



MAIS Technical Architecture Team Findings

DRAFT #1

April, 2006



Introduction

Introduction

Strategic Plan Definition and Objectives

- **A strategic plan defines goals and actions to be taken over a period of time to accomplish longer range business objectives.**
 - For purposes of this plan the term “strategic plan” is used to encompass a set of strategies for positioning the MAIS technology infrastructure such that it will accommodate and support the future technology plans of our various IT customers, in the most efficient and effective manner possible, and be compatible with industry directions, trends and best practices.
- **The Objectives of this Technology Strategic Planning Project Are:**
 - Review our business priorities and identify the implications of addressing these from a technology infrastructure perspective
 - Assess the current state of the management areas which include technology infrastructure
 - Recommend strategies based on the state of our current environment and industry best practices
 - Gain consensus on recommended strategies

Introduction

Technology Infrastructure Areas Addressed

- The shared technology infrastructure, applications and technology program areas to be reviewed are organized into the following major architecture domains:
 - Application Development Platforms
 - Database Management
 - Disaster Recovery
 - Middleware
 - Network Management
 - Security
 - Server Hardware & Operating System
 - Storage Management
 - Systems Management



Application Development Platforms

Application Development Platforms

Findings – Current State

- **Application development is done primarily in proprietary languages**
 - PeopleTools and ClickCommerce tools are used for most customization and configuration activities
 - Java is used for some narrow set of applications (e.g. OUD web applications, Gateway)
 - .Net used in eResearch primarily by vendor today
- **Number of development environments is limited**
 - Development and Infrastructure teams gain flexibility through additional environments. Infrastructure teams lose efficiency with more environments. Organization has reached an equilibrium (compromise) on the number of environments for most applications.
- **Developers adopt some tools based on individual preferences**
 - Comparative technical evaluation of developer productivity tools rarely happens. Usually developer productivity tools are selected based on the experience of one or more developers.

Application Development Platforms

Findings – Current State

- **Production and testing environments are not identical**
 - Due to cost constraints Test and Development environments do not have identical HW as production.
- **Few automated testing tools exist**
 - Load testing software is available, but regression testing and system testing software is not available, so these activities are performed manually.
- **STAT! is our primary version control tool**
 - STAT! is designed for use with PeopleSoft, but leveraged with other applications as well

Application Development Platforms

Findings – Emerging Trends

- **Application development will shift to Java and .Net**
 - Vendor directions and internal priorities will result in the shift away from proprietary languages to Java and .Net (C#).
- **.Net development will grow rapidly in 2006**
 - The Business Intelligence Web Reporting Project will drive the deployment of a complete development environment and services in 2006.
 - This environment will be completely based on .Net products
 - eResearch development in .Net will grow in 2006
- **Competitive pressures may force us to implement bolt-on technologies to extend the life of our legacy PeopleSoft Applications**
 - Application technologies will continue to change quickly in the upcoming years, but most University systems will continue to be based on PeopleTools technology from 2003. Expectations of students and staff may drive us to put alternative front-ends on these obsolete technologies, much like the University did with the mainframe in the late 1990's.
- **Charging model will not change**
 - We will continue to develop applications and infrastructure under a “General Fund” design principle
 - No infrastructure or application changes will need to occur to support charge back

Application Development Platforms

Issues

- **We are not familiar nor skilled in the major potential Tool Frameworks at the present time**
 - Training will be required for infrastructure providers and for application developers
- **Timeline for Tool selection process and development environment remains unclear**
 - We'd like to choose a tool set as soon as possible, but selection of a tool set will likely tie us into an application vendor before all the facts about the vendor products are known
- **How do we handle version control in these new environments?**
 - All the operational processes that we have today will need to be redesigned, and new technologies will need to be used
- **Services introduce new system management complexities**
 - A shift from RDBMS based to a SOA based development approach will require work to define a common XML based schema
 - Data management and administration will be needed to support services, much like they were to support the shift to relational databases

Application Development Platforms

Industry Insight / Trends

- **Large ERP vendors are moving to Java as main development tool**
 - Declarative interfaces will be introduced by vendors to simplify development
- **.Net will grow in usage at departmental level**
 - Many University units are committed to a Microsoft infrastructure and usage of .Net in these units is likely
- **Next generation IDE's will be more declarative and will begin to lower the expertise necessary to build applications**
 - These enhanced environments will evolve over the next several years, so short-term development efforts will still require considerable expertise and programming knowledge to succeed
- **Services will change the nature of programming**
 - The emergence of services will require new approach to application design

Application Development Platforms

Industry Insight / Trends

- **Use of Meta Data Repository could become more prevalent**
 - We are not sure exactly how this will play out in the future, but it is possible that meta data will be shared across systems, or at least be leveraged by in a proprietary fashion by vendors
- **Process orchestration tools will become more prevalent**
 - Process flow and orchestration will become part of development tool set
 - Use of these tools may shift from development teams to business teams
- **Applications delivered as services will alter the development landscape**
 - Today's environment: Less development with some applications delivered as "Applications as a service"
 - Future environment: Components of applications will be developed or bought as discrete services

Application Development Platforms

Strategic Recommendations

■ Understand containment strategy for PeopleSoft

- ❑ We need to establish an approach for how or if we will contain the use of PeopleTools in the future
- ❑ We could choose to implement bolt-on technologies to avoid PeopleTools coding
- ❑ Establish a timeline in conjunction with the containment strategy to minimize investment in PeopleSoft Application Development and invest as much money in our next Application Development Platform as soon as possible

■ Make decision regarding platform choice for Java development

- ❑ Some time in the next 1-2 years MAIS will need to commit to a primary development tools provider (e.g. open source, Oracle, IBM). The timeline will likely be driven by the selection of the DAC replacement product, and our strategy for containment of PeopleTools.
- ❑ As part of this selection we will need to research potential development tools, utilities and supporting infrastructure (e.g. version control)
- ❑ .Net tools will also need to be selected, although Microsoft-provided tools will be default

Application Development Platforms

Strategic Recommendations

- **Align middleware and application tool selection timelines**
 - Application development platform needs to be chosen as late as possible, but before it is needed to support development projects
- **Explore pilot opportunities**
 - Try to gain experience with tools sets, application platforms and services through pilot projects like the development of Web Reporting system.
- **Adopt the approach of “Where we can, design new applications as services. Where we have existing legacy applications, wrap code and deliver as services.”**
 - The appropriate service interfaces may lower the need for system replacement in some cases
- **Establish goals and vision for testing tools**
 - Determine if we want to embrace regression testing tools. Determine if we should alter our approach to load and stress testing in any way.
- **Begin to leverage new reporting tools**
 - Business Intelligence projects will result in the use of a different set of reporting tools than are used today. Timeline for shifting to these new tools needs to be established.



Database Management

Database Management

Findings

- **We manage a heterogeneous mix of database platforms**
 - We have 50 databases at Oracle 9i, 2 databases at Oracle 10gR2 and 2 databases at 8i due to application requirements
 - We currently have about 61 MS SQL Server 2000 database instances
 - We support IMS v7 and DB2 v7 on the Mainframe
 - Additionally, there are several instances of DB2 databases embedded in applications such as in the storage architecture and TSM
 - We also have at least one instance of MySQL (Vista Plus) although this is not managed directly as the application presents this as a “black box”
- **Oracle binaries are not standard across servers today by design**

Database Management

Issues

■ **Current database architecture does not support high availability**

- ❑ The current non-redundant / non-High Availability design of the Database architecture layer does not position us to meet future MAIS availability goals (Oracle & SQL Server)
- ❑ We have not implemented Oracle Hot Backups (we do hot backups for SQL Server)

■ **Database administration efficiencies**

- ❑ Managing an environment with such a heterogeneous DB mix leads to operational inefficiencies
- ❑ Oracle Enterprise Manager (OEM) is not utilized consistently and to its full extent
- ❑ Proliferation of full sized Databases
- ❑ Our occupancy rate for Oracle Databases is not at targeted levels and other Database platforms do not have targets established
- ❑ Internal Databases (MySQL, DB2) are not managed/reviewed by the DBA Group

Database Management

Issues

- **Database platform selection for applications is unclear**
 - We don't have a framework to strategically determine what DB platform to use when an application supports both Oracle and MS SQL Server
- **The current DW extract process / approach will not meet web reporting currency of data requirements**
- **The frequency and impact of patch applications are currently an issue that impact system availability, consume resources and contribute to operational inefficiencies**
- **Database security**
 - Audits of permissions granted to individual ID's does not occur
 - Vendor SW arrives w/ inappropriate application account privileges established

Database Management

Industry Insight / Trends

■ New database technologies

- ❑ In Memory Databases to support applications with special performance needs
- ❑ XML Databases (to support integrated XML)
- ❑ Self-managing / Autonomic Databases
- ❑ Continuous Data Protection (up to the minute recovery capabilities)

■ Open source becoming more prevalent

- ❑ Oracle's stated direction is RAC on commodity-based HW running Open Source OS (Linux)
- ❑ MySQL is likely to grow into an enterprise caliber database in the next few years

■ DBA's need to become more multi-DB skill proficient

- ❑ Most DBAs are skilled in one vendor database and its proprietary tool set

■ Automatic Storage Management by the DB Platform rather than the OS

- ❑ Competition between database vendors and storage vendors to control the allocation and management of storage

■ Standby DB's for rolling upgrades (no or minimal upgrade outages)

Database Management

Strategic Recommendations

■ Improve Database availability

- ❑ Research and investigate potential architecture redundancy and availability approaches – Oracle Real Application Clusters (RAC), Stand-By Databases, etc.
- ❑ Investigate tools for automated patch application
- ❑ Establish more robust backup and recovery management
- ❑ Select and implement an ETL / Change Capture tool to address the Data Warehouse population and data currency needs

■ Improve toolset for database administration

- ❑ Investigate implementing a cross-platform Database Management tool to increase operational efficiencies and counteract efficiency loss of heterogeneous DB environment
- ❑ Investigate tools to automate or simplify database management and support
- ❑ Leverage Oracle Enterprise Manager and/or other tools more effectively

■ Continue to support Oracle and MS SQL Server as our only DB Platforms for new applications

- ❑ As open source solutions become more mature, investigate them for potential adoption as a supported DB platform

Database Management

Strategic Recommendations

■ Adopt procedures and policies to gain efficiencies and reduce costs

- ❑ Establish a formal Information Lifecycle Management (ILM) policy / approach across MAIS
- ❑ Retire z/OS based IMS / DB2 reliant applications in order to retire support for these DB platforms on z/OS
- ❑ Establish target occupancy rates for all Database environments
- ❑ Evaluate the ongoing need and requirements for separate ODS environments from Production OLTP
- ❑ Establish a policy and review process for new database requests
 - Determine the base set of environments that will be needed (e.g. Development, Test, Stress, Prod, Shakedown) and process for altering the list
- ❑ Transfer management responsibilities for SW applications with internal DB's to the DBA Group



Disaster Recovery

Disaster Recovery

Findings

- **Current Disaster Recovery approach utilizes external DR vendor SunGard**
 - Offsite Tape based Recovery Approach
 - Recovery Time Objective: 2-5 day recovery window
 - Recovery Point Objective: Maximum of 1 day of data loss
- **Testing at SunGard has been suspended in order to focus resources on completion of Arbor Lakes Parallel Machine Room occupancy**
 - We have successfully tested recovery at SunGard several times and are confident in current DR procedures
- **With the implementation of the AL Parallel Machine Room, we are planning to implement an internal DR approach after completion of transition to new data center**
 - First test of new approach in first quarter of FY2007
- **MAIS is the University leader in DR**
 - MAIS provides staffing support to ITCS, but ITCS has not yet developed complete solution
 - Units on campus are interested in MAIS providing DR capabilities which they can leverage

Disaster Recovery

Issues

- **New DR Plan to leverage new data center is not yet complete**
 - Approach is defined, and infrastructure is being implemented, but recovery plans need to be developed and tested (first quarter of FY2007)
 - Planned architecture may need to be enhanced to assure that Windows servers are appropriately addressed
- **Testing approach may impact capacity and/or availability of development and test systems**
 - Development and Test servers would be used in testing and in the case of a real disaster
 - CPUs and TIO will need to coordinate testing schedules
- **Current DR approach is designed for “smoking hole” scenarios, and may not adequately address limited disaster**
 - New DR approach may be able to better address this need
- **DR approach may not address Regional disaster**
 - Data facilities are six miles apart, and both could be destroyed in a large scale regional disaster
 - This is a calculated risk that is understood and accepted

Disaster Recovery

Industry Insight / Trends

■ Improved technologies to respond to “limited” disasters

- ❑ Implementation of Point-In-Time (PIT) copy solutions is prevalent
- ❑ These solutions help to mitigate against a frequent source of downtime, namely data corruption and they also help to shrink planned downtimes for backup
- ❑ Major approaches for implementing PIT are controller-based solutions (IBM Flashcopy, etc.) or Software-based solutions (Oracle 10g Flashback, etc.)

■ Capacity on demand for in-house recovery is becoming more mainstream

- ❑ Servers configured with capacity on demand enable pre-loaded but idle CPUs and memory to be turned on at the recovery site for DR testing, and in the event of disasters. This reduces the overall cost of dedicated hardware for DR

■ Stretching local clusters across a campus to increase return on investment

- ❑ Local clusters stretched across buildings or campuses is becoming more popular as a way of taking already-purchased redundancy to achieve some degree of DR

Disaster Recovery

Strategic Recommendations

- **Update DR plans**
 - Leverage new data center and storage replication options
 - Use test and development systems as the primary recovery platforms
- **Fill technical gaps in DR architecture**
 - For example, Windows environment may not be adequately accounted for in storage mirroring architecture
- **Establish new testing approach**
 - Execute tests in utilizing ASB Data Center and equipment
 - Develop regular schedule for testing
- **Review business continuity plans**
 - In light of reduced RPO and RTO, business offices should update their plans accordingly
- **Investigate offering DR services to other campus units**
 - Develop business case for: DR equipment hosting, Periodic testing and remote storage hosting



Middleware

Middleware

Findings – Current State

■ **Current infrastructure is very PeopleSoft-centric**

- ❑ The majority of the current infrastructure is designed purely around PeopleSoft required and supported components such as the Tuxedo App Server, Application Messaging / Integration Broker, Process Scheduler, Report Repository

■ **Three web server environments are currently in use**

- ❑ WebLogic, WebSphere, IIS, Apache, and Tomcat are all use at MAIS today. None of these are fully exploited as a complete web development and delivery platform. WebSphere has been used for development, but only in a limited fashion.

■ **Custom integration programs tie together tools with PeopleSoft**

- ❑ Unicenter, Vista Plus and Dazel are all integrated with PeopleSoft through custom UNIX scripts

■ **Application integration is primarily file based**

- ❑ With the exception of a few component interfaces and database links, all system integration is accomplished through file transfers (SFTP) utilizing a custom developed interface architecture of Unix scripts
- ❑ This file based integration adds complexity to the Unix <-> Windows interactions

Middleware

Findings – Current State

- **Directory services are only available in Windows environment**
 - MAIS maintains its own domain and directory service to support windows services
 - Campus directory not leveraged in any meaningful way
- **Workflow is application specific**
 - Each application has its own workflow architecture
- **Applications security is application specific**
 - Each application has its own access control processes and technology
- **Sophisticated batch scheduling is supported, but not used ubiquitously**
 - CA Unicenter is used to large application batch activity. Batch activity often spans across applications and platforms.
 - Windows environment uses Microsoft specific scheduling capabilities
 - To save costs, some UNIX scheduling utilities are used in place of Unicenter for simple jobs

Middleware

Findings – Emerging Trends

- **Oracle Fusion appears to be likely future application platform**
 - MAIS has not officially committed to the Oracle Fusion applications as its future direction, but their adoption in five to seven years seems likely, therefore we should plan middleware accordingly
- **Applications will adopt SOA principals**
 - Initially we will want to expose our applications through services, and eventually we will architect our applications in a complete SOA framework
 - Authentication and authorization will become increasingly important to facilitate the complex interaction of services
 - SOA environment will require defined Service Levels for services in order to avoid operational challenges
- **Services require new infrastructure**
 - Web services infrastructure (e.g. UDDI directory, WS-Security) will be needed to enable the construction and deployment of services
- **Real-time and near-real-time interfaces are needed**
 - System-to-system integration will need to occur through web services
 - Messaging architecture will be needed to handle guaranteed delivery of message to multiple systems (Enterprise Services Bus)

Middleware

Findings – Emerging Trends

- **Cross application workflow will be needed**
 - Business processes will flow across applications, and no longer will it be able to rely on an application specific solution
 - A centralized work flow architecture will need to coordinate flows across applications
 - A general purpose rules engine may need to be part of this architecture to support cross application processing
- **Cross-application and cross-platform scheduling will be needed**
 - The adoption of a services architecture may complicate or significantly change job scheduling requirements
- **The University's Enterprise Directory will be relied upon for more services**
 - To gain efficiency and reduce redundancy, the new University ED will be relied upon as a central source of some information
 - Centralized Identify Management will be needed to coordinate things like: provisioning, authentication and authorization.

Middleware

Issues

- **Customers will continue to prefer “best of breed” functionality, and this leads to a decrease in operational efficiency for the infrastructure provider**
 - Identifying and holding to some infrastructure standards could mitigate this
 - Establishing long-term commitment to Oracle Fusion (or another platform) could mitigate this
- **Users are gradually demanding increased availability at lower costs**
 - Getting to a 7x24 or near 7x24 architecture could have large costs. It’s unlikely that large funding is available to extend hours of operation, but users are beginning to demand it. This could lead to making outsourcing more attractive to meet high availability needs.
 - The move to an SOA & Services architecture may drive the need for 7x24. The cross-application integration that often exists in SOA will make availability a more important feature.
- **The selection of supporting Middleware components (UDDI, Enterprise Service Bus, WS-Security, etc.) which reside outside of a base framework will be difficult**
 - Should these products be implemented utilizing a “best of breed” approach or would a single vendor approach provide greater benefit?
 - Supporting middleware components will need to support both .Net and J2EE base frameworks
- **We will be reliant on services managed by non-MAIS areas**

Middleware

Industry Insight / Trends

- **Enterprise Relationship Planning (ERP) systems will become SOA-based**
 - Oracle, SAP and Microsoft are all committed to service oriented architectures for their applications. Oracle and SAP have committed to large scale re-architecting of their applications to achieve this vision. Many Microsoft products already include these technologies.
- **PeopleSoft applications and infrastructure are being replaced by next generation Oracle products**
 - Fusion applications will begin to emerge in 2008, and will likely be adopted by the University between 2011 and 2013.
 - Fusion applications will rely heavily on Oracle provided middleware
- **Security information will move out of the application into centralized identify management (IdM) services**
 - As IdM becomes more ubiquitous, application providers will begin relying on standards and stop building proprietary solutions into their application
- **Niche application vendors will continue to be acquired in key verticals**
 - There will be continued consolidation in many vertical markets
 - Those niche players that survive will provide services not provided by larger players and will offer integration options to fit in with ERP vendors

Middleware

Strategic Recommendations

- **Gradually shift infrastructure to prepare for long-term application changes**
 - Control costs through a step-by-step implementation of components (versus a big-bang)
 - Develop a planned approach to roll-out new functionality such as messaging architecture, workflow, identity management, etc. by the summer of 2006
 - Implement infrastructure and develop skills so the shift to new applications can be smoother
 - For example, start using Oracle Fusion Middleware with current PeopleSoft applications
- **Establish infrastructure guidelines for new applications**
 - Select vendor products which adhere to these guidelines
 - Establish key infrastructure standards, and get executive support so that future application acquisitions will leverage existing infrastructure
 - A replacement for DAC is likely to be one of the first new acquisitions, so standards and directions will need to be in place to support this decision
 - Establish capabilities in both a .Net and J2EE application platform
 - We have capabilities for a .Net base infrastructure now and need to start the selection process to choose a Java Platform
 - Ensure interoperability between any .Net and J2EE developed applications or Vendors

Middleware

Strategic Recommendations

- **We will adopt a strategy of purchasing versus developing middleware**
 - Development of components (e.g. customizing open-source middleware software) will only be done if it can provide an identifiable strategic advantage
 - In general, middleware development will only include necessary integration that can't be acquired from a vendor (e.g. batch architect scripts)
- **Ensure core middleware functionality is not duplicated by the various application platforms**
 - Some middleware will be identified as a “core” component and will be leveraged across all environments
 - Vendors such as Microsoft, Oracle and other application providers may encourage to use their middleware even if it duplicates core components which we already run
- **MAIS should evaluate and strategically determine which middleware components we will run and manage and which components we will rely on others to manage**
 - For example, ITCS may be relied upon for components such as authentication and directory services
 - MAIS may choose to become an infrastructure provider for campus in some areas such as: workflow, process orchestration, and messaging



Network Management

Network Management

Findings

■ Staff Networks:

- ❑ The relationship w/ ITCOM has improved due to current staffing arrangement and this has significantly helped communications
- ❑ MAIS has interaction and input with ITCOM and works collaboratively and in cooperation
- ❑ All switches are the same standard architecture (Cisco 3550) and provide 100MB
- ❑ 10 MB to the desktop currently and moving to 100 MB to all B&F desktops w/ Cat5e capable of Gigabit Ethernet speeds
- ❑ The B&F RADIUS system (Primary & secondary) is the primary authentication

■ Wireless:

- ❑ 28 access points across B&F
- ❑ Operated and maintained by ITCOM and limited to conference rooms

Network Management

Findings

■ Data Center Networks:

- ❑ No bandwidth concerns in tactical timelines and still have capacity (port density)
- ❑ Acquisition of DWDM technology allows a single fiber pair to provide multi-protocol transmission capability between data center to accommodate existing and new technologies
- ❑ University has established Cisco as primary vendor
 - Makes acquisition easier; provides consistent support
 - Does not leverage competitive bidding process therefore may lead to higher costs
- ❑ Capability exists in the data center to move to Gigabit Ethernet speeds

■ WAN:

- ❑ ITCOM manages overall campus WAN
 - We maintain WAN link for storage between our two data centers
- ❑ WAN links to SunGard will be phased out

Network Management

Issues

- **There could be more scope & boundary issues between MAIS & ITCom as we assume more network layer management**
- **Some localized network bandwidth restrictions in virtual firewall implementation**
- **Relationship between middleware and network components are not always well understood**
 - This could lead to less than optimal utilization of network resources
 - Ideally monitoring of the network and middleware would be more closely coupled
- **Challenges exist with access from home (ie. VPN)**

Network Management

Industry Insight / Trends

- **Advanced network architecture will enable long term growth**
 - Dense Wave Division Multiplexing (DWDM) equipment will allow the separation of the growth paths of fibre channel or iSCSI storage transmission methods from the physical cable plant and ensure that the future of storage transmission methods is state of the art.
- **Network segmentation will improve performance**
 - Network segmentation and the reduction of the size of existing broadcast domains in both the data center and staff networks will improve performance and enhance the visibility of applications across the wire
- **Wireless standards will continue to evolve and better address areas such as security**
 - 802.1x port based network access control will allow the staff networks to maintain an open policy to network guests by offering an alternative network to hosts that might be considered less secure.
- **VoIP is continuing to gain industry momentum and will require implementation of QoS as well**
 - Despite this trend, UMich will not adopt VoIP in the next 2-3 years
- **Wireless will not supplant physical cable plant infrastructure in the near-term**

Network Management

Strategic Recommendations

- **Implement 802.1x standards to improve network security**
 - Implement 802.1x port based access control to restrict access to MAIS staff networks to BFIT maintained workstations.
- **Improve network performance through segmentation and Quality of Service (QoS)**
 - Voice over IP (VoIP) and multicast video will require dedicated bandwidth to operate properly. This will be accomplished through the implementation of Quality of Service (QoS) in network switches.
 - Network Segmentation will improve visibility into existing applications and prevent performance problems by reducing the size of broadcast domains
- **Leverage DWDM technology to position MAIS to be a highly available, reliable, and disaster tolerant service provider**
 - The implementation of Dense Wave Division Multiplexing (DWDM) equipment as part of the Arbor Lakes data center build out will allow the separation of the growth path of fibre channel storage transmission methods from the physical cable plant and ensure that the future of storage transmission methods is state of the art
 - DWDM will be leveraged to support the storage strategy which provides data site redundancy and backup in support of our internal Disaster Recovery approach
- **Integrate network monitoring more closely with consolidated Systems Monitoring Tool and Application monitoring**



Security

Security

Findings

- **Security Initiatives undertaken by SNS are categorized as falling into one of six categories**
 - Prevention, Containment, Detection, Reaction, Evidence Collection and Recovery. This categorization is used to identify redundant initiatives and focus efforts toward a comprehensive strategy.
- **Detection and Prevention projects have dominated the early agenda since SNS formation, with firewalls and intrusion detection systems going in first.**
 - The agenda is starting to diversify and cross over with networking projects, such as a virus/worm Containment project using Virtual LANs in the new data center.
- **Shared accounts are used for some automated processes**
 - “1” and “2” accounts are used for automated processes and shared accounts for administrative tasks and lead to erroneous conclusions in security audits.
- **Increased number of hosting arrangements for University administrative systems**
 - All aspects of security need to be evaluated and regularly reviewed to assure University IT assets are properly protected

Security

Findings

- **The incident response policy formulated by the ITSS Incident Management Policy committee has standardized both policy and procedure around investigations & evidence collection and strengthened the university approach to investigating IT related security incidents by formalizing doctrine.**
 - Divisional level security policies are being developed in reaction to risk assessments by both internal and external audits, consistent with ISC and ISACA security management best practices.
- **MAIS Security has articulated a “defense in depth” strategy around providing layers of defense to critical MAIS systems. The strategy aligns itself with the three-tier model of client/server computing.**
 - In such a model, the user interface (web servers), functional process logic (application servers), data access (Oracle databases) each have their own specific security concerns while all tiers share the need for “baseline” security technologies.

Security

Findings

- **MAIS Security has involved itself in the ongoing plans for a university identity management strategy.**
 - This has been accomplished partially through the Two Factor Authentication project, which brings a common authentication mechanism to the university community to supplement passwords. It has also been accomplished by participation in the Enterprise Directory project, looking to align MAIS authentication goals with the broader issues of authentication and system authorization.
- **MAIS Security has worked with Business & Finance IT to try and strengthen the direction of desktop user security.**
 - This has included consulting with regards to desktop firewall settings, agent based intrusion systems, the use of encryption and Public Key Infrastructure for authentication. In conjunction with the virtual firewall, the attacks against desktop systems has dropped from hundreds per month to effectively zero. The number of incidents related to impaired desktop due to infection has dropped, which has resulted in improved uptime and efficiency for MAIS employees.

Security

Industry Insight / Trends

- **Secure data transfer via batch file processing will become outdated in favor of application messaging within the next five years**
- **Biometrics are growing in popularity**
 - MAIS has chosen not to pursue biometrics, but may need to revisit this decision in the future.
- **Digital certificate technologies will become more prevalent in the market**
 - MAIS will use tokens as a bridge technology, to get from non-reusable one time passcodes to digital certificate technologies.
 - Certificate based credentialing will overtake tokens and will be a required part of any federated identity system within higher education
- **Detection heuristics will advance to allow near real-time quarantine decisions to be made.**
 - These technologies will combine Network Admission Control (NAC) with Intrusion Prevention (IPS) to allow infrastructures to detect protocol misuse and respond according to prescribed policy. This will aid in stopping self-propagating worms, viruses, etc.

Security

Industry Insight / Trends

- **WS-Security will be a key enabler of a service orientation**
 - MAIS security group must develop expertise in this area.
 - SOA architecture will communicate trust relationships between the components via SAML (XML) assertions utilizing WS-Security
- **System baselining, whereby a system is completely validated against a “health policy” will become part of the next generation of desktop systems.**
 - Microsoft calls this Network Access Protection, and it is integral to Windows Vista and Longhorn. The System Health Agent will have an exposed API and can be used by administrators to validate any condition.
 - This can have the largest effect on laptops, which often travel and use remote access methods. They can be swept and validated before they are allowed network access through an interaction of the remote access system and the directory policy.

Security

Strategic Recommendations

- **Scope of the Security & Network Services Team should expand to support Business & Finance**
 - Apply ITSS developed RECON assessment methodology and implement industry best practices as appropriate
 - Classify assets and assess appropriate security approach
 - Establish appropriate departmental security standards
- **Expansion of two-factor authentication should be pursued**
 - Investigate extending use to other systems such as departmental or other campus systems
- **Investigate feasibility of Security Information Management framework**
 - Manage security event information in an integrated approach with other system messages and events
 - Evaluate and possibly pursue comprehensive logging approach to provide advanced notification and monitoring capabilities.

Security

Strategic Recommendations

- **MAIS should lead the university adoption of a Public Key Infrastructure**
 - MAIS should adopt a leadership position in PKI and coordinate activities over the affected campus IT communities
- **MAIS should encourage and support the adoption of SmartCard technology**
 - MAIS should work with the MCARD office, the Key Office and other stakeholders to transition logical and physical access to a single device
- **Investigate alternatives for shared system accounts**
 - Find alternatives to the use of “1” and “2” accounts
- **Refine requirements for vendor hosting of administrative systems**
 - Update standards and process that will be used when vendors host a University administrative system



Server Hardware & Operating System

Server Hardware & Operating System

Findings

- **Consolidation and virtualization have been implemented for all operating systems**
 - MAIS has moved to physical server consolidation aggressively via recent capital replacement cycles
 - The number of physical servers managed has been reduced by 28% over the last year
- **MAIS is beginning to implement policy-based resource utilization**
 - Already in use in the Windows virtual server arena (VMWare) and is in the process of being implemented in the AIX arena
- **Current approach is primarily a 1-to-1 mapping where each application resides on its own exclusive OS Image**
- **The role and fit of Linux in the MAIS environment has not been determined**
 - No adoption / research / strategy regarding Linux
 - We have limited Linux experience as an organization
- **We have no framework in which to determine the OS we will utilize when an application supports AIX/Linux and Windows**
 - Criteria used today are not strategic and have more to do with team capacity and resource availability

Server Hardware & Operating System

Issues

- **Emergence of 64-bit Intel hardware**
 - Transition approaches and technologies will need to be investigated
- **Our resources and skills are tied to particular OS & HW combinations**
 - We have traditionally specialized by AIX on RISC, Windows on Intel, and z/OS on MF
 - We have no deep Linux system administration experience or skills
- **We are not as efficiently distributing server computing resources as we could be**
 - Capacity increases at the HW layer for AIX have to be made in large and costly increments which do not always align well with demand
 - We have no logical way of determining when to adopt a scale-up vs. scale-out system architecture for any given application
 - Our project funding model does not easily fit with the cost structure of server virtualization or with application consolidation (e.g., hosting multiple applications on 1 server image)

Server Hardware & Operating System

Industry Insight / Trends

■ Virtualized OS

- Virtualization enables more effective use of server resources

■ Multi-core central processor chips

- Reduces heat and power requirements and increases server performance

■ Commoditized and standardized blade servers

- Reduce data center footprint
- Lower administration overhead
- Improved redundancy
- Potential savings if “build out” approach is appropriate

■ AIX / Linux Affinity

- IBM has a long term commitment to LINUX and may eventually lead to the discontinuation of AIX

■ Adoption of Grid Computing will expand

- Currently applicable mostly for specialized computing which requires significant computing resources

Server Hardware & Operating System

Strategic Recommendations

■ More effectively utilize server resources

- ❑ Develop a decision framework model to assist in the determination of scale-up vs. scale-out decisions
- ❑ Establish a post implementation resource utilization review process
- ❑ Implement CPU Pooling (AIX)
- ❑ Implement VMotion for VMWare virtual servers
- ❑ Establish a guideline of consolidating applications on shared HW where possible rather than implementing with the default 1:1 application to server philosophy
- ❑ Continue to leverage existing investment in the p595 Squadron IBM hardware for growth in the scale-up approach.

■ Develop a decision framework model to assist in the determination of OS

- ❑ Model would be based on strategic parameters such as skills, support costs, resource availability, etc.
- ❑ Perform a review and assessment at project initiation to make this determination

Server Hardware & Operating System

Strategic Recommendations

- **Evaluate where / when our architecture could benefit from adoption of Linux**
 - Evaluate the fit of Linux to our environment
 - Implement a Linux pilot
 - Identify Linux skills needs and develop appropriate training plans
- **Consider alternative purchasing approaches to drive down cost**
 - Consider bulk purchasing approach to drive down cost, versus smaller purchases spread over time
 - Establish a timeline for reevaluate primary vendors for server hardware
 - Establish a consistent purchasing decision framework / vendor for the x86 space
- **Achieve DAC system replacement allowing for retirement of Mainframe HW & OS**



Storage Management

Storage Management

Findings

- **MAIS has adopted and implemented tiered storage for cost efficiencies of storage**
 - MAIS utilizes used/remanufactured components for non-new equipment
 - MAIS is migrating to higher capacity drives over time
- **Heterogeneous environments make storage less tied to AIX**
 - Storage management has expanded beyond initial storage consolidation project for AIX servers and is now expanding to all managed platforms
- **MAIS has adopted a disk-based backup approach for better disaster recovery preparedness and for file restoration**
 - MAIS moved to a LAN-free backup architecture
- **MAIS has invested in equipment to support a multi-vendor storage environment**
 - Even with this capability for multi-vendor support, we are primarily single vendor aligned
- **Storage management is currently distributed across System Support, WES and BFIT**
 - Technologies could allow us to gain efficiencies by consolidating management

Storage Management

Issues

- **Currently no incentive to use storage wisely**
 - ❑ No formal archive and purge policy is in place
 - ❑ No clear standards established for how/when to utilize tiered storage
 - ❑ Currently no reports on storage use by environment, growth, and cost
 - ❑ Data is not mapped to tiered storage (Oracle – Static DW tables can be moved to low-end storage)
- **Lack of suitable storage management tools**
 - ❑ Current vendor provided storage management tools lack rich feature sets and automation capabilities
- **Need a more formalized and integrated disk capacity projection process with documented assumptions**
 - ❑ Disk capacity projections are informally created and are used for budgeting
- **Offsite tapes are not encrypted**
 - ❑ Industry best practices and recent events have shown a potential security risk for mishandled un-encrypted tape data (tape loss by offsite tape storage vendor, etc.)

Storage Management

Issues

- **Database and storage management tools have overlapping features**
 - It is unclear how to make a determination which one should be used
- **It is unclear how governance of storage is handled**
 - Do applications determine storage tier or are storage placement decisions managed by storage team?

Storage Management

Industry Insight / Trends

- **Use of Data Encryption for tape and disk that travels off-site**
- **Document storage is increasing within applications**
 - Should files be stored in the database or in the file system
 - Problem also exists with email storage
- **iSCSI / SAS are emerging trends**
 - BFIT is implementing iSCSI for file services
 - MAIS needs to continue to investigate and understand these technologies as they evolve
- **By 2008, 80% of organizations will have dedicated storage groups**
 - MAIS currently does not
- **Regulations are driving storage growth and data retention requirements**
 - Admissions lawsuit is an example of a legal requirement that has driven extended storage needs

Storage Management

Strategic Recommendations

- **Consider the creation of a dedicated Storage Management Group**
 - Determine what storage would or should be covered by a central group
 - Charge Storage Management Group to create the 3-year Storage Architecture Plan to address Capital Replacement, Storage Automation and Storage Governance
 - Charge Storage Management Group with determining and documenting how to enforce efficient use of storage
- **Establish a formal Archive and Purge approach for MAIS managed systems**
- **Pilot and evaluate tape based encryption**
- **Enhance our storage architecture to further support High Availability and flexible maintenance schedules**

Storage Management

Strategic Recommendations

- **Consider acquisition of Storage Management Tools**
 - Research and evaluate current capabilities and features of Storage Management toolsets in order to assess if market is mature
 - Select and purchase Storage Management tools to help efficiently manage centralized storage
- **Consider alternative purchasing approaches to drive down cost**
 - For example, follow MCIT approach of re-bidding entire storage architecture on a regular schedule instead of just incremental purchases for growth and replacement
 - Take advantage of multi-vendor capability of our environment by purchasing commodity hardware from lowest cost provider



Systems Management

Systems Management

Findings

- **A majority of the monitored data is collected, summarized and trended in a custom developed Capacity Planning system**
- **MAIS provided applications are reliant on numerous non-MAIS managed resources (DNS, Cosign, Campus Backbone, etc.)**
- **MAIS currently utilizes a collection of point solutions by specialty area for monitoring and management**
 - Only rudimentary “Up/Down” type events are communicated to a central console
 - Events reported to the central console are not correlated
 - There is no monitoring from an “end user” perspective

Systems Management

Findings

- **Advanced features of CA Unicenter NSM have not been fully utilized**
 - ❑ Business process view (Worldview) not implemented
 - ❑ No agents, auto-discovery or reporting enabled
- **Microsoft Operations Manager is used to manage Windows environments**
 - ❑ Only rudimentary monitoring is passed to Unicenter NSM
 - ❑ MOM sends some SNMP traps to CA Consolidated console
 - ❑ MOM is setup to also page and email directly as well as conduct Web & Active Directory monitoring
- **Oracle Enterprise Manager is used to manage Oracle databases**
 - ❑ Only rudimentary monitoring of Oracle is passed to Unicenter
 - ❑ Many custom scripts w/ direct email notification; No SNMP Traps sent; OEM v9 Agent enabled in some DB's w/ direct email notification; Manual once/day space script
 - ❑ Application Monitoring: Custom Unix scripts w/ direct page or email notification
- **Cricket and Cisco tools used to manage Network**
 - ❑ Some SNMP traps sent to CA console

Systems Management

Issues

- **No view of application behavior for MAIS managed resources**
 - ❑ Performance or response time of an Application or service is not proactively monitored from an end-user perspective
 - ❑ Many 3rd Party Applications are not instrumented for monitoring and are a “black box”
 - ❑ Messages / Alerts not aligned with Business Services
 - ❑ No Help Desk Integration or exposure
 - ❑ Our ability to provide application availability from an end-user perspective is often impacted by our dependence on non-MAIS managed resources
- **Current monitoring approach leads to inefficient and silo troubleshooting by area**
 - ❑ Our culture of monitoring and information sharing is by technical area and not Service oriented
 - ❑ Monitoring (what & how) is determined by each individual group
 - ❑ Notification and escalation approaches are inconsistent

Systems Management

Issues

- **TIO resources are inefficiently used**
 - Time tracking data indicates that “monitoring” is one of the largest production support activities, yet the teams all agree we are not up to industry standards
 - Extensive custom development and support of monitoring / management solutions is required
- **Monitoring requirements are not always identified in advance for new applications or functionality**
- **We do not have a centralized and searchable knowledge store of encountered monitoring issues and their resolutions for reference**

Systems Management

Industry Insight / Trends

- **As availability moves toward 7x24, there is an increased use of mobile devices for remote support, monitoring and response**
- **Corrective actions can be automated to occur without immediate human intervention**
- **Vendor provided “agents” are being used increasingly to monitor resources**
- **Monitoring of resources from a Business Process or Service view rather than by individual component will continue to increase**
- **As architectures are becoming more distributed and complex, more detailed monitoring information is being required at each component layer**
- **“Manager of Managers” approach is being adopted to integrate separate monitoring tools into an overall single view**

Systems Management

Strategic Recommendations

- **Implement a comprehensive systems monitoring framework for MAIS Managed resources**
 - ❑ Expose this comprehensive systems monitoring framework to more of MAIS – specifically the Help Desk, Operations and within the rest of TIO
 - ❑ Create Business Process Views of monitored resources
 - ❑ Automate notification, escalation and responses where possible
 - ❑ Investigate and implement auto-discovery tools for monitored resources
 - ❑ Require major architecture components and point solutions to utilize the comprehensive monitoring framework to reinforce a central collection and management view
- **Add simulated application transactions from an end-user perspective to monitoring scope**
 - ❑ Implement sampling stations at key points on campus which simulate end-user transactions and test availability of underlying required components (DNS, Cosign, etc.)
- **Enhance our SDLC Methodology to capture monitoring requirements during design/build and also to include a post-implementation review cycle**