IT Governance: Shared IT Infrastructure Advisory Committee (SIAC)

Agenda

3:00 to 4:00 **11/26/2013** **CSE 507**

Members Attending: Cromer, Fitzpatrick (ex officio), Olson, Sallot (acting Chair)
Others Attending: Burdette, Curry, Madey, Miller, Oulman, Spatz

1. Reschedule Dec. 24th meeting? **All**

Canceled – Next meeting 1/28/14

2. IAM Strategy Project **Warren Curry**

See attachment

- We're being presented with opportunities to improve IAM (Identity & Access Management), particularly in view of the fact of the mainframe going away, so the registry needs to be replatformed at minimum.
- Existing governance structures are informal
- See attachment for overview of the plan and timeline

3. Common SIP Domain Name **John Pankow**

See Addendum 1

- Pankow unavailable to present this month
- Suggestion to table until Pankow can be available.
- Group approved/none opposed

4. Office365/SkyDrive **Iain Moffat Oulman**

- Enterprise Systems is working on self-attestation portal for SkyDrive. OSG is working with InfoSecurity (Cheryl Granto) on this, as well; SkyDrive will be 25GB 'self-provisioned' alternative to Drop-Box for faculty/staff.
- Other O365 Services: Student Migration Portal opened earlier this month; moved ~ 1,100 so far. All feedback is that things have gone smoothly. Will start pushing the message out louder after 1st of year. Cromer suggests announcement on ISIS home page.
- IMAP is disabled for students; you can authenticate via IMAP, but it can't get your folder-list.
- All new students are going straight into O365.
- Question re: whether forwarding is/will-be allowed? Fitzpatrick says InfoSecurity is reviewing with Legal, etc.

5. Infrastructure Applications Advisory Committee (standing item) **Eric Olson**

- Did not meet this month.

IT Governance: Shared IT Infrastructure Advisory Committee (SIAC)

6. GatorLink Credential Authentication in Labs **Dan Cromer**

- When do GatorLink accounts get disabled in AD, after students graduate? What is the process?
- Curry: Autogroups feed from registry to AD; for each UF Affiliation, there's a corresponding autogroup. Warren can consult with Dan and help him set up the AD definitions. See also http://identity.it.ufl.edu/identity-coordination/uf-directory-affiliations/student-affiliations-lifecycle/ including the Affiliations Reference listing (right-side menu).
- Miller suggests this same question extends to access to Wireless Networking
- Curry: Yes, Wireless Networking and also VPN
- Curry: Authorization policies are the domain of the service-provider
- Fitzpatrick: Policies are set by InfoSecurity
- Miller & Curry: WiFi & VPN both need policy; should he go to Rob Adams? Or the Security Committee?
- Fitzpatrick: Miller should make a recommendation to this committee, which can then channel it through UFIT Governance
- Suggestion to consult with the Campus IT Directors?

7. Other Topics? **All**

8. Next Meeting – the 4th Tuesday from 3:00pm to 4:00pm – 1/28/2014 in CSE 507

Additional Information:

- UF IT Governance Home: http://www.it.ufl.edu/governance/
- Shared Infrastructure Advisory Committee (SIAC) website: https://connect.ufl.edu/it/SIAC/

Addendum 1: SIP Interoperability Plan

Kris,

A group representing the interests of UF Health and UFIT NetServices, Academic Technology, Open Systems and Telecom met on Wednesday, November 06, 2013 to discuss a plan to establish a common SIP domain name to use in URIs for telephony, videoconferencing, and other SIP services at the University of Florida. It is intended that the name should be short and not representative of any specific service.

The group selected UC.UFL.EDU as the recommended domain name for this purpose. Alternatives considered were MEET.UFL.EDU, MEETME.UFL.EDU, FINDME.UFL.EDU, and CALLME.UFL.EDU.

We would like the Shared Infrastructure Advisory Committee to provide the final recommendation for this domain name and request that this topic be added to the meeting agenda at your earliest convenience.

Please find attached a diagram showing an overview of the services involved with this request.

Regards,

John Pankow, on behalf of:

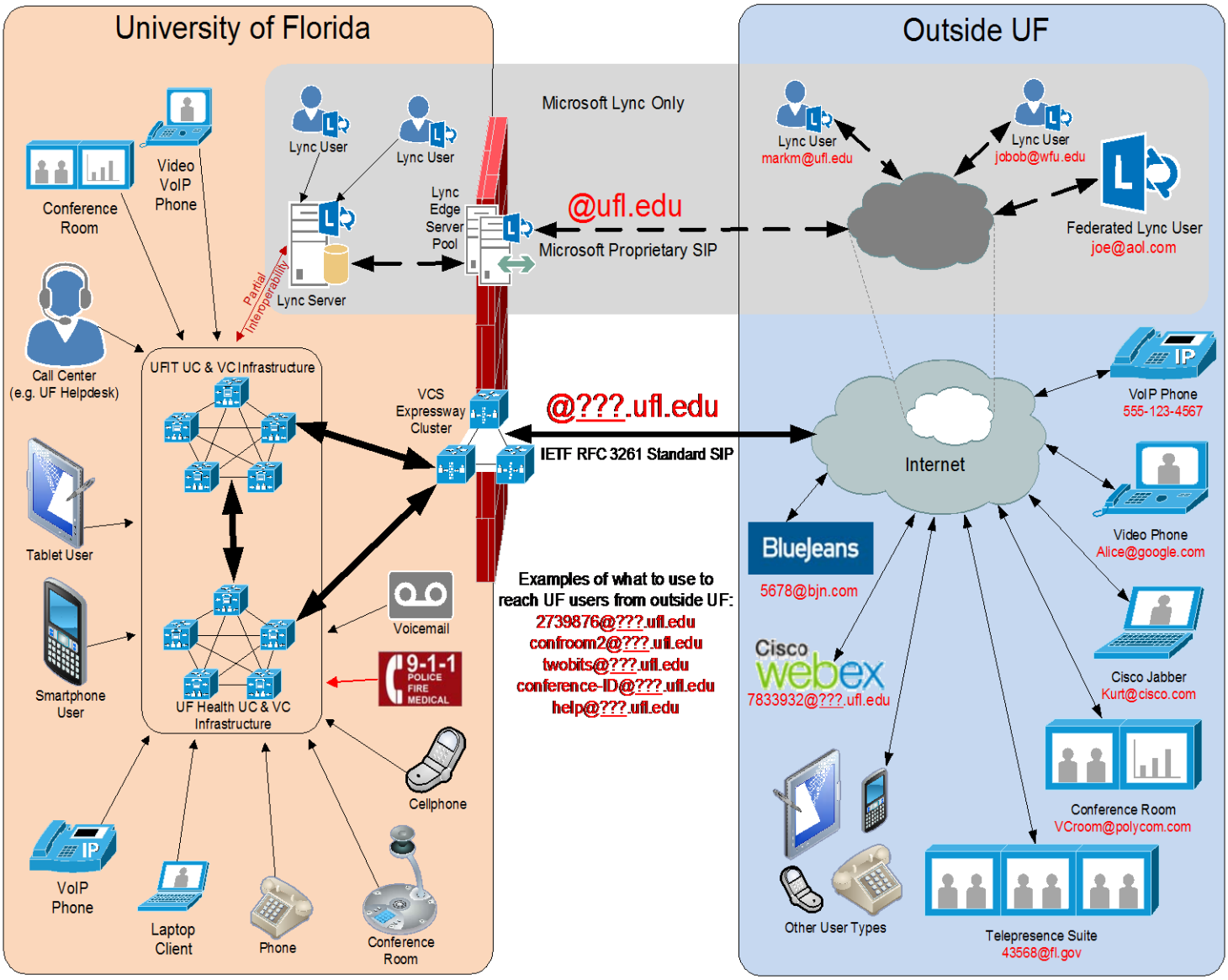
Ilundain, Jaime jilund@UFL.EDU
Madey, John P jmadey@ufl.edu
Livoti, Thomas tlivoti@UFL.EDU
Deleon, Jason A jadeleon@UFL.EDU
McCallister, Mark markm@ufl.edu
Griffin, Chris cgriffin@ufl.edu
Moffat, Iain P C ipm@ufl.edu
Pettus, Patrick patrickp@ufl.edu

IT Governance: Shared IT Infrastructure Advisory Committee (SIAC)

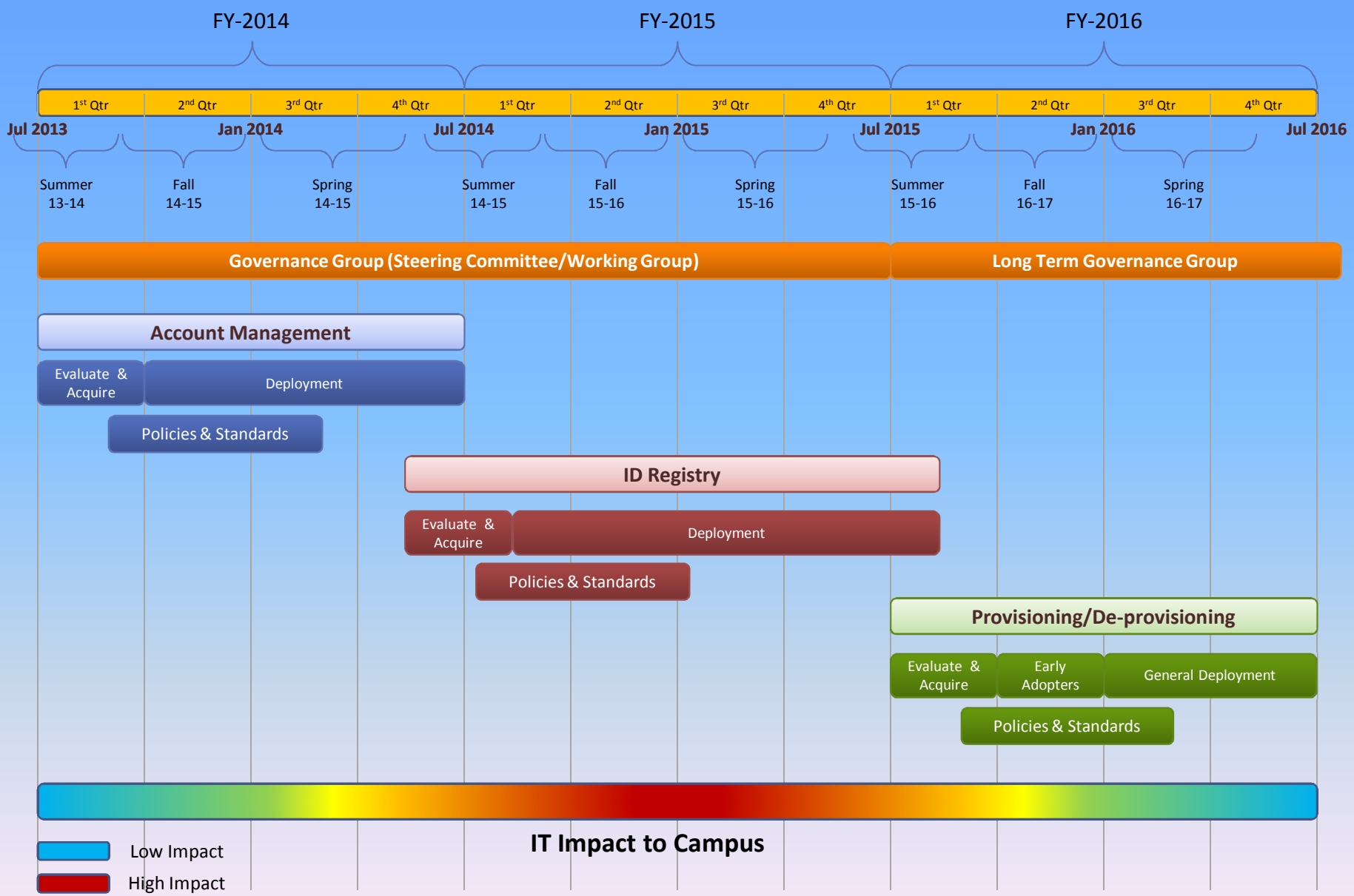
November 6, 2013

SIP Interoperability Plan

Version 2.3



IAM Projects Timelines



IAM Project Objectives

User Category	Pain to be Addressed	Benefits to be Added
Individual End-User	• Confusing self-service functionality • Notification of user account changes are insufficient • Password management issues • UF online directory not accurate, needs additional search, org contact info • Lack of mobile device support for account changes/passwords • Self-asserted accounts is a fragile and disjointed end-user experience • Guest accounts vs. Visitor network usage requires clarification	• Improved user experience for self-service account management including password management • UF online directory improvements including mobile and workstation access • Mobile/Social credentials support where appropriate • Multiple device management (phone, tablet, laptop, etc.) support • Password management experience improvement along with compliance with new policies and standards
Business Silo's, Organizations	• Single Sign-on not functional in all areas • Support delays due to slow updates • UF Active Directory standards issues across multiple domains • Onboarding &Termination processes are disjointed, confusing, and manual • Person Registry duplication issues • Role assignment process is confusing, multi-layered • Configuring access to resources is both too centralized in some cases and too distributed in others • Guest accounts are difficult to configure	• Single Sign-on available for all systems as required • Federated Access support improvement • Duplicate/incorrect data issues efficiently managed • 2-Factor authentication available where required • Automatic notifications of account issues to appropriate parties • Certification/Attestation process greatly improved • Provisioning/De-provisioning improvements to enhance ability to access appropriate resources • Finer grain entitlement management to address segregation of duties, training requirements, etc. • Better integration with HR and Student systems events
IT Support, Administration	• Mainframe to be eliminated will result in the ID Registry having to be deployed and re-configured for new infrastructure • Support providers have to access multiple, disjointed interfaces for troubleshooting user issues in the current IAM environment • Privileged accounts are manually managed locally • Synchronization delays between account management source and credential stores needs to be minimized • Current management of Active Directory groups lacks consistent standards, creates scalability and usage issues	• Active fraud detection measures, anti-phishing measures will be incorporated • Privileged account provisioning will be better managed and monitored • Identity management console will provide a unified interface for support users • UFIT cost reductions are realized by removing dependency on mainframe • Centralized audit views of runtime authorization events, allowing for easier detection of malicious behavior • Improved data quality assurance programs
University Wide	• IAM Governance not formally identified, IT community has been primary driver of IAM solutions • Current system is not configured for high availability • Certification/Attestation process needs improvement • Identity Management analytics need improvement • Campus wide adherence to published IAM/Security policies and standards needs improvement	• Broader involvement of campus business participants in IAM governance • Coordination of Policies and Standards becomes more responsive to business needs • Improved long term support for InCommon.org and other security federations • Improved regulatory compliance (FERPA, HIPAA, PII, etc.) • Simplification of security audits for governance/compliance