Message from the Vice Provost’s Office

August 2011

This is a time of transition for Computing Services. We are completing the interval — and in large measure, the work — of our 2006 Strategic Plan and developing a new Strategic Plan guided by the University’s Strategic Plan of 2008 and the results of the university’s collective efforts in information technology (IT) over the last five years. Future plans must take into account the increasing maturity of cloud computing, the extraordinary growth in end-user use of mobile devices, and the potentials of virtualization technologies. In this, our second Biennial Report, we focus our attention on the achievements of the last two years, achievements that represent the considerable talent and commitment of the Computing Services staff. The information in this Biennial Report is mapped to our 2006 Strategic Plan.

We continue to believe that these successes are built on leveraging integrated architectural frameworks that form a technological foundation, and best practices in project and process management that facilitate the work across and beyond the division. Once again, the report describes work that is most usually and increasingly accomplished cross-organizationally.

Our continued partnerships with IT support providers in the schools as well as colleagues in the central administrative offices remain critical to serving a world-class research university that thrives on distributed governance.

Although we have been able to enhance a number of campus services in the last five years, much of our effort has necessarily been expended on rebuilding the IT infrastructure and creating new patterns of planning and delivery. The considerable progress we have made should support our ability to provide services more flexibly, quickly, and securely going forward. This is certainly our goal.

We appreciate the university’s investments in information technology and are committed to being responsible for assuring effective and efficient use of those investments. We continue to pursue strategies that incorporate a blend of best practices, adaptive management, and selective innovation. It is a privilege to have this opportunity.

Carrie E. Regenstein
Associate Vice Provost for Computing Services

Joel M. Smith
Vice Provost for Computing
Chief Information Officer
Mission Statement

Computing Services provides Information Technology (IT) infrastructure and services to support the research and education missions of Carnegie Mellon.

Vision Statement

Computing Services strives to be among the best information technology organizations in higher education by continually learning about the rapidly evolving IT needs of research, education, and institutional administration at Carnegie Mellon and how to combine industry-standard production services with innovative solutions to meet those needs.

VALUES

- Outstanding service enabling world-class research and education
- A welcoming workplace for the highest quality staff
- Collaboration
- Planning, project management, evaluation
- Initiative and innovation
# Table of Contents

Message from the Vice Provost’s Office     i  
Mission Statement, Vision Statement and Values     ii  
Table of Contents     iii  

1 Redefining Services to Accommodate an Evolving University     1  
1.1 Focus on Academic Technology Services     1  
1.1.1 Clusters (Computer Labs) for Teaching and Learning     1  
1.1.2 Computing@Carnegie Mellon (C@CM)     4  
1.1.3 Evolving and Adapting Media Technologies and Services     5  
1.2 Modernization of Legacy Infrastructure     7  
1.2.1 Systems Virtualization     8  
1.2.2 Network Funding Model and Technology Upgrades     8  
1.2.3 Continued Focus on Disaster Recovery     9  
1.2.4 Enterprise Systems Monitoring and Storage     10  
1.2.5 Enterprise Information Systems and Applications     11  
1.2.6 Integrated Email and Calendar     16  

2 Secure Computing     19  
2.1 Authentication and Identity Services     19  
2.1.1 Shibboleth, InCommon and Web Login     19  
2.1.2 Password Reset Tool     20  
2.1.3 Multi-factor Authentication: One-time Password Service     21  
2.1.4 Commercial Certificate Service     21  
2.2 Information Security Office     22  
2.2.1 Incident Prevention and Detection     22  
2.2.2 Training and Awareness     23  
2.2.3 Security Assessment Partnerships and Guidance     24  
2.3 Secure Integrated Infrastructure (SII)     25
3 Evolving Management Infrastructure  27
   3.1 Planning Based on Technology Integration and Architectural Roadmap  27
   3.2 Enhancement of Planning and Project Management Office and the Tactical Planning Process  28
      3.2.1 Special Attention to Most Complex Projects  29
      3.2.2 Improved Decision-making and Governance Models  29
      3.2.3 Improved Project Portfolio Management  29
      3.2.4 Introduced Service Management  30
   3.3 Revitalized Attention to Division Human Resources (HR) Support  31
   3.4 Improved Internal Communications  33
   3.5 Common Practices  34
4 Looking Forward  35
To meet the evolving business needs of the university, Computing Services must redefine services and modernize the legacy infrastructure on which those services are built.
— Computing Services 2006 Strategic Plan

1.1 Focus on Academic Technology Services
Computing Services provides and maintains a reliable, usable environment to support the university’s educational mission. Technology-rich spaces are available to faculty members and students within public computer labs, or “clusters,” and University Registrar-controlled classrooms across campus. The division continues to partner with the Eberly Center for Teaching Excellence, Office of Technology for Education, faculty members and students in an ongoing effort to enhance the technology and spaces in support of an improved academic experience.

1.1.1 Clusters (Computer Labs) for Teaching and Learning
A 2009 report titled “Redefinition of Clusters” included the following key findings:

- Student access to software collections is often hindered due to high reservations in cluster spaces.
- Faculty members and students require consistent and timely access to software.
- The layout of existing cluster spaces does not meet the teaching and learning needs of our faculty members and students.
- Partnerships with academic departments are key to supporting the growing specialized software and cluster space needs for students.

In response to these findings, Computing Services piloted virtual software delivery for student computers, began work to deliver a collaborative teaching cluster and initiated new partnerships with several academic and administrative departments across campus.

Software Delivery for Student Computers — Virtual Andrew
Software needed for academic classes and educational purposes must be consistently installed and highly available to students and the faculty. As our population and educational increasingly rely on technology and specialized software applications, demand for access to computer labs grows. Due to this high demand for cluster space, student access to facilities and to specialized software installed in clusters is often sacrificed during high-volume course reservation times.

To meet this need and ease the current overload on physical space in clusters, Computing Services embarked on a project to investigate and pilot mechanisms to deliver software to student computers—
the Virtual Andrew project. This service would enable Carnegie Mellon students with different computers and platforms to access academic software used for their courses without physically visiting a cluster location.

In the first half of 2010, Computing Services evaluated various technologies to allow software access directly on student-owned machines. The evaluation included an analysis of technology, cost and software license limitations. It was determined that a virtual desktop infrastructure product (VDI) would provide the best combination of flexibility, consistency and accessibility for students. VMware View was chosen as the technology for a subsequent proof of concept evaluation and pilot.

During the proof of concept phase, the VMware View technology was demonstrated for selected faculty members who teach in clusters, and members of the internal project team. It was determined that the installation and use of the product were intuitive and straightforward. Upon further inquiry into usage requirements, key considerations included:

- Performance: speed and responsiveness
- File storage: ability for students to save and retrieve files
- Software availability: remote access to as much software as possible with greater flexibility to request new or updated software applications

These requirements informed the development of a pilot version of the Virtual Andrew service released in fall 2010. The pilot provided students with a limited library of academic software and complete end-user documentation for using the service. Throughout the pilot, the project team worked to evaluate and assess usage patterns, scalability, cost and performance. During the fall 2010 semester, 780 unique users accessed Virtual Andrew in 4,993 sessions. Students use Virtual Andrew to access specialized software, which means they can avoid inclement weather or walking alone late at night; they can also access the software when they are away from Pittsburgh entirely.

The initial pilot was expanded in spring 2011 to include an extended set of software applications as well as collaboration with select faculty members who used Virtual Andrew in addition to the physical clusters for their classes. This exercise helped the project team understand the impact on teaching and learning activities as well as any teaching activity issues encountered with the new service. During this phase of the pilot, Virtual Andrew served over 1200 unique users.

Faculty partners interviewed reported generally positive feedback from their students. All four of the faculty members (teaching five classes)

Virtual Andrew: Student Comments

“...I missed a week of school due to a family emergency, but it was easier for me to keep up with my work since I was able to access the cluster software on Virtual Andrew”

“It made it much easier to do work from home and at my own pace, which is important to me because I live 7 miles from campus.”

“...I felt free to do more work over a span of time rather than in one rush, so I ended up less stressed and turned out higher quality work.”

“It was able to spend more time on assignments because I could do the assignments from my own laptop.”

“made it much easier to start my homework on time because I didn’t have to schedule time to go all the way to the cluster”
reported interest in using Virtual Andrew for teaching future or different courses. Of the student respondents, 54 percent indicated that access to Virtual Andrew changed the way they normally do coursework. Many respondents were happy to be able to use Windows programs on their Macintosh or Linux computers. Several students stated that Virtual Andrew helped them to budget their time and produce higher-quality coursework.

Based on the success of the technical evaluation, proof of concept, requirements gathering and controlled pilot, plans are underway to grow Virtual Andrew into a general campus service.

Collaborative Teaching Cluster (CTC)

Faculty members who teach in cluster spaces require support for multiple instructional activities in one space. They are engaging their classes in a wide variety of activities, from students working alone and observing faculty lectures, to group discussion, critique, and sharing of student work. The current cluster layout and audio-visual equipment work well in a lecture environment; however, they do not support modern teaching methods.

To address this need, Computing Services developed plans for an experimental space that would encourage collaboration and interaction. The collaborative teaching cluster (CTC) will support diverse instructional strategies using technology. The new design focuses on three main areas aimed to address deficiencies in existing cluster spaces:

1. Foster a naturally collaborative environment.
2. Accommodate faculty and student interaction and engagement.
3. Support multi-mode pedagogical needs and classroom activities.

The CTC pilot opened in Wean Hall in fall 2011.

Design Highlights

- Long rows of tables were replaced with an innovative design using “Y”-shaped tables and flexible seating. By removing long rows of tables and inflexible machine configurations, the CTC design allows for more natural interactions between students and instructors. This eliminates the “front of the room,” enabling faculty members to teach from any chosen location in the space.
- The room layout improves visibility lines for all class participants and eases faculty member movement through the space, facilitating consultation with students at computers.

Technological Highlights

- In keeping with other classroom spaces, the CTC features a fully equipped lectern, complete with document camera.
- Projection is provided to a series of six wall-mounted liquid crystal display (LCD) screens throughout the room. Each screen can display a different digital image from an individual resident computer or laptop, or one computer can project to all six screens simultaneously. These LCD screens also allow for split-screen display, enabling faculty members to project
course materials and demonstrate techniques on the resident cluster computer side-by-side.

- Students working from their personal laptops are well supported in the CTC. Using Virtual Andrew will provide a consistent Windows platform and software configuration. Power outlets on the tabletops will support three laptops at each table (15 total). In addition, each table will have audio-visual capabilities for one laptop to project to the six LCDs.
- The desktop monitors swivel, enabling faculty members to teach to students and not to the tops of their heads.
- A whiteboard wall, mobile whiteboards and special film placed over the windows allow for ample dry erase board surfaces.

1.1.2 Computing@ Carnegie Mellon (C@CM)

Computing@Carnegie Mellon (C@CM) is a required course aimed at helping students develop foundational skills in information literacy and in safe, responsible and effective computing. Class sessions focus on the tools, technologies and services specific to Carnegie Mellon. In order to better address the diversity in students’ pre-existing knowledge, to provide increased flexibility to accommodate students’ scheduling constraints and support needs, and to reduce our resource consumption in terms of staffing and cluster reservations, Computing Services began to explore alternative delivery methods in 2008. After a successful pilot in 2009, the C@CM course was redesigned for delivery in a hybrid format—using both on-line and limited in-person instruction—through the Open Learning Initiative’s (OLI) online course environment.

While the C@CM staff and Faculty Advisory Committee continue to hold the predominant role in designing the instructional materials and assessments, the current C@CM OLI course curriculum was developed in collaboration with content experts from Computing Services, University Libraries, the Human-Computer Interaction Institute, Enrollment Services, Student Affairs, the Vice Provost for Education and the Office of Technology for Education (OTE) along with OLI course developers and learning scientists from the Eberly Center for Teaching Excellence. Although the curriculum has historically been well regarded, these
partnerships offer enriched subject-matter expertise resulting in greater breadth and depth across the curriculum and provide more effective learning intervention strategies designed by Eberly’s learning scientists.

Since the initial pilot, the structure, delivery methodology, curriculum and support model for C@CM have been re-engineered in a manner that is appropriate for self-directed learning while providing human support on an as-needed basis. In the initial iterations, support services were overprovisioned including recitation, supplemental lecture and peer tutoring. This structure allowed for modification and adaptation as appropriate, with the expectation that the need for human support would be reduced by applying learning about student performance provided by OLI’s course environment.

One of the initial reasons for transitioning C@CM to a hybrid delivery model was to reduce the impact on clusters availability. By using online delivery and renovating the C@CM teaching assistant office space into a multi-purpose teaching and learning space for instructor intervention when needed, Computing Services was able to reduce the number of cluster reservations by 59 percent, thus making the cluster facilities open to other faculty members. The activities and assessments within the new C@CM OLI course are automatically graded by the OLI system rather than manually, reducing consumption of the C@CM teaching assistants’ time.

One of the greatest benefits to transitioning to the OLI environment is the abundance of interaction-level data that is collected on student engagement with the course materials and their performance on the assessments. Decisions about student support and grading are made based on these observations and continued guidance from the C@CM Faculty Advisory Committee.

1.1.3 Evolving and Adapting Media Technologies and Services

Evolving Classroom Technologies and Services for Departments

The technology-enhanced spaces (86 University Registrar-controlled classrooms and over 19 clusters) that provide infrastructure for teaching and learning activities are evolving into a campus utility. Departments and schools are choosing to adopt the audio and video standards deployed in Registrar-controlled classrooms in their own classrooms and other spaces. Computing Services has partnered with a number of departments to deliver classroom upgrades that support the technology standard set by Computing Services. These partnerships include teaching and learning spaces within Academic Advising, the School of Architecture, Biomedical Engineering, the Department of English, Mechanical Engineering, Osher Lifelong Learning Institute and the Department of Philosophy.

In addition to the trend of adapting to a classroom standard, Computing Services has partnered with departments and schools to develop a more technology-enhanced classroom to support distance learning initiatives. These facilities incorporate technologies for global and interactive communications in the classroom with the familiar look and feel of a standard classroom. Some of these key technologies include multi-camera videoconferencing, course capture and computer content sharing to allow classes to share and create information with Carnegie Mellon remote campuses or other institutions globally. Campus units with which Computing Services has partnered to develop such spaces include Engineering and Public Policy, Heinz College and the Department of Mathematical Sciences.
Evolving Audio and Video Services for Departments

Computing Services has received requests from throughout the campus community for more readily available and accessible audio and video services. These requests resulted in the development of a self-serve model for some audio and video services. They are self-serve in the sense that no assistance from Computing Services is required in order for members of the community to use the facilities. The model depends on reliable infrastructure and clear user interfaces. The self-serve model provides more flexible, efficient and cost-effective service delivery. Three new services prompted the development of this self-service model:

- **Doha Room**
  The Doha Room is a common space in the Resnik Hall dormitory that replicates aspects of the Qatar campus—people, academics, lifestyles, traditions and celebrations. The audio, video and videoconferencing technologies in this facility provide opportunity for sharing information, exchanging ideas and communicating between the Pittsburgh and Qatar campuses. All technologies in this space are available to students in a self-service capacity. This project was sponsored by Housing and Dining Services in collaboration with Student Life.

- **Schatz Dining Room Audio Upgrade (University Center)**
  The audio system in Schatz Dining Room was outdated. Requests for audio enhancement in the space required a Computing Services technician to deliver supplemental equipment and be present to operate the equipment. An upgrade was completed to support a more efficient and flexible model in which event organizers may self-operate the resident audio system or use their own audio or personal mobile device, if scheduled for use in advance.

- **McConomy Auditorium Self-Service Model (University Center)**
  An upgrade to McConomy Auditorium was completed in collaboration with the Office of Admissions. The upgrade allows presenters to self-operate the projection system using a resident control panel and their personal computer.

**Videoconferencing for an Evolving University**

Carnegie Mellon's global focus has been one of the driving forces affecting a dramatic increase in videoconferencing (VC) usage. Computing Services has seen an increase in campus adoption of VC technologies and colleges, and departments are expanding their own VC equipment. The Pittsburgh campus has over 130 VC systems of which just over 70 such systems are maintained by Computing Services. A project was completed to transition Computing Services-maintained VC systems from individually-managed units to an enterprise and centrally-managed infrastructure. This enables us to support current and standard security practices as well as provide enhanced services such as directory dialing and direct call routing with the Qatar campus VC infrastructure for robust videoconferencing.
Telepresence Technology

As part of a project supported by the Qatar Foundation, the Pittsburgh and Qatar campuses are linked by a new Cisco Tandberg Telepresence System.

Telepresence systems are redefining the remote meeting experience. They are a set of technologies that allow remote participants to feel as if they are present, providing the sensation of being at the same table. The telepresence system is a collaboration technology that offers immersive quality, high-definition display and ease of use. To maximize and properly take advantage of the features this system has to offer, Computing Services has constructed a room following vendor-recommended acoustics and lighting design to create an open atmosphere for participants to feel as if they are in the same room.

The fall 2011 installation of the telepresence system required a close collaboration with stakeholders of the space in Posner Center, Office of the President and University Libraries. Because Posner Center houses a gallery of rare and historic books and artifacts on extended loan from the Henry Posner, Jr. Foundation, this project required close attention to access procedures and security protocols for the meeting space in addition to the standard components associated with a room installation.

1.2 Modernization of Legacy Infrastructure

Recognizing the strategic value of information technology to the university’s core missions, Computing Services continues to emphasize updates and maintenance to its IT infrastructure and systems. With the advice of the Executive Steering Committee on Computing (ESCC), Computing Services and its partners in the various administrative and academic units at the university have made substantial progress in dealing with “deferred maintenance” to the IT infrastructure. Areas of particular focus have been security; modernizing the core computing, storage, and networking services; enterprise administrative systems; and establishing financial and logistical planning for routine maintenance of core IT infrastructure supporting both research and education. This section describes the 2010-11 projects that were key to achieving goals set in these focus areas.

ESCC

The ESCC membership includes the Provost; Vice Presidents for Campus Affairs, Advancement and Research; the General Counsel; the Chief Financial Officer; Deans of two colleges; and a representative from the Academic Leadership Group. It is an advisory committee to the Vice Provost Office (Vice Provost for Computing and Chief Information Officer, and the Associate Vice Provost). The Academic Leadership Group. It is an advisory committee to the Vice Provost Office (Vice Provost for Computing and Chief Information Officer, and the Associate Vice Provost).
1.2 Modernization of Legacy Infrastructure

1.2.1 Systems Virtualization

In an effort to streamline our operations and maximize the staff’s efficiency, a virtualization project was undertaken to reduce the number of operating systems and hardware we use to construct our infrastructure. We are moving from a heterogeneous environment, including five different operating systems and three different server platforms, to a single hardware platform and only two major operating systems.

Virtualization technology continues to transform the way that Computing Services provides computing resources. By the end of 2009, we reported the capacity to run approximately 12 or more virtual guest machines (i.e., independent operating systems) on one physical server. At that time we had maximized efficiency through the use of 509 virtual machines. By July 2011, this number has grown to a total of 816 virtual machines accounting for 63 percent of our deployed servers.

1.2.2 Network Funding Model and Technology Upgrades

Historical network funding mechanisms, including base funding, outlet activation fees and the DataNet charge—a fee assessed on each campus phone line—did not adequately provide for the ongoing maintenance and capital refresh of the campus data network. In the past, requests for one-time funding addressed this gap, but continuing to rely on such requests did not allow for the budgetary predictability that the University requires of us.

In 2010 and 2011, Computing Services worked with university administration to explore and implement a new funding model for network services. The team strived to ensure that the new model more adequately associates costs with the individuals who generate them; accommodates future growth, shifts in technology and changes in the university funding models; and supports the strong history of offering ubiquitous wired and wireless network access to the entire campus community.

Recognizing the status of the campus network as a utility that benefits everyone, the new solution instituted a per-person fee. Beginning in fall 2011, students saw an increase in the technology fee. For members of the staff and faculty, a new fee went into effect for the new fiscal year beginning July 1, 2011, replacing the previous DataNet and outlet activation fees. This new funding model allows the division to address years of deferred maintenance and keep pace with technology advances.

This strategy is allowing us to be both cost-effective and to support the university’s efforts to “go green.” Virtualization of servers and storage supporting core IT services is increasing the division’s ability to respond more nimbly to the complexity of demands placed on these core services.
Secure Wireless Connectivity

In January 2011, Computing Services initiated an internal division pilot of a secure wireless network. The new network includes strong encryption inherent to the Wi-Fi Protected Access II (WPA2) security protocol, offering additional privacy and enhanced protection of data “in the air.” Individuals using the new secure wireless network are required to log in using their Andrew userID and password, providing an added layer of security.

After a successful pilot for the division, in March 2011, the pilot was expanded to include one of the academic buildings on campus. By August 2011, the WPA2 capabilities were extended to most academic and administrative buildings, and a small number of residence halls.

IBM Cabling Upgrade

Computing Services continued its work to replace obsolete IBM cabling with Cat6 cabling to support wired network and telephony applications. Since 2009, all IBM cabling in Cyert Hall and the East Campus Garage parking facility has been replaced. Work is currently underway to replace the cabling in Wean Hall and Margaret Morrison Carnegie Hall. The new network funding model will provide ongoing funding intended for replacement of IBM cabling in all remaining academic and administrative buildings in subsequent years. Replacement in residence halls will be considered in the future and weighed against the costs and benefits of a transition to wireless only connectivity.

1.2.3 Continued Focus on Disaster Recovery

Sensitive to the need for the university to carry on key business processes in the event that primary systems are unavailable for a prolonged time period, Computing Services has dedicated resources to the development of disaster recovery (DR) infrastructure, plans and methodologies.

Disaster Recovery Data Center Site

One of the fundamental goals of Carnegie Mellon’s renewed commitment to IT infrastructure involved the establishment of a new disaster recovery data center site to replace the existing site hosted in Carnegie Mellon’s central receiving warehouse. Acting on an assessment from an outside consultant that confirmed the inadequacy of the existing site, Computing Services contracted with a local colocation facility for three years to establish a new data center facility to host critical backup systems and network infrastructure. The migration from the old facility to the new one was completed in May 2011.

Beyond this new colocation facility, Computing Services has also established a goal of identifying a second, permanent data center site. This site will serve both the university’s disaster recovery needs as well as allow for growth in systems related to academic, administrative, and research computing. We anticipate that a second data center site will be selected sometime in 2012, with any necessary renovations commencing shortly thereafter. Our goal is to have the new site populated by 2013, shortly before the contract on our new colocation facility expires.

IT Disaster Recovery Program

Computing Services has focused the disaster recovery and business continuity effort on what we call “IT-centric DR.” This approach concentrates on implementation of processes, procedures and technical solutions to provide disaster recovery capability for university mission-critical systems on a server-by-server basis. The goal of the IT disaster recovery (ITDR) program is to implement, test and validate recovery of critical servers and IT infrastructure within established recovery time objectives and recovery point objectives.

Computing Services will work with university business units to develop and implement disaster recovery plans and supporting methodologies,
procedures, and tools. This effort includes the following:

- Definition of roles and responsibilities
- Key decision points and critical lines of communication necessary to guide, monitor and control the activities associated with responding and recovering from a disruptive event or outage
- Restoring back to a “business as usual” steady state of operations

To begin this DR process development, a project was initiated to create ITDR solutions for university applications and services using an iterative, incremental “Rinse & Repeat” (R&R) process. The goal of the R&R process is to design, implement, test, validate and make operational repeatable recovery capabilities within established recovery objectives on a server-by-server basis. The planned steps to complete this process include:

1. Document the current architecture, production processes and critical resources for the application or service.
2. Develop and design an appropriate DR architecture that is compliant with Secure Integrated Infrastructure (SII) standards and principles.
3. Acquire the necessary hardware and implement the DR architecture.
4. Collaborate with the business unit to design and determine the scope of testing criteria, complete tests and address any issues.
5. Document and assess findings, implementing process improvements where appropriate.
6. Partner with the business unit to identify roles and responsibilities for continued operations, maintenance and testing of the DR solution.
7. Repeat this process for the next key application or service.

The applications and services servers included in this initial pilot are Payroll Services, the Human Resource Information System (HRIS), the Student Information System (SIS) and Oracle Financials. Once the R&R process is complete, we will have a tested DR replacement for each server capable of running the software of the primary server, housed in an alternative (off-campus) data center.

**1.2.4 Enterprise Systems Monitoring and Storage**

Computing Services replaced its previous open source systems monitoring software (MON) with a commercial monitoring tool (Zenoss). The new solution provides an improved interface and more robust and reliable monitoring functionality. The previous system lacked a framework
for monitoring new applications and devices and required extensive system customizations to meet these needs. The new solution provides this functionality and better accommodates monitoring requirements. Overall, the new monitoring system allows Computing Services to identify problems earlier and respond more quickly, ultimately providing improved service to our users.

In addition to system monitoring, Computing Services’ enterprise storage, Storage Area Networking (SAN), has expanded and improved in a number of areas. These enhancements focused on the following areas:

- Improved availability, security and capacity of the SAN environment.
- Added redundancy in the underlying networking and host connections in order to avoid downtime as a result of failures in the underlying supporting architecture.
- Developed various “failure domains” to allow application owners to isolate potential failures.
- Created multiple “security domains” in order to provide better separation and protection of data.
- Significantly increased total SAN storage capacity to address the increase in user’s storage requirements, especially due to the growth of the virtualized systems.

Work to achieve these improvements required significant collaboration across division groups. We also participated in user groups and beta testing activities with our SAN vendor. Close work with the vendor facilitated the implementation of many of our improvement suggestions.

### 1.2.5 Enterprise Information Systems and Applications

Carnegie Mellon is achieving the desired integration of business processes, information systems and staffing through deliberate creation and application of architectural principles, governance structures, project management and review of its enterprise system projects. All the major projects—evolution of the Student Services Suite, replacement of the Human Capital Management systems and upgrades for Oracle Financials—have steering committees consisting of both business and technical staff members. Those steering committees govern the projects largely through consensus.

Reaching that consensus leads to what we believe to be a workable mix of evolving both business processes and technology and keeps the changes synchronized. Periodically, leaders of the steering committees report to and seek the advice of the Executive Steering Committee on Computing (ESCC) to help the university coordinate business processes and technologies that support those processes.

**Student Services Suite (S3)**

Computing Services has pursued a number of projects to update the university’s student information system (SIS), transforming the legacy system into what we call the Student Services Suite (S3). We carefully considered the cost-effectiveness and state of development of current commercial student information systems and decided that the best option for the university was to update the underlying technology and user interfaces to its legacy SIS. Computing Services engaged consultants who specialize in analysis and modernization of “legacy systems” to help
with the work and substantial progress that has already been made in this process.

- **Online student invoices, eBills, have replaced paper-based invoicing.** Prior to the release of eBill functionality, students and their parents received paper-based bills only. The eBills project produced a Web application for students to retrieve a PDF copy of their monthly invoice. Students may optionally register their parents to receive an electronic copy of the bill. This enhancement delivered a valuable service to students and their parents while eliminating one of the largest paper-producing services of the Student Information System.

- **Student self-service application has been modernized with significant functionality improvements.** The existing student self-service application, Student Information Online (SIO), was converted to modern application architecture with significant improvements in functionality. Two legacy applications—the searchable online course schedule (Course Information Online) and the application for graduation (Graduation Online)—have been replaced by incorporating the functionality into SIO.

- **Modernization of SIS administrative application infrastructure and interfaces.** A suite of initiatives (titled the “S3-Homogeneous Technology Phase”) is currently under construction with the primary goal of modernizing the current SIS administrative application infrastructure and interfaces. The underlying Ingres database will be replaced by an Oracle database and all legacy text-based user interfaces will be replaced with a modern Web interface. All batch processes will be converted to use a consistent set of new interactive technologies. Small scale improvements in functionality will be undertaken during this phase.

The future roadmap for the S3 project has been defined and initiated with anticipated completion in the next three to five years. Once SIS is upgraded to a sustainable platform, the next phase—S3 Functionality Focused Phase—will leverage this work to make substantial functional improvements in the Student Information System. This phase will include the implementation of a new Financial Aid system, new Student Financials, continual improvements to the student self-service application and possible implementation of Kuali Student\(^3\) Enrollment modules.

### Kuali Student

\(^3\) Kuali Student refers to an effort by a number of universities under the aegis of the Kuali Foundation to build an open-source student system for higher education. Carnegie Mellon may be able to use some of the software produced by that effort.

### Human Capital Management and Payroll Systems Replacement

After developing detailed requirements for new Human Resources (Human Capital Management—HCM) and payroll systems, the university decided the best course of action would be to acquire a new commercial system. After an extended process of specifying requirements, issuing requests for proposals from all suitable vendors and analyzing those responses, Carnegie Mellon is in the process of negotiating a hosted solution to replace its current human resource and payroll systems and a licensed time and labor solution. We expect the project to take approximately three years to complete.

From the fall of 2008 through calendar year
2009, Computing Services worked with third-party consultants to create detailed, prioritized functional and technical requirements for HCM, payroll, international payroll, and time and labor systems. This requirements work included definition of specifications for system integrations, documentation of current business processes, identification of business process improvement opportunities and development of a change impact assessment.

In 2010 we issued a request for proposals. Through vendor visits, product demonstrations, technical assessments, reference calls and a total cost of ownership assessment, we narrowed the selections for HCM and payroll solutions to Workday and PeopleSoft and to Workforce Software for the time and labor solution. With substantial campus support for Workday, we focused on addressing remaining functional and technical gaps in that solution. Contract negotiations with Workday and Workforce Software are currently in progress.

We are now evaluating international payroll solutions as well as implementation partners for all solutions. Implementation of the HCM, payroll and time and labor solutions began in fall of 2011 and will continue for three years.

A data validation project to analyze, cleanse and prepare current HCM data for migration to a new system began in February of 2011 with expected completion by the end of the calendar year.

**Application Virtualization**

Over the last several years, Computing Services and campus business partners have struggled with security and support issues for enterprise applications that required specific versions of client software which often contained known security vulnerabilities. These are the applications that access our most sensitive data and systems (e.g., Oracle Financials, Oracle Applications Desktop Integrator/ADI, Electronic Health Records/EHRS, etc.). Applications and components require security patches to remain secure, and application vendors often fall behind in certifying patches resulting in applications with different, incompatible version requirements (e.g., Java/JRE, Operating Systems, .Net Framework, Oracle Client, etc.). A satisfying balance between data and system security, user experience and system and application support (including patching and testing) has been difficult to achieve. This problem continues to be compounded by the increasing frequency of security patches. One promising strategy for achieving better balance is application virtualization.

Overall, virtualizing applications has the potential to provide great benefits in terms of security, customer experience and supportability. The ISO led a discovery project and implemented a few early pilots using application virtualization and the results were very promising. We hope that in the long term, the virtualization strategy could reduce dependency on desktop applications and provide a viable strategy for delivering applications to new devices such as tablets and mobile devices.

Moving forward, Computing Services will implement an application virtualization strategy initially focused on specific enterprise use cases. The strategy calls for development of a scalable, sustainable design, including an appropriate governance model.
Oracle Financial Upgrade to R12
Computing Services and Financial Services have embarked on a project to upgrade the current Oracle 11.5.10.2 E-Business Suite (EBS) of applications to version R12. Extended support for Oracle EBS 11i will end in November 2011 and it is necessary to upgrade in order to maintain an adequate level of support for the university’s Oracle Financial systems.

A related hardware modernization project, “Oracle Financials Re-architecture” will roll out concurrent with the R12 Upgrade project. With Oracle R12, Carnegie Mellon will move from a single-node Sun hardware platform running the Sun Solaris UNIX operating system to a multi-node Red Hat Linux configuration. The re-architecture will allow compliance with the division’s Secure Integrated Infrastructure principles. The move to the Linux operating system will also achieve economies of scale and standardization of the skill sets needed to support the platform. The Financial Data Warehouse has already been re-architected and will not be part of these activities.

Enterprise Service Bus (ESB) with the Oracle Financials System
The Oracle Financials System (E-Business Suite) interacts with multiple internal and external applications. Currently, we employ a wide variety of integration methods: synchronous, asynchronous, batch, real-time, automated and manual, each implementation requiring a unique solution for authorization, monitoring, security and fail over. These interfaces are difficult to maintain, as they often require modification when the systems at either end point change; they are also difficult to troubleshoot when problems arise. The current set of interfaces cannot be adapted to support real-time integrations, business process changes or new technical requirements without rewriting most of the code.

To address these issues in new integrations, Computing Services will begin development of a standard mechanism to manage file transfers between systems. We are currently evaluating an Enterprise Service Bus (ESB) product to handle security, file routing, monitoring and file transformation when necessary. The service bus can act as a central clearinghouse for inter-application communication and provide services that include encryption, improved management, service orchestration, audit trails and more. The result of these changes can be more flexible, manageable and robust communication between applications.

Our solution for Oracle Financials R12 file feeds uses the ESB to do the file routing and a Java messaging system to queue the files. Computing Services will develop a standard, reusable authorization service to secure the...
communications, as well as services for extracting and displaying useful file transfer metrics. All file-based integrations in and out of the financial system are within scope for this initial implementation. A new Web-based user interface will be developed for submitting files manually. Both the Web interface and automated system-to-system file transfers will use the same set of services.

Developing these components as services and using the ESB to manage the services will make it easier in the future to integrate an individual, discrete business process into a broader business process that contains multiple steps and touches multiple systems. It also allows for easier integration with Oracle's other Services-Oriented Architecture (SOA) Suite products that will form the basis of future Oracle EBS releases. It should decrease the time required to bring in new external partners such as banks, and allow us to make changes to file formats or even some file content without modifying code.

By taking this SOA approach and encapsulating programming and business logic in a set of discrete services, we should only have to handle minor modifications to the systems at each end of the integration. We expect the ESB to place bank and feeder files in whichever locations the upgrade team specifies for Oracle Financials processing. This should not generate much extra work for those doing the upgrade or for other system owners that need to transfer files to the financial system. The target completion date for this project is August 2011.

Electronic Health Records System (EHRS)
The Electronic Health Records System (EHRS) project delivered a fully-integrated, secure electronic medicals record system for use by

Student Health Services (SHS) and Counseling and Psychological Services. The new system includes patient scheduling, reporting, immunization and insurance monitoring, and visit information. The project implemented a new support model within the division, by hosting the system within the university network and allowing the third-party vendor access to their application for maintenance, upgrades, and support. This model allows for university control of network access, data protection, and ownership of the infrastructure necessary to support the EHRS.

Over 86 percent of all undergraduate students seek care from SHS during their tenure at Carnegie Mellon and every full-time student has contact with SHS at least once. In a single calendar year, SHS accommodates over 21,000 student visits. The benefits realized by this implementation include reduced time spent on data entry and appointment scheduling by up to 80 percent due to self-service scheduling, patient input of medical and immunization history, and self-check-in. The EHRS provides an adequate audit trail of access to student medical records. Increased efficiency during patient visits is also
demonstrated by the ability of providers to have real-time access to records and medical information in the exam room, without the need for paper charts.

**Sponsored Projects Exchange System (SPEX)**

The Sponsored Projects Exchange System (SPEX) is a FileMaker-based award management system used by the Office of Sponsored Programs (OSP). The OSP relies on this system to track proposal and award activity. Although the OSP plans to replace the aging system in the 2012-13 timeframe, Computing Services and OSP recognized this system as critical to the ongoing operations of the institution and implemented an interim solution to ensure stability and security.

Work was completed to upgrade the FileMaker database; implement a new server infrastructure and development environment using the virtual machine infrastructure; transition the service to the Secure Integrated Infrastructure (see page 25) environment; deploy client security enhancements for SPEX client software using Cisco AnyConnect to secure connections; and develop system monitoring during business hours.

**Web Content Management System (CMS)**

In 2006, Computing Services, in partnership with University Advancement, released the current Web content management service (CMS) to university units. As part of this service, the division provides significant consultative support in addition to the core technology. This personal attention has been a key factor in the success of the service, which now supports approximately 300 sites covering nearly the entire administrative component of the university and a growing plurality of the university’s academic Web presence.

In order to properly support this growth and requests for a broader set of features, Computing Services has entered the early stages of a project to evaluate the existing CMS technology. As part of the project, we will assess customer needs and revisit our support processes to ensure that the service continues to meet the needs of the institution.

### 1.2.6 Integrated Email and Calendar

Computing Services has provided the campus with email and calendar using the Cyrus email environment and Oracle (“Andrew”) Calendar services for over a decade. Although the current Cyrus environment provides a reliable email system, it lacks some modern email features. In recent years, Computing Services has received numerous requests from university business units for improvements to our current email and calendar services. These requests focus on integrated email and calendar client applications, mobile phone support, improved webmail and advanced email features.

Our email and calendar concerns assumed a new sense of urgency when Oracle released a new calendar product to replace Oracle Calendar and announced that premier support for Oracle Calendar would end. A great deal of university administrative work relies on a robust enterprise calendar.

Therefore, Computing Services initiated a project to examine the issues and costs of an alternative calendar service — with a goal of accommodating the requests for integration with email service — for faculty and staff members and graduate students.

The results of the initial project to examine issues and costs of an alternative calendar solution indicated that, for the faculty, staff and graduate students, Microsoft Exchange Server would provide the best integrated email and calendar solution. Exchange provides a viable enterprise calendar that is integrated with email and that, because of its market dominance, provides...
widespread, regularly-updated support for mobile devices. This recommendation was vetted with the Executive Steering Committee on Computing (ESCC).

The next phase of this evaluation included meetings with the leadership and key IT personnel within academic and administrative departments. The goal of these discussions was to listen and understand the business productivity concerns associated with a change in email and calendar systems to better inform an implementation plan. These conversations took place in summer and fall 2010 and identified the following common needs and concerns:

- Increased need for immediate, seamless integration of email and calendar with mobile devices.
- Increased demand for integrated email and calendar functionality at the enterprise (university) level. Belief that organization-wide adoption of an enterprise calendar system is best considered at the level of the administrative unit. Schools will continue to see mixed email and calendar adoption. Therefore, a model to support this usage trend is desirable.
- Security, privacy and reliability concerns associated with outsourced options are still prevalent.

Based on the technical evaluation of possible solutions and the information gathered through discussions with university stakeholders, the following implementation plans for an alternative email and calendar solution for the faculty, staff and graduate students were set into motion:

- Microsoft Exchange will be provided as the integrated email and calendar solution for central administrative units.
- Schools will be given the choice to “opt-in” to the Exchange solution. Deans and department heads will decide whether all, none, or portions of their organizational units will migrate to Exchange. Individual faculty can elect to opt-in to Exchange if they choose. Academic departments and individuals not moving to Exchange will continue to use Cyrus email and Oracle Calendar, until it is decommissioned.
- Computing Services will start to seek input concerning email and calendar services for undergraduates in fiscal year 2013.

Extended Deployment Plan

Through summer and fall 2011, Computing Services conducted an early adopter program with groups internal to the division and later with two external departments. The purpose of this program was to test and improve implementation of the Exchange service including the migration process, documentation, training and ongoing support model. Special attention was given to the calendar challenges faced by administrative staff members who support multiple executive-level calendars. This included close consultation and “power-user” group meetings with these individuals.

In late 2011, the Exchange team will evaluate and plan for a 2012 campus deployment based on information gathered from experience throughout the Early Adopter program. At that time, Computing Services will communicate plans for engaging with interested departments and individuals. This will be a phased deployment scheduled according to availability and the business calendars of individuals and departments. Computing Services will work closely with departments throughout their migration.
Carnegie Mellon is an internationally recognized leader in computer security, through its research and information programs in cyber security, survivable systems, computer security incident response, and policy. In August 2004, the Information Security Office (ISO) was established with dedicated resources to coordinate and sustain an information security program to address vulnerabilities and risks to information and technology infrastructure across campus. Since the inception of the ISO, the division has aggressively taken steps to move from a default “open” to a default “protect” infrastructure and to address the need to reduce decentralized storage of sensitive data. Computing Services continues to deliver and evolve services to improve security and reduce institutional and individual risk. The following accomplishments have enhanced the security of the computing environment and helped address current compliance standards and policies.

— Computing Services 2006 Strategic Plan

2.1 Authentication and Identity Services

Like many other institutions, Carnegie Mellon is reviewing and re-engineering its Identity Management (IdM) platform to better position itself for cloud, federated and future services. The modernization of our current IdM environment will ultimately include group management, permissions management, compliance with InCommon assurance levels and the ability to interact with government and other academic entities. Computing Services views identity as a critical emerging infrastructure for any modern institution of higher education and continues to dedicate the resources necessary to support renovation and growth. Following are examples of recent accomplishments and future directions.

2.1.1 Shibboleth, InCommon and Web Login

Shibboleth technology enables organizations to build a single-sign-on environment. The architecture defines a way of exchanging information between organizations and providers of digital information in a secure manner. It is often used to support federations, or “trust relationships,” that facilitate access to resources for the federation’s members. For example, several research consortia, such as TeraGrid, form trust relationships that allow participants to use their credentials (username and password in some cases) from their home institution to access shared data and tools. By allowing individuals to access Web-based resources across institutional boundaries via a single login, it unites us with organizations external to Carnegie Mellon. This technology is an important component in protecting both the security of the data and the privacy of the individual.
Carnegie Mellon has joined InCommon and has two identity providers in the federation: one represents the Carnegie Mellon community and the other is a guest identity provider where guests gain access by invitation only. We already have a number of service providers in the federation and InCommon is being used as the local Carnegie Mellon federation. We expect to have about 200 service providers in InCommon over the course of the next 18 months. Although some service providers may not see a need to grant access to external identities at this time, use of identity providers within the federation makes re-configuration trivial should the service access policy change in the future.

Computing Services has provided guidance for Web service owners to install and configure the Shibboleth authentication technology. As campus Web services transition from our existing Pubcookie-based WebISO authentication service to Shibboleth authentication, consumers of these applications will become accustomed to the new Web Login page for entering their account userID and password. Computing Services will continue to communicate and educate the community as services are transitioned.

Some Carnegie Mellon services that have already transitioned to Shibboleth authentication include: CILogin for TeraGrid, Faculty Course Evaluation and the Taleo Talent Management System. Plans over the next several months include the transition of services including ADP iPay; National Institutes of Health (NIH) PubMed and other NIH services; National Science Foundation (NSF) FastLane; and Research.gov. Additionally, the School of Computer Science is moving to Shibboleth-enable their applications through a Computing Services’ hosted identity provider.

Tartan-ConnectID

Tartan-ConnectID is the second Carnegie Mellon identity provider within the InCommon federation. For services that are Shibboleth-enabled and configured for use by external identities, Tartan-ConnectID allows a person outside the Carnegie Mellon community to securely access an application or service provided by the university. Through the registration process, a link is established between the individual’s external provider (e.g., Google, AOL, Yahoo, InCommon) and a local Carnegie Mellon identity. This process allows the individual access to certain services offered at Carnegie Mellon and other institutions of higher education.

My Plaid Student is the first application to make use of Tartan-ConnectID. My Plaid Student allows students to authorize and invite external individuals (e.g., parents or guardians) to access their invoice information. My Plaid Student expansion plans include the addition of grades, financial aid award letters, schedules, etc. In addition to providing better access to student information, this effort is expected to result in decreased costs for invoices, financial aid letters, and other student-related paper mailings. Other benefits are expected in terms of expedited admissions, financial aid, and other student account workflows.

2.1.2 Password Reset Tool

In continued efforts to improve security and services associated with Andrew account passwords, a new password reset service was released to the campus community in spring 2010. The new self-service utility offers improved security questions and is available 24/7 to reset forgotten passwords. The Computing Services Help Center has historically received a high volume of password reset requests; this self-service tool allows individuals to reset passwords for themselves to reduce any delay in application or system access.
Because the service may only be used if an individual has pre-set the security questions, all incoming students are now required to select and answer three security questions when establishing their initial password. Faculty and staff members are strongly urged to configure their security questions for the service but are not required to do so.

2.1.3 Multi-factor Authentication: One-time Password Service

The ISO has operated a One Time Password (OTP) authentication system for over four years. The system is used for two-factor authentication to remotely access protected servers (i.e., those within the SII environment; see page 25). These servers house some of the most sensitive data at the university and two-factor authentication is one of the special security measures in place to safeguard this information.

The OTP service was initially implemented to allow Computing Services to learn early lessons about managing the service and to potentially explore other two-factor alternatives.

In response to demand, and in preparation for the expiration of the original two-factor devices, a project was initiated to explore replacement OTP services. The ISO examined use cases and available technology and decided to continue an expanded OTP service replacing the previous solution with the Vasco OTP solution.

The Carnegie Mellon OTP service consists of the following two factors:

1. A Vasco key fob or smartphone application that displays a six digit number that changes every 32 seconds (something one has).
2. A password set by the individual (something one knows).

By combining the six-digit number and the individual's password, a one-time password is created. This one-time password expires in 32 seconds and is only useful for one login. This makes guessing a password virtually impossible as it changes every 32 seconds and requires physical possession of the fob and knowledge of the fob owner's password.

The initial OTP service was extended to 55 individuals. With release of the Vasco OTP service in 2010, the new service now supports 155 individuals.

2.1.4 Commercial Certificate Service

The Information Security Office worked to transition from a homegrown internal Certificate Authority to a new commercial solution. The internal certificate service required individuals to download and install the Carnegie Mellon root certificate to work properly. In many cases, users did not install the root certificate and simply clicked through certificate warning messages, an undesirable security practice. Commercial certificates, on the other hand, are pre-installed in Web browsers eliminating the need for additional installation and the potential to condition users to click through warnings. While the ISO also operated a commercial certificate service, costs were passed along to the requesting department so most departments limited their use. Finding a more competitively priced and featured commercial provider to replace the existing commercial provider was part of this effort as well.
In April 2010, the ISO began issuing commercial SSL certificates from Comodo to qualified members of the university community. (Comodo was subsequently selected by InCommon for their commercial certificate program based on the research and negotiations of this effort.) These certificates are typically used to provide service authentication and protocol encryption for Web sites (e.g. HTTPS/SSL/TLS) and are recognized automatically by nearly all popular Web browsers. In addition to the standard SSL certificates used on most Web servers, several variations on these certificates are also available; these include Unified Communications certificates, Wildcard certificates, certificates with additional Subject Alternative Names, etc. The Comodo certificates are offered at no cost to university Web developers, are valid for up to three years and no longer require individuals to install Carnegie Mellon root certificates.

2.2 Information Security Office

2.2.1 Incident Prevention and Detection

The ISO continues to develop tools and pioneer initiatives to take preventative action against malicious activity. Work continues to support existing tools described in the 2008-09 biennial report such as First Connect and Identity Finder. In addition, two new efforts have been launched to proactively protect computers and data: the Patch Check Web tool and Application Virtualization project (discussed in section 1.2.5 Enterprise Information Systems and Applications).

Patch Check Web Tool

In 2010, the ISO recognized a significant increase in the number of campus Windows computers being compromised by credential-stealing malware spread through routine Web browsing. These attacks tricked the Web browser into silently opening malicious files that exploit outdated versions of Adobe Acrobat, Adobe Reader, Adobe Flash, and Java even when updated anti-virus software is running. These exploits were not new but became more prevalent through malicious advertising services on very popular, legitimate websites. Simply visiting a site could silently infect a computer as ads rotated on the site and delivered infected content.

Applying software and plug-in patches is often a cumbersome task, and even IT professionals are not always certain their computers are up-to-date. Acknowledging this difficulty, the ISO developed
a Web-based Patch Check tool. On a regular basis, individuals are asked to visit the Patch Check Web site (https://www.cmu.edu/iso/patch-check/) from each of their Web browsers. The site runs a check to confirm whether or not the latest, safe versions of browser software, Adobe Acrobat, Adobe Reader, Adobe Flash and Java are installed and provides guidance for updating if needed.

Nothing on the Web remains a secret for long. Soon after its release to the campus, the ISO received dozens of requests from peer institutions to use the Patch Check tool and/or to get access to its source code. Since then, a variety of similar sites have sprung up. The ISO will be evaluating those sites as possible replacements to improve quality and eliminate maintenance burdens.

Expansion of Intrusion Monitoring
Since 2009, the ISO Security Engineering and Operations team has expanded Intrusion Detection System (IDS) capabilities within the enterprise data center environment. With this expansion comes greater ability to monitor the servers that host mission-critical business systems for evidence of attack and compromise. Timely alerts from the IDS improve incident detection and response time and mitigate adverse outcomes.

2.2.2 Training and Awareness
The ISO continues to offer training and awareness programs including Malware Removal, Security 101 and Identity Finder. Over the last several years, significant effort has been dedicated toward extending this training to C@CM student participants (see section 1.1.2 Computing@Carnegie Mellon (C@CM). Through close partnership with the course development team, the ISO has contributed to the Safe and Responsible Computing units.

Additionally, the ISO continues efforts to raise campus awareness regarding phishing especially given greater frequency in targeted phishing attacks. Phishing is an attempt to acquire personal or sensitive information by impersonating a trusted entity to lure the recipient into providing information or visiting a malicious web site. Often, phishing aims to acquire credentials like our Andrew ID and password, placing university information at risk as well as personal information.

Beginning in 2010, phishing awareness campaigns included the use of two interactive online games; Anti-Phishing Phil and Phyllis. Anti-Phishing Phil is used to educate the community on how to identify phishing URLs, where to look for clues in Web browsers and how to use search engines to find legitimate sites. The companion game, Anti-Phishing Phyllis, asks...
Secure Computing
2.2 Information Security Office

players to help Phyllis teach her school of fish how to avoid phishing traps in fraudulent emails. Traps covered in the game include fake links, malicious attachments, cash prizes, “respond-to” emails asking for sensitive information and more. Players are taught to verify the information presented, rather than trust easily-forged email features such as logos or URLs to decide if a message is fraudulent or not.

2.2.3 Security Assessment Partnerships and Guidance

As the ISO continues work to make information security a standard consideration in university operations, we are asked to partner and provide consultation on an expanding portfolio of projects. Following are a few representative efforts:

Research Requirements

The ISO partnered with researchers, IT personnel, and the Office of Sponsored Programs to address information security requirements for export controlled data. This work included the review of technology control plans, active security assessment, and the development of documentation to address gaps between the published Data Protection Guidelines and regulatory requirements.

Contract Boilerplate

An ISO-led Computing Services team collaborated with the University Contracts Office to develop standard security contract terms to bring consistency to contract language and mitigate risks inherent with cloud adoption. Terms included right to audit, data breach notification, media sanitization and third party sharing. The ISO will continue its collaborations with the Contracts and Purchasing Offices to improve documentation, assessment and approval processes. This work helps educate and empower campus buyers to facilitate the purchasing process without incurring unnecessary risk related to security and business continuity.

Software as a Service (SaaS) Guidance

Adoption of cloud services is on the rise. Services ranging from Internet-based backup to survey sites like SurveyMonkey are easily and inexpensively acquired, so much so that they can be initiated with the click of a mouse, not subject to the usual review and scrutiny applied to more expensive purchases or contracts. As a result, data—sometimes even restricted data—is leaving the enterprise and hitting the cloud without due process. Providing SaaS guidance by helping the community balance the risks and rewards of the cloud through education, process, documentation and assessment is a developing role for the ISO. Keeping pace with increased demand will be a challenge.

HIPAA, FERPA and PCI DSS Compliance

In 2010, ISO collaborated with a number of campus partners to ensure university compliance with the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA) and the Payment Card Industry Data Security Standards (PCI DSS). Some of the efforts in 2010-11 include:

- Collaborating with Student Health Services, Human Resources Benefits and Office of General Counsel to revise the original HIPAA Information Security Policy and documentation resulting in publication of the HIPAA policy. The director of the Information Security Office became the designated HIPAA security officer.
- Partnering with the university’s FERPA officer to ensure compliance in recording exposures of student information.
- Working with the Office of General Counsel, Finance Division, various departments within Computing Services and specific business units to assess applicability and progress towards PCI DSS compliance.
Early Implementations of Information Security Policy and Guidelines

After first evaluating and addressing its own compliance, the ISO began the process of shepherding early adoption of the Information Security Policy and related documentation. These early adopter efforts include a joint assessment project with University Advancement; work with the Office of Sponsored Programs and Electrical and Computer Engineering (ECE) to apply policies to export controlled research; and inclusion in the requirements for the annual compensation review process.

2.3 Secure Integrated Infrastructure (SII)

As Computing Services has grown to accommodate the expanding technology requirements of the university, it has become increasingly important to consolidate our disparate computing environments into a single, secure, scalable production-ready environment. This environment is used to house both infrastructure and applications systems. The Secure Integrated Infrastructure (SII) program was instituted to develop this unified and secure computing environment along with supporting processes to review, secure and place systems properly within the SII. All systems — whether they are modernizations of existing services or new services — are reviewed for compliance to SII principles and are placed within the area of the SII environment that provides the appropriate security controls.

Efforts are underway to migrate all of Computing Services’ systems to the SII environment. Of the 1,194 physical and virtual servers that Computing Services manages, 67 percent have been moved into the SII environment. SII differentiates systems as providing either “infrastructure” or “application” services. Infrastructure systems provide service to other computing systems, as well as end users. Application systems provide service only to end users. Because the infrastructure systems provide core services, they are moved into the SII environment first. As of 2011, all of the Computing Services infrastructure services are resident in the SII environment.
As a technology organization serving a sophisticated university community, it is our responsibility to base IT planning on a well-designed architectural roadmap implementing technologies that satisfy the evolving needs of our clients. This architecture must also fulfill our commitment to develop a sound and secure environment that is consistent with industry standards. The organizational separation of the Architecture and Project Planning and Management units allows us to proactively focus on technology leadership for the university.

— Computing Services 2006 Strategic Plan

Computing Services has made great strides in evolving management strategies and organizational structures since the writing of its Strategic Plan in 2006. These are some of the highlights of the strategic initiatives anticipated at that time.

### 3.1 Planning Based on Technology Integration and Architectural Roadmap

The Architecture and Technology Integration (A&TI) organization acts as an extension of the Office of the Vice Provost regarding issues of Computing Services technical governance and the maturity of our planning processes. At the heart of this effort are identification and advocacy for divisional and industry common practices that are believed to promote overall security and flexibility while controlling the cost of Carnegie Mellon's IT infrastructure. The project planning process has been modified to include an early architectural assay conducted by A&TI to improve the quality of tactical plans submitted and, in particular, to increase awareness and potential for reusable application or infrastructure components.

One of the biggest changes in the IT landscape in the last two years is the emergence of Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) offerings. A&TI has worked with the Information Security Office to update our vendor evaluation and assessment practices to include considerations for these kinds of offerings. We have been involved in several efforts to expose and integrate emerging middleware practices from higher education into cloud vendor roadmaps and offerings. Coherent integration of cloud offerings with our evolving applications development practice and our operational security approach remains a primary concern of A&TI.

A&TI acts as the primary contact for engaging researchers on campus in their requests for Computing Services operational data for research purposes. While this work has been ongoing for several years, we are now working on a more formal characterization of the efforts to create better awareness of the activity, and especially
to allow for periodic assessment of value in the context of other services in the division.

3.2 Enhancement of the Planning and Project Management Office and the Tactical Planning Process

The Computing Services Planning and Project Management Office (PPMO) implemented project management process improvements in governance, closure, status reporting, and integration with portfolio management. The division deploys several models of project management to fit the needs of the projects. With a pool of three certified Project Management Professional senior staff members, the PPMO directly manages about a third of the most complex projects. In addition, several long-term enterprise application projects, such as student services and human resources, employ dedicated project managers with dual accountability to both Computing Services and the business partner sponsors. The PPMO provides mentoring, consulting, and some training to the division.

PPMO Managed Projects 2010-11

◊ Academic File Storage Pilot
◊ Application Virtualization (Project Management and Business Process)
◊ Calendar and Email Implementation Discovery and Delivery Program
◊ Content Management System Discovery
◊ Electronic Health Records Systems Delivery
◊ Enterprise Monitoring Selection & Deployment
◊ Enterprise Service Bus Discovery and Delivery (Consultation)
◊ Finance Project Planning and Early Preparation for R12 Update
◊ Financial Data Warehouse Migration Delivery
◊ Future Data Center Planning Delivery
◊ HR/Payroll Requirements Gathering
◊ Identity Management Program
◊ iPay Shibboleth
◊ ISO One Time Password Change (Consultation)
◊ IT Disaster Recovery/Business Continuity Program
◊ Media Tech Departmental Project Management (Consultation)
◊ Parental Access Identity Management
◊ Parental Access Student Services Suite
◊ Pre-Award SPEX Upgrade (Consultation)
◊ Oracle Financials System Upgrade (Facilitation)
◊ Secure Integrated Infrastructure Program (Service Review and Process Changes)
◊ Service Oriented Architecture Governance (Consulting)
◊ Software Delivery on Student Computers (Consultation)
◊ Student Services Suite Central Planning Roadmap
◊ Taleo Human Resources applicant tracking system
◊ TeamDynamix SaaS vs. Installed Discovery
◊ Typhoon Server Migration Delivery and Closure
◊ Voice over IP Discovery
◊ Zenoss Monitoring Discovery and Delivery
project leads within departments for mid-sized projects. By determining the levels of service needed for each project, we can apply our project management resources most efficiently.

3.2.1 Special Attention to Most Complex Projects

As the five infrastructure upgrade projects funded by a bond issue were completed in 2008, Computing Services moved its project management focus to the most complex division initiatives. Most of these projects were reviewed periodically by the Executive Steering Committee on Computing (ESCC). All required additional coordination with our business partners. The certified project managers in the PPMO managed 16 Technology Commitment projects, including My Plaid Student, the calendar and email discovery, disaster recovery and data center improvements, Human Resources’ staff recruitment replacement (Taleo), and application virtualization. Targeted project reviews were shared proactively with Internal Audit including summaries of project status, risks, finances, and schedules. PPMO is implementing project management metrics to identify the key areas where professional project managers have the greatest impact.

3.2.2 Improved Decision-making and Governance Models

Decision-making on highly complex projects that are jointly sponsored by Computing Services and business partners benefited from carefully defined governance models. Early in the project, the joint sponsors clearly defined the decision-making purview of the project partners and the project communications plans at each level. A typical governance structure gave the working project team the responsibility for changing incremental schedules, tasks or resources while maintaining the overall project plan. Changes to project scope, schedules, budget or resources that affected more than 20 percent of the project plan required decisions at a project level including executive sponsors, the project manager and team leads. The steering committee of executive and project sponsors provided strategic oversight of the project with the focus on risks, issues, goals, final deliverables and dependencies.

Periodically, the PPMO managed a project planning exercise with business partners to define tasks, resources and sequencing of the enterprise level projects. The ESCC reviewed the final sequencing resulting in a set of high-level multi-year plans referred to as the Technology Commitments document.

3.2.3 Improved Project Portfolio Management

Acquisition and implementation of a dedicated project portfolio management tool, TeamDynamix HE (higher education), allowed the division to evolve our processes for developing and evaluating new project requests. Computing Services moved from an annual planning cycle to an ongoing process that allowed us to increase agility in responding to emerging needs, improve the overall quality of project requests, right-size the effort of planning, and balance divisional transparency against
communications overload. The quality of our project requests has improved significantly as a result of increased opportunity for comment and coaching to project leads in a variety of domains, including project management, technical architecture, resource management, and security. The TeamDynamix HE tool has also allowed us to more easily track the status of projects in progress on a monthly basis, allowing for more careful management of our resources and providing additional escalation opportunities as necessary. Our increased maturity in project portfolio management has resulted in fewer projects in the pipeline at any given time, and a greater success ratio for project completion—allowing us to more tightly focus our efforts on the greatest university needs.

3.2.4 Introduced Service Management

Increasingly, divisional strategy and practice revolve around a services-based outlook for all that Computing Services delivers to the campus. In response to this trend, a number of service management activities have been integrated into a more cohesive Service Management Program. Increased attention is focused on identifying what we provide to customers and how, by defining clear deliverables and roles for the ownership and management of each of our services. A growing number of our most important services are now supported by clear Operating Level Agreements detailing expectations for operations and incident management of the service, greatly improving internal communications and responsiveness.

In addition, the PPMO has provided essential assessment consulting and assistance (assessment plans, metrics and surveys) for a number of user-
facing services and projects. PPMO consultation services have been instrumental in the successful assessment of projects including evaluation of software delivery to student computers; the Information Security Office website (www.cmu.edu/iso/); and user file storage, sharing habits and preferences. As some services have achieved a higher level of service management maturity than others, the PPMO assessment consulting service aims to meet service owners “where they are.”

We use the analogy of a division jigsaw puzzle (see Figure 11: Identification of Service Management Needs) to portray the diversity in service management needs from service-to-service. In the following example, Service A may need help with metrics; Service B could benefit from an operating level agreement; Service C needs to optimize workflow; and Service D wants to survey its customers on usage and satisfaction. This approach provides effective, individualized support for service owners as the service management development of the organization grows, ultimately completing the puzzle.

3.3 Revitalized Attention to Division Human Resources (HR) Support

The writer and management consultant, Margaret Wheatley, refers to organizations as having an “organic” nature to them. This is especially true of organizations like the Computing Services division, which is part of a university ecosystem where inter-dependencies among organizations must be leveraged for success. In that spirit, Computing Services has instituted a culture in which modifications of departmental or staff assignments are not uncommon.

Organizational alignment is most effective when it is based on a clear articulation of the organization’s goals and a shared understanding of the strategic initiatives that the organization has planned for achieving those goals. Our first step was to develop and vet our Strategic Plan in 2006. We have reported elsewhere about the early organizational realignments in which the infrastructure and applications resources were repositioned for greater effectiveness and efficiency; we note, for example, that the launch of the Secure Integrated Infrastructure (SII) initiative was a direct outgrowth of that reorganization. This work also had the effect of making Computing Services a truly “merged organization.” In fact — since the coming together of the Administrative Computing and Information Systems (ACIS) unit and the former (“classic”) Computing Services division in 2005 — we no longer consider ourselves “merged” at all; the division's senior leadership balances the good of the whole while leading their own departments as a matter of course.

Carnegie Mellon has embarked on a job study initiative that includes the reclassification of all university staff members. Computing Services used this opportunity to review all position descriptions and, significantly, to lead
the creation of a codified two-career track framework for the entire university that provides full opportunity, recognition, and reward for technologists who are individual contributors rather than future managers. Coupled with a robust annual performance review process and ongoing commitment to supporting professional development of the staff, this framework is used to encourage staff members to try new opportunities in either track, making it as comfortable as possible to experiment with lateral and advancement assignments.

Additionally, the division recently announced the new International Work Assignment Program for Computing Services’ staff members at the Pittsburgh and Qatar campuses. Many global corporations use job rotation amongst their branch offices as a way to develop future leaders, understand local issues, and build a cohesive organization that spans national boundaries. In Computing Services, we are looking to achieve these benefits by extending our work and professional development practices to include assignments on other campuses. We believe that this program will provide staff members with many learning opportunities that are part of an international assignment while allowing them to participate in important projects and exchange best practices with colleagues in other countries.
Since April 2007, all of this has been made possible by the addition of a dedicated human resources manager within Computing Services who works very closely with central HR.

3.4 Improved Internal Communications

In an effort to help Computing Services staff members learn more about the work of the entire division — which had recently expanded to new areas of service — a series of directorate (or departmental) activity reviews (nicknamed “Insights”) were sponsored throughout 2008 and 2009, in which each department presented its work to the division’s leadership. Participants indicated that they learned a lot and were glad to have had the experience. Although the Insights were an excellent “launching point” for the “merged organization,” it was clear that we needed to find more time-efficient ways to share information with each other. Several initiatives were launched to help foster communications across the division.

Informal Communications

The monthly “Bagel Days” was transformed to a series of sessions called “Bagels with Carrie.” By reserving a large conference room for 90 minutes each month, staff members are encouraged to stop by for their bagels, sit down, and chat spontaneously with colleagues and the Associate Vice Provost (formerly the Executive Director). The sessions are rotated between two primary division locations—Cyert Hall and 311 S. Craig Street—to encourage socializing across the entire division. This has proven to be a comfortable environment in which folks raise issues, request appointments, or just have fun. Many insightful conversations about divisional or university programs have emanated from these gatherings and the Associate Vice Provost has the opportunity to hear and learn a lot from colleagues.

The Architecture and Technology Integration department also instituted a monthly program of lunch hour technology transfer sessions presented by technical staff members to expose and encourage discussion of leading-edge work of the non-managerial staff. Some of the topics covered thus far include: networking, the Student Services Suite, Shibboleth authentication, storage and virtualization, data management and storage, metrics and the Information Security Office. These sessions have been well attended and offer an opportunity for staff members within the division to broaden their knowledge on topics they may not be involved with on a regular basis.

Discovery Project for Internal Communications

Per the goal identified in the 2006 Strategic Plan, Computing Services conducted a project to “help us review and improve internal communications.” Building on our efforts between 2006 and 2009, a cross-organizational team interviewed staff members and presented options concerning different types of communications. The feedback offered a sense of the staff’s priorities concerning the kinds of information they seek to learn and the types of venues in which they prefer to receive the information.

In January 2010, the outcome of this project was represented in a communication from the Vice Provost’s Office to the division staff describing practices that have since become standard operating procedure for Computing Services. Practices that were instituted include:

- Quarterly All-Staff Gatherings: All-Staff meetings are now scheduled in the winter and summer, with “Hail and Farewell” events scheduled in the spring and fall. The “Hail and Farewell” events are typically less formal and provide the opportunity to share news
of staff changes with introductions of new colleagues. All of these gatherings are held in a “round-table” format to accommodate a setting for casual interaction. To make this time as informative and useful as possible, each All Staff meeting is prefaced with an invitation to submit questions or areas of interest prior to the event. A process for submitting anonymous requests was developed.

• “Posterless” Poster Sessions: Each of the four all-staff gatherings includes “posterless” poster sessions, in which individuals are available to discuss and describe particular projects or operations of interest. Topics are selected from current project lists and requests from staff to hear more on a particular subject.

• Group Introductions: Each All-Staff Meeting includes a short introduction of a department within Computing Services. As the division grows, it is helpful to associate activities, names and faces.

• Open Office Hours: Staff members are invited to sign up for a confidential half-hour 1:1 conversation with the Vice Provost or Associate Vice Provost, who alternate each month.

Feedback has been very good about these changes and these practices have contributed significantly to our sense of being a division that no longer focuses on “having been merged.” We continue to seek input on an ongoing basis in an effort to meet staff requirements concerning internal communications.

3.5 Common Practices

In late 2009, Computing Services defined 13 common practices to create a more efficient organization with respect to providing services and defining areas of excellence that can be measured in an effective manner. The raw materials for these recommendations were gleaned from focus groups that were conducted with members of the division. Four common practices were selected for immediate focus with the following resulting deliverables.

• Desktop management - The minimum divisional standards for desktop client configuration and management were mandated: eliminating personally identifiable information; maintaining patches and security updates; installing anti-virus software; using strong passwords; and using non-privileged accounts as much as possible.

• Nonfunctional requirements – The core requirements for infrastructure and operational processes and technologies are being embedded in large enterprise projects. For mid-sized projects, standard templates will be developed for infrastructure, security and procurement practices. The original Software as a Service (SaaS) vendor questionnaire is evolving into a standard project requirement.

• Metrics and monitoring – The consolidation of monitoring and measurement of services has three foci. A commercial monitoring application was implemented in 2011 to replace aging in-house systems. Departments developed individual service metrics while the PPMO implemented a service assessment consultation arm. Metrics on productivity and optimum use of institutional resources continue to be defined on a divisional level.

• Divisional document repository – The resources to explore a divisional repository have been made available in fiscal year 2012.

The remaining nine Common Practices are being addressed at departmental levels. Some examples include improved monthly project status reporting, clearer roles and responsibilities for services using Operating Level Agreements (OLAs), and an inventory of exception cases within the Secure Integrated Infrastructure (SII) architecture.
The 2010-11 biennial report closes Computing Services’ work as it relates to the 2006 Strategic Plan. Our next chapter promises to be a time of opportunity, challenge, change, discovery and innovation. As we look to the future, Computing Services’ senior management team has defined goals for the next five years in the 2011 Strategic Plan; the plan is available at http://www.cmu.edu/computing/about/strategic/2011StrategicPlan.pdf.
Carnegie Mellon University
Computing Services
5000 Forbes Avenue
Pittsburgh, PA 15213
412-268-2638
www.cmu.edu/computing/