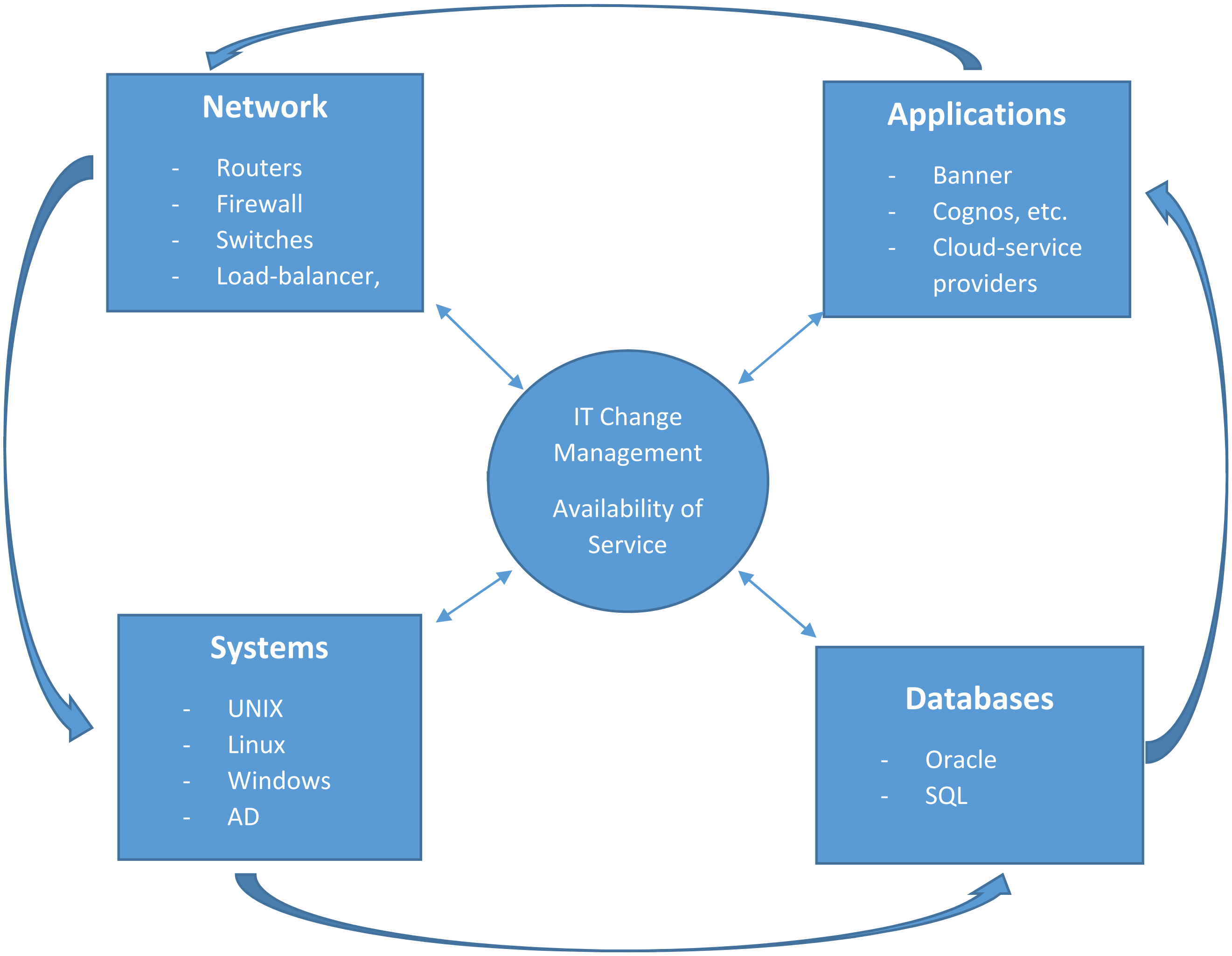
NMSU – Office of the Chief Information Officer

IT Change Management – Depiction of Infrastructure of Core Technologies



Network

- Routers
- Firewall
- Switches
- Load-balancer,

Applications

- Banner
- Cognos, etc.
- Cloud-service providers

IT Change Management

Availability of Service

Systems

- UNIX
- Linux
- Windows
- AD

Databases

- Oracle
- SQL

IT Change Management Philosophy

The above portrays visually the connectivity and interdependencies of core systems in delivering core services to the NMSU community such as the availability of Canvas NMSU's Learning Management System (LMS), Banner NMSU's enterprise resource planning (ERP) system, Cognos NMSU's enterprise reporting system, etc. These core systems depend on enterprise infrastructure such as databases, operating systems and network in order to be available to the NMSU community. These core systems should also be secure as they process, contain and transport NMSU's valuable data.

Because of the existing dependencies, any changes to any of the core systems must be reviewed and approved prior to its deployment as these changes could cause unavailability of service or risk exposures to data, which could severely affect the core operations of NMSU.

However, no changes will be deployed during the below critical operational periods of NMSU unless formally approved by the CISO, CIO, Sr. VP of Admin and Finance, Provost and President:

- Registration
- End of semesters – Grading Periods
- Year-end, etc.

The following describes how each major of the above areas handle/practice Change Management:

> Note: Each of the below Areas will develop Standard Operating Procedures (SOPs) that detail the processes that they follow in detail for business continuity purposes.

Network

The following change management process pertains to Telecom, Networking, Classroom Tech & AV Support and Technical Support center. All the changes will be tracked via Pinnacle work orders.

Year-round service maintenance.

-Based on

1) Vulnerability report

2) End of support of the software

3) Requested Features and other security requirements

4) Licensing change

-Schedule during maintenance windows

-Configuration changes and software updates on any equipment and service.

Bi-Annual evaluation and maintenance of core service equipment (update of core service equipment and software)

-Evaluate the hardware, the software and the configuration of the core service equipment.

-Perform necessary update based on the evaluation.

-Christmas break and Summer session.

-Systems affected:

1) Core network system: Internet routers, Core routers, Core switches, and firewalls.

3) Core telecom system: VoIP

2) Core Infrastructure services: VPN, Load balancer, Packet shaper, DNS/DHCP, Lab computers, Webcast

Annual Maintenance of core service equipment

-Perform mandatory purge on DHCP/DNS records.

-Mandatory software update on core infrastructure services equipment

-Based on evaluation software update on core network system and telecom system.

-Summer session.

Applications

To be incorporated in the near future

Systems

Three Operating Systems (and three ways of getting OS patches)

1. Windows

   - Use Microsoft's WSUS service and patch weekly. (Sunday mornings)

   - Have a local WSUS server that gets then provides patches to the rest of Windows boxes.

2. Solaris

   - Do quarterly patches by downloading the latest Solaris patch set from Sun. Then, patch manually from the patch set. (In an emergency, will also apply a particular patch when needed)

3. Linux

   - All production boxes run RedHat, and have maintenance agreements and subscribe to/use the RedHat Network to provide patches through a tool called "yum". These boxes are also manually patched quarterly. (Like the Solaris machines, there are occasional emergency patches applied as well)

Databases

Process for Oracle Patch Set Updates (PSU's) that include Critical Patch Updates (CPU's) that include known security vulnerability fixes:

Oracle Patch Set Updates (PSUs) that include Critical Patch Updates (CPUs, security).

1. Receive notice from database vendor of availability of PSUs.
2. Review the notice and documentation for database products and versions installed onsite.
3. Evaluate the database product risk matrix documentation.
4. Identify any components in those risk matrixes that are installed whose Base Score CVSS is higher than 7.5.
5. For affected products and version whose software components exceed 7.5, provide a list to the Manager for review.
6. Manager schedules the PSU to be applied in dba test environment.
7. Apply the PSU in the dba test environment and document the process.

   a. If issues related to the PSU, contact the vendor for advice/resolution.

8. Because CPUs don't have tests procedures from the vendor, wait 2 weeks and identify issues that might be related.
9. If no issues, Manager schedules the PSU to be applied in pre-production user-test environment.

   a. If issues related to the PSU, contact the vendor for advice/resolution.

10. Because CPUs don't have tests procedures from the vendor, wait 2 weeks and identify issues that might be related.
11. If no issues, Manager schedules the PSU to be applied in production environment.
    a. If issues related to the PSU, contact the vendor for advice/resolution.

Processes for deploying Oracle Upgrades follows a similar process