is being adopted worldwide as a mechanism to identify trusted servers and help minimize e-mail spam.
  Severity level = Moderate
- If economically possible, purchase another Barracuda Spam firewall appliance (model 400) to cluster with the current appliance and provide hardware redundancy.
  Severity level = Moderate
- Internal and external hostnames in the DNS tables do not match. This hostname should match according to the configuration of the appliance.
  Severity level = Critical

Status: *After much consideration, it was determined to take advantage of the Spam and Virus services being offered by Imperial County Office of Education. They currently have in place redundant Barracuda filters with all of the recommendations already in place.*

Blackberry Enterprise Server

Severity Level = Suggested

IVC runs the Blackberry Enterprise Server (BES) to support Blackberry device synchronization with Exchange server. There are currently 10 users on the BES server and a few of these users have been inactive for several months. It is recommended that the college revisit their strategy for supporting mobile devices such as Blackberry phones. An alternative solution is using Exchange's Active Sync to synchronize with mobile devices.

Status: *The Blackberry Enterprise Server (BES) is no longer in production. All users have switched to other services that don't require the BES server.*

Other Recommendations

Server Maintenance

Severity Level = Moderate

In general, all servers are in need of software and/or hardware maintenance. A couple of servers have warning lights indicating some type of hardware failure. During the discovery process, most if not all servers required system updates to correct security flaws or provide new features. It is recommended that a routine maintenance schedule be established for the servers. This schedule should keep in mind that servers will need to be rebooted from time to time and that it may impact end-users. It's not uncommon to schedule these maintenances windows outside regular business hours.

Status: *General maintenance on the servers has been implemented. Any servers with warning lights have been diagnosed and corrected and updates have begun to be installed. We still have room for improvement with regards to patches and updates, but we are working on a plan as we move forward into our new virtual environment.*

Server Virtualization

Severity Level = Moderate

IVC should continue its server consolidation effort through the use of virtualization technology. Given the diverse environment, it is important to choose a platform that supports different guest operating systems such as Linux and Windows. A platform such as Xen or VMWare would allow IVC to consolidate many of their servers into three or four physical servers with a common storage system.

This platform should also provide more options for IVC to strengthen it's disaster recovery initiative and simplify processes to ensure data is protected and secure.

Status: *We have virtualized most if not all physical servers that are a candidate to be moved. We are in the process of updating the cluster to Windows 2012 R2 Data Center.*

Facilities

Severity Level = Suggested

IVC should re-evaluate technology systems that relate to the control/inspection of facility systems such as HVAC, surveillance and access control. From reviewing the firewall configurations and interviewing staff, it appears several disparate systems (and possibly duplicated systems) exist to control such facilities with minimal involvement of the IT staff. There should be a broader strategy in place that includes the technology staff in the planning and installation of such systems. These systems should be scalable and use the IP network as much as possible.

Status: *We recognize the need to consolidate control/inspection facilities and are making every effort to do so through the on-going modernization of the campus. As buildings and/or facilities are modernized, we are working with the necessary parties to bring them onto the network.*

Content Filtering

Severity Level = Moderate

IVC currently redirects all external DNS requests to the OpenDNS servers. This free service is effective to block access to inappropriate sites but does not really provide visibility on what types of traffic are flowing through the network. Because IVC operates in a higher education environment, inappropriate use of network resources, such as copyright infringements, are commonplace. IVC should explore the option of

installing a system that can provide better visibility to the types for traffic flowing through the network. This will provide the tools to understand traffic patterns, prioritize legitimate traffic, block unwanted protocols and will aid tremendously when investigating a potential violation.

Status: *We have moved to Sonic Wall edge security device. This new edge security appliance provides a greater level of visibility of traffic. We have installed redundant SonicWall security appliances. These appliances will allow us to have better control over the network traffic and allow us to limit and/or block inappropriate traffic.*

Next Steps

This document can serve as a guide to administration on the next logical steps to enhance security and improve uptime and reliability. The perimeter network should be the first area of focus and ensure only necessary network traffic is allowed. The second area of focus should be on the need to improve the enterprise infrastructure such as servers, data backups, storage systems, Active Directory and other back-end systems. The third area of focus should be to strengthen internal security and access to critical systems such as the financial and student system.