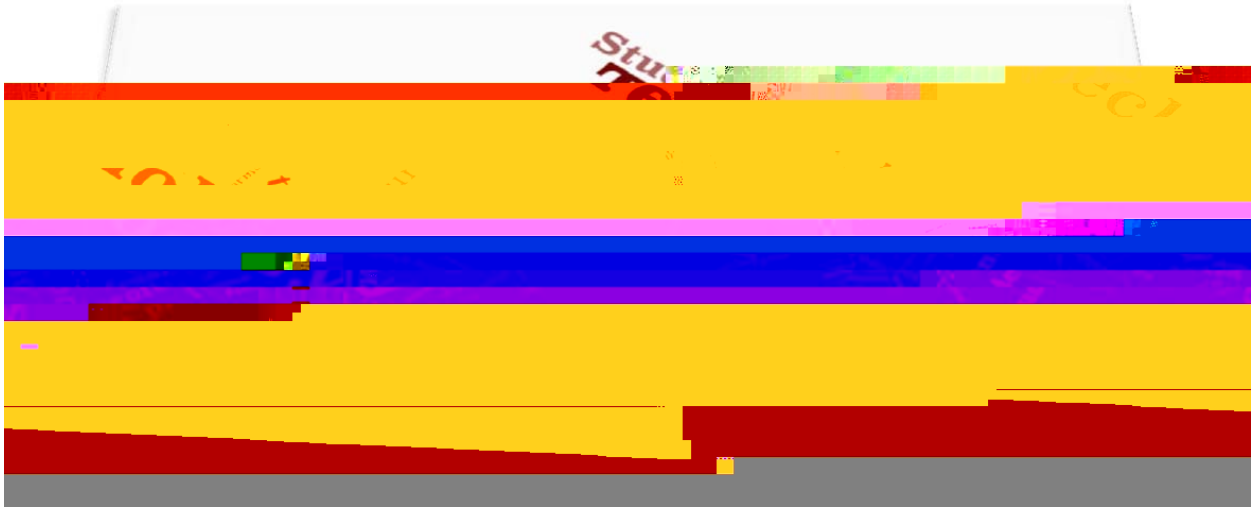
Imperial Community College District

Strategic Technology Plan 2017-2022



Committee Ap proved: 2 F W R E H U , 201

Table of Contents

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

Initiative One:

Initiative Four:
User-centered Support Structures

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

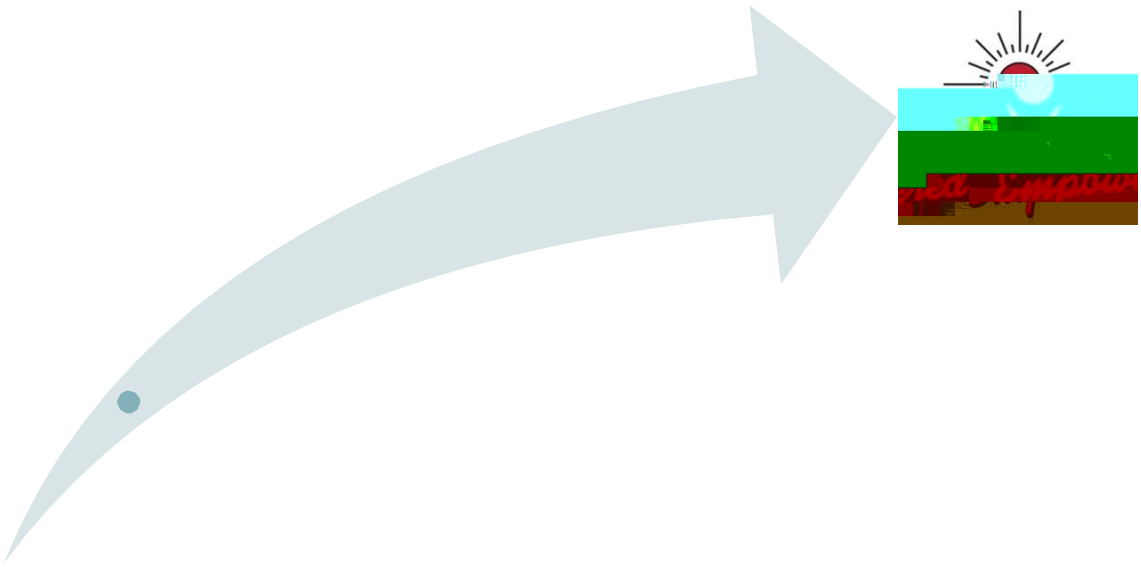
Principles in Support of Initiative Four
1. Just-in-time support
2. Best of breed web support and documentation
3. Diverse learning options
4. Actively promote use of communities

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)

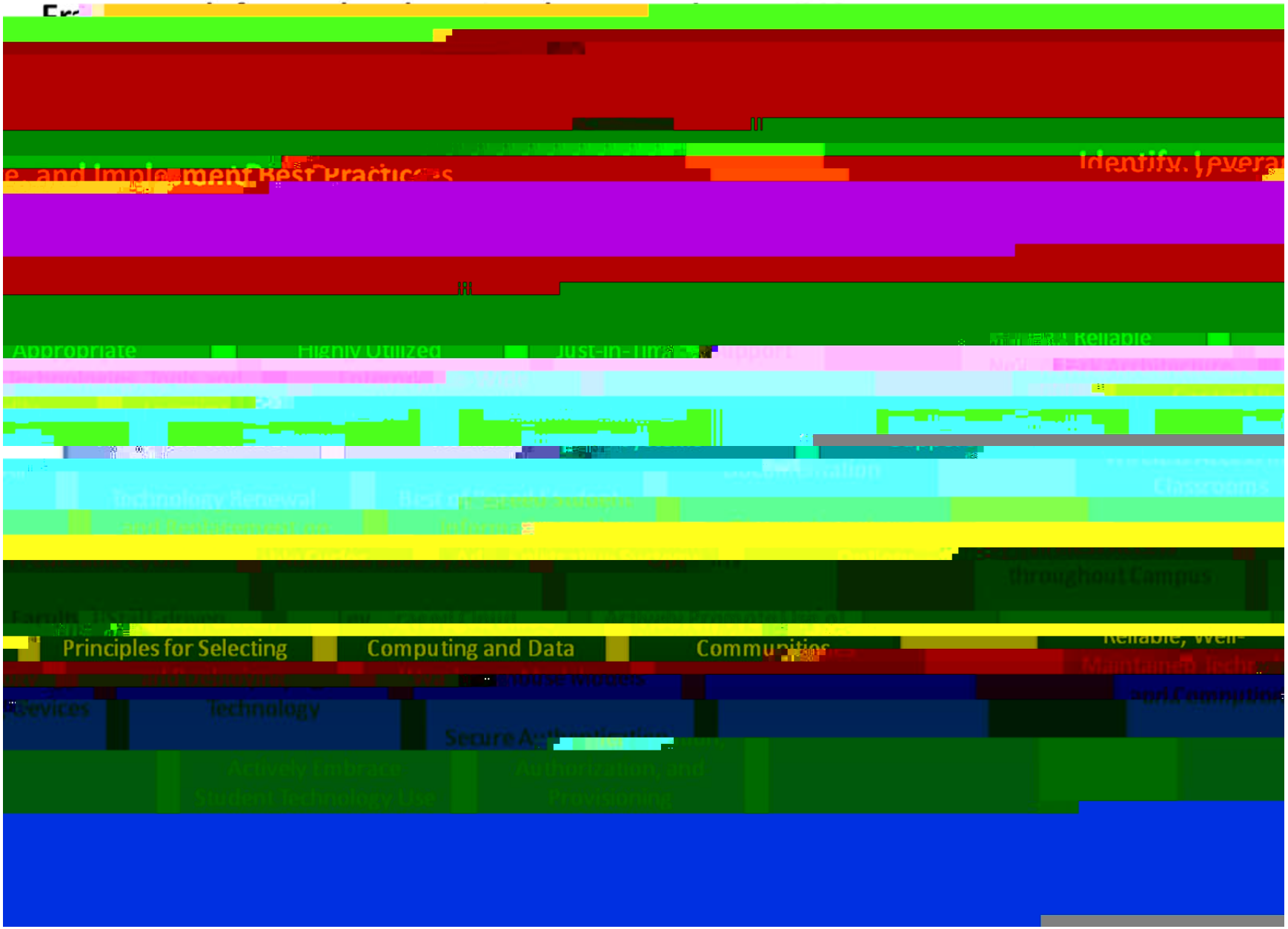


Strategic Technology Plan - 2017 Activities

The following activities are outlined for Fiscal year 2017/2018.

1. Move Banner backend servers from SPARC to new HP blade/VM Ware

Appendix A



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				

	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 technolo		

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
2.12 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.
2.13 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	

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			

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	

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.

Appendix C – Network Security Assessment

IVC us es 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 Extr icom wireless solution to provide access to mobi le 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 facult y 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)

Mod el: 5550

Software Version: 7.2(2)

Firewall configuration

Severity level = Critical

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

Recom mendations 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 recom mendations 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 curre ntly runs a single Cisc o ASA 5550 firewall ap pliance. IVC should consider installing a second firewa ll for redundancy purpose s. The firewalls can be installed in an active-standby configuration to provide hard ware fault tolerance should on e of the appliance s fail. IV C should also ensure that this critical link in th e network has premium sup port from th e 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 Micr osoft RAS/VPN se rvices in Windows 2003 server. T his provides remote access to network resources via an e ncrypted connectio n through this se rver. The server curre ntly has two ne twork interface s,

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 consid er moving ser ver farm s into a Demilitarized Zone (DMZ) connecte d to the firewall . *Recommendations redacted due to security concerns.*

The firewall is a dedicated appliance for this purpose and would centraliz ed network security in on e device. Moving servers into a DMZ has many im plications and this process woul d 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 Le vel = Mo derate

The Calexico r emote campus connects to the main campus via a T-1 lin e (1.54 Mbps). The capacity on this telecommunicatio ns circuit is not adeq uate for toda y's business requirements and it co nnects to ver y old equipment that is subject to failur e soon. It is recommende d that IVC explor e other alternatives to connect the site wi th refreshed equipment that can provid e more adequate bandwidth.

A tho rough 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 Monitoring

IVC currently uses the Hewlett Packard (HP) Procurve Manager software to manage their network switch infrastructure. The software has access to all networ k 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 ar e 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, underst and 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
  Se ve ri tylSe v(l)-1052( )-6(=)-6.9(Ml)-10.4c
  es(e)3.9(s.)334(dT()926twelnpl)edWtp r-1.6 Ortioa (r)7.6
  oes.

the public to connect with limited access to the internal campus but does provide Internet connectivity. The

- 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

- Compliance reports (protected systems, signature files)
- Threats that have been mitigated
- Top tens
- Attack vectors (Trojans, e-mail, phishing, key loggers, etc.)

-

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.
-

-

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

- 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 ba ckup 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 tr ansfers 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 curre ntly hosts Microsoft Exchange server as th eir electronic m essaging and collaboration platform. Exchange 2007 curren tly serves approximately 50 0 mailboxes for staff a nd f aculty t hat a re p rimarily accessed via the Microsoft Outlook client.

End-users may also access t he Exchange system v ia the Outlook We b Access (OWA) web interface, w hich allows users to check e-mail with a standard web browser. T his also provid es the framework for users to access their e-mail through mob ile devices via Active Sync.

IVC use s the Barracu da Spam Fire wall appliance to filter inbound and outbound mail fo r spam and viruses. End-users have the option to customize the

Exchange is running on a single se rver 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

- 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 feat ure, 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
-