IT at UC
Governance

Information Security Update
Bo presented the Data Security Compliance Framework Policy in the R&D meeting and will distribute it to this committee when it is ready. OIS is purchasing McAfee Data in Motion. The product will monitor for viruses from the server. UC is purchasing 500 licenses and they will be available by the start of the fall 2014 semester.

The HIPAA training program kick-off will be in August. It will be available via the Canopy portal in Blackboard.

A small task force from the IT Managers committee is forming to review the 90-day password change issue. Though it is not popular, it is mandatory for the College of Medicine for compliance issues. The task force will evaluate all the options for changing the length and complexity of passwords, to incorporating pass phrases, which may allow for longer time-periods between password changes.

SIS Project Update
Gary Grafe, the technical team lead, provided a brief SIS update for the committee**.** He shared high-level milestones with the group and said he would report back monthly to the IT Managers. He will seek their input as the project progresses. The fit gap analysis should be completed by 7/30. The team is trying to avoid customizations and keep the SIS system from having complex upgrades. A detailed project plan will be completed after the Fit Gap process.

IT Architecture Principles
Dom shared the document with the committee. It contains best practices for leveraging IT at the enterprise level. Dom asked all committee members to review and comment before the next meeting. The committee will vote to approve the IT Principles in their August meeting.

Canopy Portal Update
Chris Edwards reported the project phase is complete and is now in the iterative phase. The Marketing and Communications team is working on version 2 of the Canopy landing page. Chris asked the IT Managers to review the portal page and offer feedback to the Canopy team.

Web Conference Task Force Update
Chris said the committee is evaluating multiple products, including Collaborate, using a matrix developed by the team to parcel out the work.

IT Managers Committee Update for IT Council

July 23, 2014

Committee Chair
Dominic Ferreri
Director IT, AFIT
ferrerd@ucmail.uc.edu
(513) 556-1477

Committee Co-Chair
Erma Fritsche
Director IT, UL-IT
fritscej@ucmail.uc.edu
(513) 556-1437

Committee Members
Christian Amann
Bruce Burton
Greg Crase
Jorin Edgerly
Mark Faulkner
William Frigge
Shannon Funk
Yu-Chin Fu
Gary Grafe
Don Hodges
Dale Hofstetter
John Hopkins
John (Jay) Kreimer
Daniel Kuhlmann
John Lawson
Harry LeMaster
Emanuel (Lew) Lewis
Steve Morales
Diana Noelcke
Kent Norton
Megan Pfaltzgraff
Don Rainwater
Aaron Rucker
Benjamin Stockwell
Mel Sweet
Eric Tribbe
Brian Verkamp

UNIVERSITY OF Cincinnati

The task force expects to have a recommendation by October, with the goal of implementing it in spring semester 2015.

Echo360 Pilot Update
Echo was on site and the lecture capture devices will be installed in 22 classrooms the week of 7/21. The infrastructure is already in place and college contacts are in the process of identifying participating faculty. Chris asked for IT Managers to forward faculty names to him for possible participants in the pilot.

Box- Enterprise Storage
Don Rainwater provided an update for the committee. The Isilon, enterprise storage is installed, testing and data migration have begun. Box personal storage will be available by mid-August. Both service will be available in the UCIT Service Catalog along with appropriate request forms. Users should contact the UCIT Integrated Help Desk for assistance when the services go live. The Marketing and Communications team will feature the services in the Canopy ecosystem bi-weekly newsletter.

Data Center Task Force
Dom provided a brief update on the status of the Data Center developments.

IT Managers Monthly Meeting Topics
Dom reviewed upcoming topics he and Erma plan to address in future meetings and asked the committee to make suggestions for future agenda items as well. Dom's list included:

- Institutional Repository- what it is and what it means for UC
- Digital Signage Update
- Services Desk Update
- Managed Printing Update – outsourcing to outside business; raising prices to 10 c per copy and no free printing for students.
- Virtual Desktop
- Dell Update- UC lost the Dell rep to EMC. New Dell rep will be in later this month. Is there a need for an onsite Dell technician?

What Have You Heard?

- Some of the faculty are still trying to use Collaborate for fall. Formal communication did go out to inform them the Collaborate license is expired. Fall sessions should use Lync

- Kaltura is meeting with UC today. The plan is to launch as an enterprise video streaming tool. The tools will have to be reconciled with the Echo360 and build recommendation on when to use what tool based on what you're trying to do

- Tim was alerted by SnagIt- there's enough UC purchases to leverage a cost decrease. Do we need a UC license for SnagIT? Kaltura will replace screen capture tool. Windows 7 has free snippet tools.

- Turning Point- They have a cloud service. CoN is still using Turning Point for fall semester. They replaced a classroom computer. Turning Point is stored locally and can't migrate data to the cloud, which means loss of data if the computer dies. iClick, is another free options on campus.

- There is a problem with the UC Dell catalog that surfaced after the last update. After ordering parts and navigating back to the catalog section, the browser goes back to the general Dell catalog and not the UC catalog of products. Also, Dell delivery is very slow – it takes 4-5 weeks for delivery of a laptop if you order any enhancement or options other than their standard offer. Monitor delivery is slow as well. Dell claims if UC uses a standard Dell configuration, they are prebuilt and staged around the country for two-day shipping. We have one year left on the UC contract. UC will look at other vendors for shipping service and quality. All agreed that the Dell rep has become slow to respond, it takes 4-6 weeks. Dell is not delivering the product per SLA. The consensus was that CDW is more responsive in ordering, and on call backs. Dom will touch base with Purchasing to find out the options going forward. Next month the committee will discuss again what is wrong with the relationship with Dell.

UNIVERSITY OF Cincinnati

IT Architecture Principles

Core Services and Shared Infrastructure Committee

July 1, 2014

IT Architecture Principles are the general rules and guidelines that inform and support the way in which the University of Cincinnati sets about fulfilling its mission.

Purpose

These IT Architecture Principles establish a common set of guiding principles across the University of Cincinnati that embody the spirit and thinking of enterprise IT architecture and recognizes the efficiency of sharing resources to maximize the University's overall capabilities

Contents

Definitions

Academic Mission – the primary mission of the university is the generation and dissemination of knowledge

Business – In the context of the University of Cincinnati, Business refers to the delivery of the academic mission of Teaching, Research, Scholarship and Service

Data - factual information (as measurements, statistics, imagery, written texts, audio recording, etc.) used as a basis for reasoning, discussion, calculation, etc.

Business expert – A person who understands the complexities and operational procedures of a particular functional unit within the University.

Technology blueprint – A comprehensive plan that guides the implementation of strategic planning initiatives for the future state of technology and IT across the campus.

Governance Council – The IT Council is the university governance committee chaired by the CIO and advisory to the CIO

IT Domain – The overall sphere of responsibilities addressed by the IT delivery team on campus. This includes the following specific realms defined below;

Business Architecture – A description of the structure and interaction between the business strategy, organization, functions, business processes, and information needs.

Data Architecture – A description of the structure and interaction of the UC's major types and sources of data, logical data assets, physical data assets, and data management resources

Application Architecture – A description of the structure and interaction of the applications as groups of capabilities that provide key business functions and manage the data assets.

Technology Architecture – A description of the structure and interaction of the platform services, and logical and physical technology components.

Business Core Services – The fundamental services necessary to support the delivery of the academic mission of the University (eg. Registration, Payroll, Course Content Management, Grading, Degree Audit, etc.)

Service Level - measures the performance of a system. Certain goals are defined and the service level gives the percentage to which those goals should be achieved.

Intellectual Property- Intellectual property (IP) refers to creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names and images used in commerce.

Enterprise Data Architect – A senior level University administrator who oversees all University core data and the work of the University's Data Trustees.

Data Stewards - are defined as individuals assigned by and accountable to the Data Trustees. Data Stewards help define, implement, and enforce data management policies and procedures within their specific Subject Area and Business Domains, as defined in the Data Map provides a description of each business domain, the business processes handled by that business domain, and who the Data Custodian and Data Trustee is for each business area.

Data Custodians - perform several key data management functions including:

- Identifying Systems of Record containing Institutional Data
- Categorizing Institutional Data within Systems of Record according to security and privacy guidelines
- Defining access, quality and usage guidelines for Institutional Data
- Reviewing and approving requests for access to Institutional Data
- Documenting and maintaining Institutional Metadata
- Educating and sharing best practices with other data management personnel

Data Trustee - are defined as institutional officers, (i.e. Vice Presidents, Vice Provosts, Deans, Chancellors, etc.) who are appointed by the President or Provost, and have authority over policies and procedures regarding business definitions of data, and the access and usage of that data, within their delegations of authority.

Metadata – is "data about data" For example, a photograph may have metadata that captures when and where a photo was taken, the camera that captured it, the speed and aperture settings of the camera that captured the photo etc.

Technology platform - is a term for technology that enables the creation of products and processes that support present or future or past development. It establishes the long-term capabilities of research & development institutes. It can be defined as a structural or technological form from which various products can emerge without the expense of a new process/technology introduction.

Interoperability - is the ability of making systems and organizations work together (inter-operate) In the context of the University it may refer to inter-operation between Apple and Windows operating systems or between one application/software implementation and another.

Business Principles

Principle 1: Primacy of Principles

Statement:

These principles of information management apply to all organizations within the University.

Rationale:

The only way we can provide a consistent and measurable level of quality information to decision-makers is if all organizations abide by the principles.

Implications:

- Without this principle discrimination, favoritism, and inconsistency would rapidly undermine the management of information.
- Information management initiatives will not begin until they are examined for compliance with the principles.
- A conflict with a principle will be resolved by changing the framework of the initiative.

Principle 2: Maximize Benefit to the University

Statement:

Information management decisions are made to provide maximum benefit to the University as a whole.

Rationale:

This principle embodies "service above self". Decisions made from a university-wide perspective have greater long-term value than decisions made from any particular organizational perspective. No smaller group will detract from the benefit of the whole. However, this principle will not preclude any smaller group from getting its job done.

Implications:

- Achieving maximum university-wide benefit will require changes in the way information is planned and managed. Technology alone will not bring about this change.
- Some organizations may have to concede their own preferences for the greater benefit of the University.
- Application development priorities must be established by the entire University for the entire University.
- Application components should be shared across organizational boundaries.
- Information management initiatives should be conducted in accordance with the University's strategic plan. Individual organizations should pursue information management initiatives

which conform to the blueprints and priorities established by the University. The Enterprise Architecture Committee will propose changes to the plan as needed with final approval granted by the IT Governance Council.
- As needs arise, priorities must be adjusted. The IT Governance Council with comprehensive University representation should make these adjustments.

Principle 3: Information Management is Everybody's Business

Statement:

All organizations in the University will participate in information management decisions needed to accomplish the academic mission of the University.

Rationale:

UC faculty/staff/students are the key stakeholders of information and the application of technology to address Business needs. In order to ensure information management is aligned with business, all organizations in the university must be involved in all aspects of the information environment. Business experts from across the University, and the technical staff responsible for developing and sustaining the information environment need to come together as a team to jointly define the goals and objectives of IT.

Implications:

- To operate as a team, every UC faculty/staff/student will need to accept responsibility for developing the information environment.
- Commitment of resources will be required to implement this principle.

Principle 4: Business Continuity

Statement:

University operations are maintained in spite of system interruptions.

Rationale:

As University systems and operations become more pervasive, we become more dependent on them; therefore, we must consider the reliability of such systems throughout their design and use. Business premises throughout the enterprise must be provided with the capability to continue their business functions regardless of external events. Hardware failure, natural disasters, and data corruption should not be allowed to disrupt or stop enterprise activities. The University's business functions must be capable of operating on alternative information delivery mechanisms.

Implications:

- Dependency on shared system applications mandates that the risks of business interruption must be established in advance and managed. Management includes but is not limited to periodic reviews, testing for vulnerability and exposure, and designing mission-critical services to assure business function continuity through redundant or alternative capabilities.
- Recoverability, redundancy, and maintainability should be addressed at the time of design.
- Applications must be assessed for criticality and impact on the University mission, in order to determine what level of continuity is required and what corresponding recovery plan is necessary.

Principle 5: Common Use Applications

Statement:

Development of applications used across the University is preferred over the development of similar or duplicative applications which are only provided to a particular organization.

Rationale:

Duplicative capability is expensive and proliferates conflicting data.

Implications:

- Organizations will not be allowed to develop systems and tools for their own use which are similar to or duplicative of university-wide systems and tools. In this way, expenditures of scarce resources to develop essentially the same capability in marginally different ways will be reduced.
- Data and information used to support university decision-making will be standardized to a much greater extent than previously. This is because the smaller organizational systems and tools which produced different data (which was not shared among other organizations) will be replaced by university-wide systems and tools. The impetus for adding to the set of university-wide systems and tools may well come from an organization making a convincing case for the value of the data/information previously produced by its organizational system or tool, but the resulting system or tool will become part of the University-wide system, and the data it produces will be shared across the University.

Principle 6: Compliance with Law

Statement:

University information management processes will comply with all relevant laws, policies, and regulations.

Rationale:

University policy is to abide by laws, policies, and regulations. This will not preclude business process improvements that lead to changes in policies and regulations.

Implications:

- The University must be mindful to comply with laws, regulations, and external policies regarding the collection, retention, and management of data.
- Changes in the law and changes in regulations may drive changes in our processes or applications.

Principle 7: Responsibility of Information Technology at UC

Statement:

The University's Information Technology team, including central University IT staff and unit level IT staff, is responsible for owning and implementing IT processes and infrastructure that enable solutions to meet user-defined requirements for functionality, service levels, cost, and delivery timing.

Rationale:

Create cost-effective projects with clear university benefits by aligning expectations of UC faculty/staff/students with technical capabilities and actual costs.

Implications:

- A process must be created to prioritize projects.
- The University's Information Technology Team must define processes to manage business unit expectations.
- Data, application, and technology models must be created to enable integrated quality solutions and to maximize results.

Principle 8: Protection of Intellectual Property

Statement:

The University's Intellectual Property (IP) must be protected. This protection must be reflected in the IT architecture, implementation, and governance processes.

Rationale:

A major part of the University's IP is hosted in the IT domain (Information/Data Architecture, Business Architecture, Application Architecture, and Technology Architecture).

Implications:

- While protection of IP assets is everybody's business, much of the actual protection is implemented in the IT domain. Even trust in non-IT processes can be managed by IT processes (email, mandatory notes, etc.).
- Security policies will be required that can substantially improve protection of IP. This must be capable of both avoiding compromises and reducing liabilities.

Data Principles

Principle 9: Data is an Asset

Statement:

Data is an asset that has value to the university and is managed accordingly.

Rationale:

Data is a valuable university resource; it has real, measurable value. In simple terms, the purpose of data is to aid decision-making. Accurate, timely data is critical to accurate, timely decisions. Most university assets are carefully managed, and data is no exception. Data is the foundation of our decision-making, so it must be carefully managed to ensure that we know where it is, can rely upon its accuracy, and can obtain it when and where we need it.

Implications:

- This is one of three closely-related principles regarding data: data is an asset; data may be shared; and data is easily accessible. The implication is that there is an education task to ensure that all organizations within the university understand the relationship between value of data, sharing of data, and accessibility to data.
- Data Stewards must have the authority and means to manage the data for which they are accountable.
- We must make the cultural transition from only "data trustee" thinking to include "data stewardship" thinking.
- The role of data steward is critical because obsolete, incorrect, or inconsistent data could be passed to University personnel and adversely affect decisions across the University.
- Part of the role of the Data Steward, is to ensure data quality. Procedures must be developed and used to prevent and correct errors in the information and to improve those processes that produce flawed information. Data quality will need to be measured and steps taken to improve data quality - it is probable that policy and procedures will need to be developed for this as well.
- The IT Governance Council with comprehensive University-wide representation (including the current Data Trustees, i.e., university administrators at the vice presidential level who bear the ultimate responsibility) should decide on process changes suggested by the Data Steward.
- Since data is an asset of value to the entire University, Data Stewards accountable for properly managing the data must be assigned at the enterprise level.

Principle 10: Data is Shared

Statement:

Users have access to the data necessary to perform their duties; therefore, data is shared across University functions and organizations.

Rationale:

Timely access to accurate data is essential to improving the quality and efficiency of university decision-making. It is less costly to maintain timely, accurate data in a single data store, and then share it, than it is to maintain duplicative data in multiple locations. The university holds a wealth of data, but it is stored in hundreds of incompatible stovepipe databases. The speed of data collection, creation, transfer, and assimilation is driven by the ability of the organization to efficiently share these islands of data across the organization.

Shared data will result in improved decisions since we will rely on fewer (ultimately one virtual) sources of more accurate and timely managed data for all of our decision-making. Electronically-shared data will result in increased efficiency when existing data entities can be used, without re-keying, to create new entities.

Implications:

- This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an educational task to ensure that all organizations within the University understand the relationship between value of data, sharing of data, and accessibility to data.
- To enable data sharing a common set of policies, procedures, and standards governing data management and secure access must be developed, both for the short and long terms.
- For the short term, to preserve our significant investment in legacy systems, we must invest in software capable of migrating legacy system data into a shared data environment.
- We will also need to develop standard data models, data elements, and other metadata that defines this shared environment and develop a repository system for storing this metadata to make it accessible.
- For the long term, as legacy systems are replaced, we must adopt and enforce common data access policies and guidelines for new application developers to ensure that data in new applications remains available to the shared environment and that data in the shared environment can continue to be used by the new applications.
- For both the short term and the long term we must adopt common methods and tools for creating, maintaining, and accessing the data shared across the university.
- Data sharing will require a significant cultural change.
- Data sharing and data security are equally important. Under no circumstances will the data sharing principle cause confidential data to be compromised.

- Data made available for sharing will be relied upon by all users to execute their respective tasks. This will ensure that only the most accurate and timely data is relied upon for decision-making. Shared data will become the university-wide "virtual single source" of data.

Principle 11: Data is Accessible

Statement:

Data is accessible for users to perform their functions.

Rationale:

Wide access to data leads to efficiency and effectiveness in decision-making, and affords timely response to information requests and service delivery. How information is incorporated into business and academic functions must be considered from an enterprise perspective to allow appropriate access by a wide variety of users. Staff time is saved and consistency of data is improved.

Implications:

- This is one of three closely-related principles regarding data: data is an asset; data is shared; and data is easily accessible. The implication is that there is an education task to ensure that all organizations within the University understand the relationship between value of data, sharing of data, and accessibility to data.
- Accessibility involves the ease with which users obtain information.
- The way information is accessed and displayed must be sufficiently adaptable to meet a wide range of university users and their corresponding methods of access.
- Access to data does not constitute understanding of the data. Personnel should take caution not to misinterpret information.
- Access to data does not necessarily grant the user access rights to modify or disclose the data. This will require an education process and a change in the organizational culture, which currently supports a belief in "ownership" of data by functional units.

Principle 12: Data Trustee

Statement:

Each element of data has a Trustee accountable for data quality.

Rationale:

One of the benefits of an architected environment is the ability to share data (e.g., text, video, sound, etc.) across the university. As the degree of data sharing grows and business units rely upon common information, it becomes essential that only a Data Trustee makes decisions about

the content of data. Since data can lose its integrity when it is entered multiple times, the data trustee will have sole responsibility for data entry, which eliminates redundant human effort and data storage resources.

Note:

A trustee is different than a steward - a Trustee has authority over policies and procedures regarding business definitions of data, and the access and usage of that data, within their delegations of authority; however, responsibilities of a steward include defining, implementing, and enforcing data management policies and procedures within their specific Subject Area and Business Domains.

Implications:

- Real trusteeship dissolves the data "ownership" issues and allows the data to be available to meet all users' needs. This implies that a cultural change from data "ownership" to data "trusteeship" may be required.
- The Data Trustee will be responsible for meeting quality requirements levied upon the data for which the trustee is accountable.
- It is essential that the Trustee has the ability to provide user confidence in the data based upon attributes such as "data source".
- It is essential that the Trustee is able to identify the true source of the data. This does not mean that classified sources will be revealed nor does it mean the source will be the Trustee.
- Information should be captured electronically once and immediately validated as close to the source as possible. Quality control measures must be implemented to ensure the integrity of the data.
- As a result of sharing data across the university, the Trustee is accountable and responsible for the accuracy and currency of their designated data element(s) and, concurrently, must recognize the importance of this trusteeship responsibility.

Principle 13: Common Terminology and Definitions of Data Attributes

Statement:

Data terminology and attributes are defined consistently throughout the university, and the definitions are understandable and available to all users.

Rationale:

The data that will be used in the development of applications must have a common definition throughout the university to enable sharing of data. A common vocabulary will facilitate communications and enable dialogue to be effective. In addition, it is required to interface systems and exchange data.

Implications:

- We are lulled into thinking that this issue is adequately addressed because there are people with "database administration" job titles and forums with charters implying responsibility. Significant additional energy and resources must be committed to this task. It is key to the success of efforts to improve the information environment. This is separate from but related to the issue of data element definition, which is addressed by a broad community - this is more like a common vocabulary and definition.
- The University must establish the initial common vocabulary for the institution. The definitions will be used uniformly throughout the university.
- Whenever a new data definition is required, the definition effort will be coordinated and reconciled with the University "glossary" of data descriptions. The Enterprise Data Architect will provide this coordination.
- Ambiguities resulting from multiple parochial definitions of data must give way to accepted University-wide definitions and understanding.
- Multiple data standardization initiatives need to be coordinated.
- Functional database administration responsibilities must be determined and assigned to the Data Trustees by the Enterprise Data Architect.

Principle 14: Data Security

Statement:

Data must be protected from unauthorized use and disclosure. In addition this includes, but is not limited to, protection of pre-decisional, sensitive, source selection-sensitive, and proprietary information.

Rationale:

Open sharing of information and the release of information via relevant legislation must be balanced against the need to restrict the availability of classified, proprietary, and sensitive information.

Existing laws and regulations require the safeguarding the privacy of data, while permitting free and open access. Pre-decisional information (work-in-progress, drafts, etc.) must be protected to avoid unwarranted speculation, misinterpretation, and inappropriate use.

Implications:

- Aggregation of data, both classified and not, will create a large target requiring review and de-classification procedures to maintain appropriate control. Data stewards and/or functional users must determine whether the aggregation results in an increased classification level. We will continue to rely on appropriate policy and procedures to handle this review and de-classification. Access to information based on a need-to-know policy will force regular reviews of the body of information.
- In order to adequately provide access to open information while maintaining secure information, security needs must be identified and developed at the data level, not the application level.

- Data security safeguards can be put in place to restrict access to "view only", or "never see". Sensitivity labeling for access to pre-decisional, decisional, classified, sensitive, or proprietary information must be determined.
- Security must be designed into data elements from the beginning; it cannot be added later. Systems, data, and technologies must be protected from unauthorized access and manipulation. University information must be safeguarded against inadvertent or unauthorized alteration, sabotage, disaster, or disclosure.
- The University needs new policies on managing duration of protection for pre-decisional information and other works-in-progress, in consideration of content freshness.

Application Principles

Principle 15: Technology Independence

Statement:

Applications are independent of specific technology choices and therefore can operate on a variety of technology platforms.

Rationale:

Independence of applications from the underlying technology allows applications to be developed, upgraded, and operated in the most cost-effective and timely way. Otherwise technology, which is subject to continual obsolescence and vendor dependence rather than user requirements, becomes the driver.

Realizing that every decision made with respect to IT makes us dependent on that technology, the intent of this principle is to ensure that Application Software is not dependent on specific hardware and operating systems software.

Implications:

- This principle will require standards that support portability.
- For Commercial Off-The-Shelf (COTS) solutions there may be limited choices currently, as many of these applications are technology and platform-dependent.
- Application Program Interfaces (APIs) will need to be developed to enable legacy applications to interoperate with applications and operating environments developed under the enterprise architecture.
- Middleware should be used to decouple applications from specific software solutions. As an example, this principle could lead to use of web services like SOAP and Representational State Transfer (REST), give a high degree of priority to platform-independence.

Principle 16: Ease-of-Use

Statement:

Applications are easy to use. The underlying technology is transparent to users, so they can concentrate on tasks at hand.

Rationale:

The more a user has to understand the underlying technology, the less productive that user is. Ease-of-use is a positive incentive for use of applications. It encourages users to work within the integrated information environment instead of developing isolated systems to accomplish the task outside of the university's integrated information environment. Most of the knowledge required to operate one system will be similar to others. Training is kept to a minimum, and the risk of using a system improperly is low.

Using an unfamiliar application should be as intuitive as driving a different car.

Implications:

- Applications will be required to have a common "look and feel" and support ergonomic requirements. Hence, the common look and feel standard must be designed and usability test criteria must be developed.
- Guidelines for user interfaces should not be constrained by narrow assumptions about user location, language, systems training, or physical capability. Factors such as linguistics, physical infirmities of UC faculty/staff/students (visual acuity, ability to use keyboard/mouse), and proficiency in the use of technology have broad ramifications in determining the ease-of-use of an application.

Technology Principles

Principle 17: Requirements-Based Change

Statement:

Changes are made to applications and technology only in response to improving the delivery of the academic mission of the University.

Rationale:

This principle will foster an atmosphere where the information environment changes in response to the needs of the business, rather than having the business change in response to IT changes. This is to ensure that the purpose of the information support - the transaction of business - is the

basis for any proposed change. Unintended effects on business due to IT changes will be minimized. A change in technology may provide an opportunity to improve the business process and, hence, change business needs.

Implications:

- Changes in implementation will follow full examination of the proposed changes using the enterprise architecture.
- Technical improvements or system developments are not funded unless a documented business need exists.
- Change management processes conforming to this principle will be developed and implemented.
- This principle may bump up against the responsive change management principle. We must ensure the requirements documentation process does not hinder responsive change to meet legitimate business needs. The purpose of this principle is to keep us focused on business, not technology needs - responsive change is also a business need.

Principle 18: Responsive Change Management

Statement:

Changes to the enterprise information environment are implemented in a timely manner.

Rationale:

If people are to be expected to work within the enterprise information environment, that information environment must be responsive to their needs.

Implications:

- We have to develop processes for managing and implementing change that do not create delays.
- A user who feels a need for change will need to connect with a "business expert" to facilitate explanation and implementation of that need.
- If we are going to make changes, we must keep the architectures uniformly updated.
- Adopting this principle might require additional resources to ensure timely compliance..

Principle 19: Control Technical Diversity

Statement:

Technological diversity is controlled to minimize the non-trivial cost of maintaining expertise in and connectivity between multiple processing environments.

Rationale:

There is a real, non-trivial cost of infrastructure required to support alternative technologies for processing environments. There are further infrastructure costs incurred to keep multiple systems interconnected and maintained.

Limiting the number of supported components will simplify maintainability and reduce costs.

The business advantages of minimum technical diversity include: standard packaging of components; predictable implementation impact; predictable valuations and returns; redefined testing; utility status; and increased flexibility to accommodate technological advancements. Common technology across the enterprise brings the benefits of economies of scale to the university. Technical administration and support costs are better controlled when limited resources can focus on this shared set of technology.

Implications:

- Policies, standards, and procedures that govern acquisition of technology must be tied directly to this principle.
- Technology choices will be constrained by the choices available within the technology blueprint. Procedures for augmenting the acceptable technology set to meet evolving requirements will have to be developed and emplaced.
- We are not freezing our technology baseline. We welcome technological advances and will change the technology blueprint when compatibility with the current infrastructure, improvement in operational efficiency, or a required capability has been demonstrated.

Principle 20: Interoperability

Statement:

Software and hardware should conform to defined standards that promote interoperability for data, applications, and technology.

Rationale:

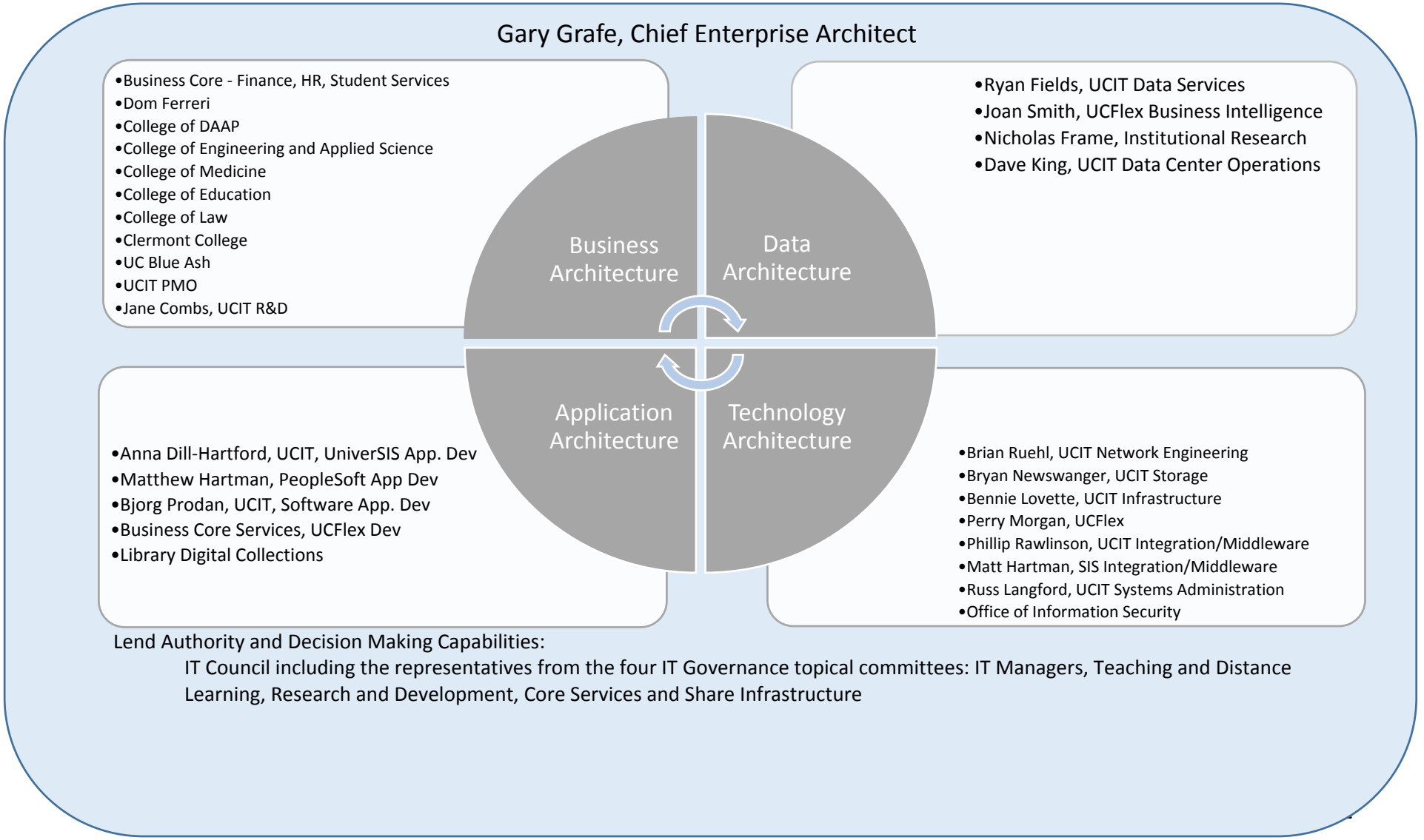
Standards help ensure consistency, thus improving the ability to manage systems, improve user satisfaction, and protect existing IT investments, thus maximizing return on investment and reducing costs. Standards for interoperability additionally help ensure support from multiple vendors for their products, and facilitate integration.

Implications:

- Interoperability standards and industry standards will be followed unless there is a compelling business reason to implement a non-standard solution.
- A process for setting standards, reviewing and revising them periodically, and granting exceptions must be established.

- The existing IT platforms must be identified and documented.

Appendix A: Enterprise Architecture Committee



Appendix B: Enterprise IT Architecture principles, directional statements, and standards

Principles embody the overall philosophy of the institution. They will be the vision aligned with the institution's mission. These principles will help enterprise architecture to focus on what is important.

Directional Statements are derived from the principles and will help Enterprise Architecture provide the roadmap.

Architecture Standards provide a way to turn principles and directional statements into actionable items encompassing specific technology requirements.