Chapter 5: Leadership, Coordination, and Governance of IT

CU-Boulder’s IT environment is characterized by complex layers of central and distributed services, support, and leadership. This chapter includes recommendations for clarifying central and departmental roles in the provision of services and support, and for clarifying and increasing participation in IT leadership and governance.

To the end of increased reliability and stability of IT resources, recommendations in this chapter call for greater centralized authority for certain aspects of the campus’s IT environment (including security and cross-campus use of the Enterprise Directory). To the end of increased efficiency and decreased duplication of services, other recommendations call for greater centralized coordination in areas such as wireless deployments and e-payment solutions. Concurrent with the implementation of these recommendations, the campus needs to ensure the autonomy of departments and their ability to customize services to meet their specific needs. Continuing to develop a model of distributed desktop support is one way to achieve this.

This balance between cross-campus concerns and departmental autonomy is possible only in a culture that supports effective, broad collaboration and cooperation. To promote such a culture, recommendations call for broader and deeper input and increased participation, particularly by faculty, in strategic and tactical oversight of IT initiatives and management of the campus’s IT environment. Recommendations also call for increased communication, which is crucial to the development of a collaborative culture, and which also facilitates successful implementation of cross-campus IT initiatives and the continued provision of a comprehensive suite of IT resources.
5.1 Centralized Coordination and Management of IT

Recommendation: Specific aspects of IT on the CU-Boulder campus should be coordinated centrally to best achieve efficiency and to decrease duplication. These aspects include wireless deployment, a security infrastructure, and maintenance of DNS/DHCP servers. Other aspects of IT, such as the Enterprise Directory, server hardware registration, and software compliance, should be managed centrally to ensure that campus-wide standards are maintained for reliability and stability of the campus IT infrastructure. To achieve this, the campus should determine, prioritize, communicate, and enforce which areas need centralized coordination and which need to be managed centrally.

Discussion of the Recommendation

Current Situation
As in many higher education institutions, the computing and network resources at CU-Boulder have evolved into a complex, layered, and in some cases, duplicated IT environment. Several units on campus (such as Financial Aid, the University Memorial Center, Housing, JILA, LASP, CIRES, CLIPR, Computer Science, Physics, and Aerospace Engineering) maintain their own IT staff and services. Now, with increasing costs and concerns for security, the campus is clarifying what IT services need to be centrally coordinated, as well as what aspects of academic and campus computing need centralized oversight to maintain the reliability and stability of the campus IT infrastructure.

Rationale
While customization and autonomy of many aspects of IT in particular departments continues to be desirable, three forces are motivating a campus-wide discussion regarding coordination and/or centralization of a basic set of IT services: 1) the need for efficiency, given the current fiscal constraints; 2) the increasing interconnectedness between IT resources, which create potential vulnerabilities for the entire campus; and 3) the need for compliance in the areas of software licensing and library subscription services.

Due to increasing IT costs (and decreasing support from the State), a strong need exists to have efficient utilization of IT resources. For example, an opportunity for this exists with file storage systems. A wide variety of file storage systems are available on campus but their use is often constrained by available capacity, financial limitations, and technical proficiency. Faculty, students and staff are increasingly mobile, requiring tools to easily move files from a local desktop or lab systems to central servers. A centralized, campus-wide solution would provide a needed file sharing service to faculty, students, and staff.

Another opportunity exists with credit card payments, which are widely accepted on campus as a means of payment. Formal policies, guidelines, and/or best practices are not established, widely disseminated, and/or not routinely followed. Coordinating this initiative would provide stability and consistency across campus.

Increasingly, any IT resource on campus has the potential to negatively impact a wide variety of other IT resources on- and off-campus; therefore security is another salient area on campus potentially needing increased coordination and centralization. Because an increased reliance on IT as part of the university’s business and academic communications infrastructure continues to
grow, a security infrastructure should be developed to ensure the integrity and stability of the IT infrastructure.

A final area where increasing coordination and centralization might be needed is with software compliance. External vendors are demanding that higher education institutions better track their computing and software licenses. As external vendors continue to develop better tools to track their licenses, the CU-Boulder campus will need to respond with increasing vigilance over their software agreements and licenses.

Specific Recommendations Include
Authority for the following areas should be centralized or be centrally coordinated. The items are categorized into three areas: efficient utilization of resources, security, and compliance.

**Efficient Utilization of Resources**

**What should be centralized:**

1. **Continued development of the Enterprise Directory**
   
   The Enterprise Directory is a general-purpose service, usable by a variety of campus constituencies; however, for it to be a trusted, reliable source of information, a single unit on campus must have ownership and responsibility of it. The primary advantage of the Enterprise Directory is to tie together independent applications (such as SIS, HR, PeopleSoft) and enable relationships as well as resolve discrepancies between these applications. Other advantages include the ability to enable campus-wide calendaring, authentication & authorization, identity management, access management, and account management. To manage privileges granted to individuals, the campus computer and network infrastructure needs to identify who individuals are when they login (identity management), verify that individuals are who they say they are (authentication), and grant individuals access to the privileges they need (access management/authorization). See section 3.2, Enterprise Directory Services.

2. **Centralized server (hardware) registration.** Currently there is no centralized server registration on campus. Centrally coordinating server hardware registration is necessary to maintain and track what services specific servers are providing. This is an important step in developing a campus-wide network security plan. Also, the server hardware registration ties an identity to a specific hardware address, which enables troubleshooting relating to continued operations and security.

3. **Networking Services.** Voice and Backbone networking services must continue to be centralized to ensure economies of scale and manageability. These critical campus services are most efficiently provided centrally, by ITS.

**What should be coordinated:**

4. **Wireless deployment.** In 2002, a IT policy was approved by IT Council to grant authority to ITS to coordinate and regulate wireless deployment on campus. Wireless access allows campus spaces including common areas, classrooms facilities, and labs to be “smart.” Coordination is critical because wireless networks are being installed at an ever-increasing rate. If this process isn’t managed, competing signals will degrade the overall performance of the wireless network, jeopardizing wireless signals for everyone. Recognition of ITS’s centralized authority to coordinate wireless would ensure stability and reliability of the campus wireless environment.

5. **Setting minimum standards for servers.** Currently this is not happening on campus. Providing and coordinating a minimum standard for all campus servers by ITS would ensure...
that all servers will have a certain amount of security built into them, and allows for more efficient central support management.

6. Coordination of Domain Name Servers (DNS) and Dynamic Host Configuring Protocol (DHCP). Currently this is not happening on campus. Centrally coordinating IP addresses would significantly decrease individual manual work done by local administration support; decrease duplication of IP addresses; and ensure a www.colorado.edu scalable mapping scheme. Providing centralized authority for DNS and DHCP would provide greater efficiency by freeing local administrators from this administrative task to provide more specialized local support.

7. Coordination of e-payments. While e-payments are an accepted means of payment on campus, formal policies, guidelines, and/or best practices do not uniformly exist. Coordination of e-payments would provide stability and consistency across campus.

8. Development and coordination of a campus-wide file storage system. Currently, this is not happening on campus. While a wide variety of departmentally owned file storage systems exist on campus, there is not a centralized, coordinated repository for electronic data. Faculty, students and staff are increasingly mobile, requiring tools to easily move files from a local desktop or lab systems to central servers. A centralized, campus-wide solution would provide a needed file sharing service to faculty, students, and staff.

Security

What should be centralized:

1. Develop and coordinate an IT communication infrastructure that responds to specific IT related issues. Currently an IT incident response system does not exist on campus. For example, if a computer virus or trojan worm successfully infiltrates the campus, a campus-wide plan on how to best communicate the problem and the anticipated resolution to the campus does not exist. An incident response system would give the campus a reliable conduit to communicate in the event of an emergency or in a situation that specifically and significantly jeopardizes the campus computer and networking infrastructure.

2. Mandate email filtering. Currently this is not uniformly happening on campus and poses a significant security risk. Email filtering prevents “worms” from infiltrating an email system, wiping out email, data, and spreading to other user’s computers. Similar to antivirus protection, email filtering is particularly important because of an increased proliferation of worms, which presents a higher risk to the campus.

What should be coordinated:

3. Maintain and provide antivirus protection. This is happening on campus in a varied and inconsistent way. Centrally coordinating antivirus protection on campus minimizes successful attacks on campus that could lead to loss of data and disruption of computing and network resources. Coordinating antivirus protection is important because of a large increase in number of viruses attacking the campus. Individual academic or research departments would be less likely to be protected against virus threats if no centralized coordination continues.
Compliance

What should be centralized:

1. Ensure compliance with software licensing. Currently ITS is only able to track software licenses within ITS. External vendors, such as Microsoft, are demanding that higher education institutions better track their computing and software licenses. These external vendors have better tools to track computing and software licenses than existed in the past. Negligence on the part of the campus could translate into litigation for the university. A centralized authority could provide effective oversight rather than relying on individual departments to track and manage their license agreements.

2. Compliance Review of campus-wide IT policies. The Office of the Associate Vice Chancellor for Academic and Campus Technology (AVCACT) was established in 1998 and has enforcement authority over IT policies. The AVCACT Office has implemented policies but historically has not played an authoritative role. Now, the complexity and the interdependence of the campus computing and network infrastructure increasingly ties together everyone on campus and necessitates compliance with accepted campus-wide IT policies, guidelines, and processes. In the near future, the AVCACT Office might need to play a more active role in the enforcement of campus-wide policies, practices, and standards that have been developed by campus-wide constituencies in order to maintain the security and reliability of CU-Boulder’s computing and network resources.

Steps

Implementation

- Research, develop, and implement tools and processes to allow for DNS, DHCP coordination; wireless registration; and minimum standards for servers (see specific recommendation in section 3.1, Wireless).
- Continue working on the Enterprise Directory and IT Service Provisioning Infrastructure and solidify the steering committee and governance infrastructure for the IT Service Provisioning Infrastructure (see specific recommendation in sections 3.2, Enterprise Directory and 3.3, IT Service Provisioning Infrastructure)
- Support security initiatives on campus to develop an antivirus protection solution and email filtering. Develop an incident response system to communicate to the campus in the event of an IT-related emergency (see specific recommendation in section 4.2, Security).
- Develop, communicate, and enforce a server (hardware) registration process as well as a campus-wide software licensing policy.
- Continue to develop appropriate campus-wide IT policies as needed. Explore strategies for communication, acceptance, and enforcement of such policies.

Communication

A comprehensive communication plan will be developed to outline the suggested changes and solicit campus-wide involvement.

Policy & Standards

- Development of campus-wide antivirus and email filtering policies.
- Outline standards for minimum server requirements.
- Develop standards for centralized server (hardware) registration.
- Develop a campus-wide policy for software licensing.
**Required Involvement**

**Governance & Authority**
ITS will have operational responsibility for these initiatives with oversight provided by The Office of Academic and Campus Technology.

**Required Departmental Involvement & Responsibilities**
- AVCACT for policy development and oversight.
- ITS for centralized operations support.

**Expected Costs**
No additional costs are expected from these recommendations, but rather significant campus coordination.

**Annual IT Infrastructure Investment**
See specific infrastructure investment sections in other areas of this report (e.g. Enterprise Services, ITSPI, Security, and Wireless.)

**Operating and Maintenance**
Not applicable.

**Personnel**
Not applicable.

**Funding**
See specific funding sections in other areas of this report (e.g. Enterprise Services, ITSPI, Security, and Wireless.)

**Timing**
Immediately – fall 2002.
5.2 Management, Leadership, and Advisory Structures for IT

Recommendation: The CU-Boulder campus should re-configure the existing IT leadership and advisory body (IT Council) to reflect the complexity of the campus’s IT environment, and the need for increased participation by and communication with a wide array of campus constituents. The campus also should assess the roles, responsibilities, overlap, and effectiveness of the wide range of other committees addressing IT issues. The roles and responsibilities of the Office of the Associate Vice Chancellor for Academic and Campus Technology with respect to campus IT management and leadership should be clarified and communicated to the entire campus.

Discussion of the Recommendation

Current Situation
The complexity of CU-Boulder’s IT environment is evident in the diversity and number of units and staff providing IT services and support across campus. That environment can be characterized as one that supports cross-campus collaboration on many IT issues, but also as one that needs improved coordination and communication. Successful collaboration by multiple units on campus-wide initiatives such as the Enterprise Directory, for example, stands in sharp contrast to instances in which multiple units provide similar or even duplicated services—such as educational technology support—with little communication among each other, and no coordinated communication to the constituents who use their services. It is an environment that increasingly needs effective, well-coordinated management, leadership, and advisory structures that are broadly representative, and engaged in providing both strategic and tactical direction for the entire campus. A description of the current structures follows.

- The Office of the Associate Vice Chancellor for Academic and Campus Technology (AVC ACT) oversees campus-wide IT initiatives—including both academic and administrative initiatives. Staff in this office work closely with ITS on policy development, planning, and communication, and also function as support staff for ATLAS (the Alliance for Teaching, Learning, and Society) and other academic IT initiatives.

- The Executive Director of ITS reports to the AVC ACT. Because it provides a broad array of services to the entire campus, ITS also implicitly and explicitly provides direction for IT on the CU-Boulder campus.

- CU-Boulder's IT Council, which is managed by the Office of the AVC of Academic and Campus Technology, comprises representatives from central units on campus, as well as faculty, student, and staff representatives. The Council meets roughly twice a month to fulfill its charge to:
  - provide strategic leadership, coordination and guidance concerning campus-wide IT initiatives and vision;
  - provide high-level management—policy, budgetary, and organizational—recommendations related to campus-wide IT issues; and to
  - provide communication and advocacy for IT initiatives.

- In addition to IT Council, the campus also has many other committees that address IT issues. Membership within and across these committees is varied in level; topics addressed by these committees are likewise a mix of strategic and tactical issues. In
addition to these more strategically-oriented groups (such as the Committee on Electronic Communication), there are committees focused on specific, ongoing issues (e.g., the ICWG [Instructional Computing Working Group], which oversees student computer fee funded labs), and ad hoc committees focused on short-term initiatives (such as Educational Technology Strategic Planning committees). There is some membership and some topic overlap between campus IT committees.

Overall Recommendation:

Based on feedback from campus focus groups, a survey of IT Council members, and discussions at IT Council, the campus should consider re-configuring its IT oversight structure to provide broader, and deeper input into decisions about the campus’s IT environment and its development, and about IT communication and policy enforcement issues. There is a need for greater faculty participation in strategic IT work, and, to the end of better communication and broader campus involvement, a need to have cross-representation on IT advisory and leadership structures with other existing groups on campus, such as the BFA, ASC (Arts and Sciences Council), UCSU, and UGGS. There needs to be a distinction between advisory and oversight bodies that provide strategic oversight and those that provide tactical oversight.

Based on feedback from campus focus groups, the Office of the AVCACT needs to continue to provide strategic direction of IT on campus and oversight of IT initiatives. It also should take on a coordinating function in the area of educational technology.

Specific Recommendations Include:

- Streamline the membership of IT Council, and supplement the Council with (FACE-IT: Faculty Advisory CommitteE for IT), administrative, and student IT advisory bodies. IT Council would retain faculty, student, and staff representation. Structure the four committees to include standing ex officio members who act as technical experts. Delineate between the strategic oversight of the IT Council, and the strategic/tactical oversight of the other three committees. The faculty advisory group will likely focus on educational technology issues—including support, facilities, and I/IT Literacy and Fluency; the administrative advisory group will likely focus on business process re-engineering and other administrative IT issues; and the student group on both undergraduate and graduate student issues related to IT. Nonetheless, there will be overlap between the topics that the groups might address, because each will be concerned with infrastructure issues that impact both academic and administrative functions on campus. To foster the effectiveness of the committees, there will be cross-representation on all.

- Assess the roles, responsibilities, overlap, and effectiveness of committees addressing IT issues.

- Clarify and communicate the roles and responsibilities of the Office of the AVCACT.

Steps

Implementation

All aspects of the implementation assume broad campus participation, input, and communication.

- Develop plans for establishing FACE-IT and administrative advisory body; and for the reconfiguration of the IT Council.

- Clarify functions of AVCACT office, make staffing recommendations, and complete both AVCACT website and communication plan.
• Develop primer for IT on campus that clarifies roles of ITC, FACE-IT, administrative IT body, student IT body, and the Office of the AVCACT. Online and hard copy should be distributed to new (and existing) administrators as part of communication plan. Develop orientation for new (and existing) members of all IT advisory bodies.

Required Involvement

Governance & Authority
The Office of the AVC for Academic and Campus Technology and the Office of the Provost will provide oversight of the Office of the AVCACT.

Required Departmental Involvement & Responsibilities
Campus-wide involvement is needed for successful implementation of changes in IT leadership and advisory bodies, and in Office of the AVCACT.

Expected Costs

IT Leadership Bodies
Current operating expenses for IT Council ($7500 per year) are enough for IT Council and any new IT leadership and advisory bodies.

AVCACT
A potential need exists for additional staffing to expand the role of the AVCACT office to include greater coordination with other campuses and system office, and to include a larger role in educational technology. The coordination of educational technology will necessitate at least a .5 FTE faculty associate.

Funding
Funding would come from the AVCACT GF budget.

Timing
• Fall 2002: develop plans for reconfiguring ITC and the Office of the AVCACT; develop communication plans and website.
• Fall 2002: solicit input about plans from current ITC and campus groups such as UCSU, BFA, Staff Council, CEC, Council of Deans.
• Fall 2002: Initial meetings of FACE-IT.
• Spring 2003: Newly configured ITC begins meeting; administrative IT and student IT advisory bodies begin meeting.