1) Meeting Overview/Announcements: Linda Pizzo (10 minutes)
   - Sign in Sheet
   - Next Meeting February 14, Medical School Lecture Hall A
   - Introduction New Staff

2) Emergency Preparedness Initiative: Sam Simon (30 minutes)

3) Logical Access and Change Management Impact: Tim Brooks (20 minutes)

4) Information and Performance Management Initiative (University-Wide Reporting Solution) : Linda Pizzo and Renee Canavan (20 minutes)

5) Q & A
Meeting minutes of the Saint Louis University Business Managers held at 9:00 a.m. on Thursday, January 10, 2008 in the Busch Student Center room 172.

Business & Finance Staff Present:

Keith Emge   Melissa Ezell   Mary Drexl   Sharon Gajewski
Greg Haney   Jeff Hovey      Lee Kneibert   Michael Lucido
Tom Meadows  Lori Myers      Annaliese Neff  Linda Pizzo
Gary Whitworth  Lisa Zoia

Guests:

Tim Brooks   Rene Canavan   Ken Gebken   Jen Haegele
Kevin Jones  Mike Lauer   Sam Simon   Travis Wilson

Number of Business Managers Present: 65

Linda Pizzo welcomed everyone to the meeting. Next month’s meeting will be held on February 14 at the HSC Campus, Medical School, Lecture Hall A. Please check the meeting schedule for the location of all future meetings.

Introductions – Gary Whitworth introduced Michael Lucido as the new Associate Director of Best Practices. Michael came to Business and Finance from Facilities Services where he served as Property Manager. Michael also worked in the President’s office prior to his appointment with Facilities. Michael encouraged all Business Managers to contact him with any concerns, suggestions, etc. His phone number is 977-3199 and his email address is lucidoma@slu.edu. Everyone welcomed Michael.

Emergency Preparedness – Sam Simon, the University’s Director of Emergency Preparedness addressed the business managers. Sam reviewed the efforts underway across the University to have a comprehensive plan in place to deal with an unplanned event, whether it is weather related or an unstable student, faculty or staff member. Sam is meeting with an Emergency Planning Committee to take the individual plans that are in place in various departments and schools and form one cohesive plan. The objective is that in the event of an emergency, everyone knows what to do, where to go and who is in charge. The emergency contact system has been set up so that all students, faculty and staff can be contacted simultaneously if necessary. The phone numbers being used are those that individuals have provided on their employee contact information in Self Service Banner. Everyone needs to be reminded to keep that information current. Sam served as a former Homeland Security Rep for St. Louis city, county and the surrounding counties and has extensive training in emergency preparedness. He was also the former Director of Public Safety for the City of St. Louis. Sam will make a presentation of his plan to the Executive Committee in February and then set a timeline to bring the program University-wide. They are considering resurrecting Building Captains so that each campus building has one person responsible for the people in that building. Until the program is rolled out, Sam suggested visiting the FEMA website www.fema.gov, click on NIMS in the left hand margin under “Quick Links”. The site has information about training and certification that is available. There is also good information on the site for preparing at home and getting children involved.

Sam also introduced the new Director of Public Safety, Mike Lauer. Mike retired after 20 years with the St. Louis Police Department where he achieved the rank of Lieutenant and was commander of the Homicide Division. Mike spoke saying he is honored to working at the University and hopes to serve the SLU community well.
Sam Simon also thanked Pat Pisarkiewicz and Dee Marty for their incredible support and assistance as he came on board at SLU.

**Saint Louis University Quality Assurance Program** – Tim Brooks spoke to the Business Managers about the changes that are coming with the Logical Access and Change Management Implementation. The goal of the project is to ensure the confidentiality, integrity and availability of our computer systems, applications and data. One of the first steps that will be taken is to implement stronger passwords. Passwords must be changed every 180 days or approximately twice each year. Reminder emails will be sent 3 weeks out, 2 weeks out, 1 week out to users to change their passwords. The Change Management portion of this initiative will:

- Ensure that any changes made to an application or system will not have a negative effect on other users
- Require that all changes to computer information systems be subject to a review and approval process
- Require all changes to be properly documented
- Improve overall uptime and availability of resources
- Use the help desk “Remedy” to process all change requests

This initiative will allow greater transparency and assist the University in remaining compliant. For more information on this program please click here.

**Information Management Initiative – University-Wide Reporting Solution** – Linda Pizzo gave a presentation on a new initiative that will establish an institution-wide solution to provide University executives, faculty and staff the information, metrics and reports needed to effectively manage their respective units. The goal is to provide one source for consistent and reliable data that is easily accessible and requires little manipulation. Linda is working with Rene Canavan from IT and Gary Whitworth is leading the initiative. Updates will be provided to the Business Managers as this initiative develops. For more information click here.

Linda Pizzo adjourned the meeting at 10:15 a.m.

Minutes respectfully submitted by Mary Drexl.
“Quality assurance and institutional effectiveness are derived from open-mindedness and always questioning the norm.”

**Logical Access and Change Management Implementation**

**Project Goal:**

The implementation of logical access and change management controls is designed to ensure the confidentiality, integrity and availability of our computer systems, applications, and data. Our goal is to provide a secure, stable computing environment for the faculty, staff, and students of Saint Louis University.

**Project Impact:**

- **Logical Access**
  - Stronger password management policies and procedures
    - Password must be a minimum of 8 characters
    - Password must not be the same as your “SLU net ID”
    - Password must be constructed using 3 of the 4 following character types:
      - Uppercase alpha (A, B, C, D, E, …)
      - Lowercase alpha (a, b, c, d, e, …)
      - Numbers (1, 2, 3, 4, 5, 6, 7, 8, 9, 0)
      - Special characters (!, #, $, %, &, *, etc.)
    - Passwords must not be easily guessed: must not be names, dictionary words, phone numbers, birthdays or contain their “SLU net ID”
    - Passwords must be different from the previous 12 passwords.
    - New Users provided with a temporary password, will be forced to change their passwords after their initial log in.
    - All “SLU net IDs” will automatically expire every 180 days. The User will be prompted to change their password before expiration.
    - Please note that a user with three consecutive unsuccessful login attempts will be temporarily locked-out of their account.
  - Will eliminate weak, easily guessed passwords
  - Will eliminate inactive accounts

- **Change Management**
  - All changes to computer information systems will be managed according to the following controls:
    - All change requests will be subject to a formal review and approval process
    - Formal review and approval process will be segregated by Business Process Owner, ITS Functional Managers, Change Control Manager, and Change Control Board

Saint Louis University
Quality Assurance Program
• All change requests that meet the one or more of the following parameters must be transferred to the ITS Project Office for review and signatory approval:
  • > $25,000
  • 300+ man hours
  • 3+ ITS departments
• All changes will be properly documented throughout the change management lifecycle
• Change requests will be assessed for business impact and business risk
• Change requests will be tested and assessed for backout plans
• All change tests will be verified
• All change implementations will be verified
• All unauthorized changes will be mitigated
  o Will ensure changes requested by one individual business unit do not have a negative effect on other users.
  o Will improve overall uptime and availability of electronic resources.
➢ Logical Access and Change Management workflow
  o User account and change requests integrated into current Service Desk system, Remedy.
  o Developing consistent set of service delivery expectations for requests.

LACMI Project Schedule

➢ Planning & Communication – completed November 16, 2007
➢ Technical Requirements – completed December 7, 2007
➢ Design Phase – completed January 4, 2008
➢ Communication & Training – in progress, due to be completed January 18, 2008
➢ Implementation Phase – begins January 21, 2008
  o Password Management Policy Changes to be implemented over 20 week period to minimize disruption.
➢ Post Implementation Review – begins March 17, 2008
➢ Target Project Completion Date – March 28, 2008

Next Steps:

➢ Thorough socialization of upcoming changes to processes and procedures
  o Executive Level (PCC)
  o Department Level (Business Managers)
  o Faculty & Staff (see attached message)
  o Student (see attached message)
  o ITS Training
  o Department walkthroughs
➢ Staggered rollout of password enforcement mechanisms for password management policies beginning after February 1st
➢ Change management procedures will be implemented and documented by the end of March.
Message to all Faculty and Staff on password and account management controls:

NOTICE: CHANGES TO YOUR SLUnet ACCESS PASSWORD COMING IN FEBRUARY!!!!

In an effort to improve the security and stability of the entire University computing environment, the Quality Assurance Office is updating the current password requirements for all faculty, staff and students. If your current password does not meet the new requirements, you may be temporarily unable to log into any systems that require you’re “SLU net ID”.

All “SLU net” passwords will automatically expire every 180 days. The User will be prompted to change their password before expiration. Please note that a user with three consecutive unsuccessful login attempts will be temporarily locked-out of their account.

- For Novell log-in users: If your password does not comply with the new requirements or is expiring, you will receive a one time notification to change your password when you log-in.
- Users of Macintosh, Linux, or UNIX will NOT receive this notification. If you log into your computer locally, but access University data you will be temporarily unable to retrieve folders or files until your “SLU net” password has been changed to meet the requirements.

The new password requirements are as follows:

- Password must be a minimum of 8 characters
- Password must not be the same as your “SLU net ID”
- Password must be constructed using 3 of the 4 following character types:
  - Uppercase alpha (A, B, C, D, E, …)
  - Lowercase alpha (a, b, c, d, e, …)
  - Numbers (1, 2, 3, 4, 5, 6, 7, 8, 9, 0)
  - Special characters (! #, $, %, &, *, etc.)
- Passwords must not be easily guessed: must not be names, dictionary words, phone numbers, birthdays or contain their “SLU net ID”
- Passwords must be different from the previous 12 passwords.
- New Users provided with a temporary password, will be forced to change their passwords after their initial log in.

ITS recommends that all Faculty and Staff review their passwords to ensure they meet the above requirements before February 1, 2008.

To change your password, please go to www.password.slu.edu and follow the instructions. If you require assistance or feel your account has been temporarily disabled, please contact the ITS Customer Service Center at helpdesk@slu.edu or call 977-4000.

Saint Louis University and the Quality Assurance office appreciate your assistance in helping us provide you a stable and secure computing environment.
Message to all students on password and account management controls:

NOTICE: CHANGES TO YOUR SLUnet ACCESS PASSWORD COMING IN FEBRUARY!!!!

ITS recommends that all students review and change their “SLUnet” password before February 1, 2008. In an effort to improve the security and stability of the entire University computing environment, the Quality Assurance Office is updating the current password requirements for all faculty, staff and students. If your current password does not meet the new requirements, you will be temporarily unable to log into any systems that require you’re “SLU net ID”.

All “SLU net” passwords will automatically expire every 180 days. All students, faculty staff will be prompted to change their password before expiration. Please note that a user with three consecutive unsuccessful login attempts will be temporarily locked-out of their account.

The new password requirements are as follows:

- Password must be a minimum of 8 characters
- Password must not be the same as your “SLU net ID”
- Password must be constructed using 3 of the 4 following character types:
  - Uppercase alpha (A, B, C, D, E, …)
  - Lowercase alpha (a, b, c, d, e, …)
  - Numbers (1, 2, 3, 4, 5, 6, 7, 8, 9, 0)
  - Special characters (!, #, $, %, &, *, etc.)
- Passwords must not be easily guessed: must not be names, dictionary words, phone numbers, birthdays or contain their “SLU net ID”
- Passwords must be different from the previous 12 passwords.
- Users will receive notification and be required to change their password every 180 days
- New Users provided with a temporary password, will be forced to change their passwords after their initial log in.

The University recommends that all students check their “SLU net ID” account at least once a month by simply logging onto the gateway site or your individual email account.

To change your current passwords please go to www.password.slu.edu and follow the instructions. If you require assistance or feel your account has been temporarily disabled, please contact the ITS Customer Service Center at helpdesk@slu.edu or call 977-4000.

Saint Louis University and the Quality Assurance office appreciate your assistance in helping us provide you a stable and secure computing environment.
Information Management Initiative

Business Manager’s Meeting
January 10, 2008
The Information Management Initiative will establish an institution-wide solution that provides University executives, faculty and staff the information, metrics and reports needed to more effectively manage their respective units and achieve University goals.
Information Management Initiative

Vast amounts of data are stored in Banner and other systems. However...
- it is not always easily accessible
- it requires a great deal of manipulation prior to distribution or analysis
- it is not consistently applied based on commonly accepted institutional definitions
Information Management Initiative

• Relevant, timely, accurate and consistent information is needed to make informed operational and management decisions.

• Transactional data needs to be migrated into management information
INFORMATION MANAGEMENT INITIATIVE

* Information needs to reach all levels of campus
* Data from staff levels must be transformed to executive levels

EXECUTIVES:
Need visibility into progress towards our goals, objectives

MANAGEMENT:
Need timely trends, summaries, analytics of our operations

STAFF:
Need detailed reports & queries in many Formats and ad-hoc access

- Board of Directors
- President
- Provost
- Vice Presidents
- Deans, Directors, and Department Chairs
- Planning and Decision Resource
- Financial Planning & Budget
- Business Managers
- Admissions
- Advancement
- Business & Finance
- Human Resources
- Information Technology
- Registrar
- SLU Care
- SLUCare
- The Museum of Saint Louis University
Goals

• Provide a holistic solution to the University’s reporting needs
• Provide a consistent source of institutional data based on commonly accepted definitions
• Provide end users with direct access to data that support their needs.
• Maintain data security and integrity
• Promote best practices within the University
Questions/Comments?