IT at UC
Governance

IT Managers
Meeting Summary

April 11, 2017
9:30 AM - 11:00 AM
University Hall, Room 450

Welcome and Meeting Objectives – Dom

Review and approve the summary of 3-14-17 meeting – Dom

The March meeting summary was approved with the notation of a minor spelling error.

New Business

Brief Update on UC_ Secure - Hunter Bridewell

Hunter informed the group that SecureWireless is being replaced with UC_Secure. The new service was initiated last Monday and approximately 3,900 devices have been registered. In May, the SecureWireless name will be hidden; by May 15th the name will no longer exist. On June 1st SecureWireless will be deactivated. Everyone is encouraged to migrate to UC_Secure as soon as possible.

IT@UC Governance Committees: Updates, Strategies

- **Information Security & Compliance** -- Bo Vykhovanyuk, Katrina Biscay, Matt Williams
  Table Top Exercise — Anita Ingram, Cindy Lusby

Anita opened the program with a brief overview of risk management and the risk Heat Map. She has moved the university to looking at risks from a holistic viewpoint. Risks can be both a positive (opportunities) and negative. IT ranks in

IT Managers Committee

Committee Co-Chair
Dominic Ferreri
Asst. Vice President, Client Services
ferrerd@ucmail.uc.edu
(513) 556-2039

Committee Co-Chair
Brian Verkamp
Asst. Dean, College of Education, Criminal Justice, and Human Services
brian.verkamp@uc.edu
(513) 556-2264

UNIVERSITY OF Cincinnati

the top 10 risks for the university. She gave an example of the ramifications of an incident where the university had to refund a semester of tuition. This would cause serious funding issues and possibly shut down the institution. She mentioned that Bo and Nelson are presenting the IT Enterprise Risk Management (ERM) survey to the Administration and Board.

Bo opened the table top exercise with a display of the heat map and a Risk Register. The register is a list of all possible risks that could affect the institution. After his overview, Bo then started the table top exercise by asking 34 questions regarding risks and their impact and likelihood.

Action Items:

What Have You Heard?

- Yu Chin inquired about Chris Edwards' departure. It was reported that in the interim Paul Foster would be taking over Chris' responsibilities for eLearning.
- Eric Tribbe reported that there are some new models on the Dell website.

Adjourn: The meeting was adjourned at 10:53 am.

REMINDER: Next month the IT Managers meeting will be located next door in room 454 University Hall.

Attendees: Andrew Becker, Don Hodges, Clarence Brown, John Kreimer, John Lawson, Don Rainwater, Yu-Chin Fu, Tom Cruse, Erma Fritsche, Nathaniel O'Der, Megan Pfaltzgraff, Matt Williams, Eric Tribbe, Bruce Burton, Bill Frigge, Dom Ferreri, Mel Sweet, Harry LeMaster, Jon Adams, Kent Norton, Vernon Jackson, Paul Foster, Dale Hofstetter, Jamie Byrne, Michael Tadele

Risk Tabletop Domain Legend

Unified Governance & Management of IT
Functions and resources typically centralized within the IT organization that usually have scope spanning the IT organization. In the majority of cases, these functions and resources are part of or are closely tied to the Office of the CIO.

IT Support Services
Functions and resources associated with providing general support for the institution that is not specific to teaching and learning or administrative applications.

Educational Technology Services
Functions and resources associated with and specific to supporting teaching and learning at the institution.

Research Computing Services
Functions and resources associated with and specific to supporting research at the institution.

Network & Data Centers Infrastructure
Functions and resources associated with supporting the Network and Data Centers operated by the institution.

Identity Management & Security Integration
Functions and resources associated with providing information and systems security services and programs for the institution, including directory, identity management, and access provisioning/de-provisioning functions and roles, etc.

Information Systems & Applications
All systems and applications not specific to other IT domain areas that are required for institution operations, including ERP and other administrative applications.

Risks:	Unified Governance & Management of IT	IT Support Services	Educational Technology Services	Research Computing Services	Network & Data Centers Infrastructure	Identity Management & Sec. Int.	Information Systems & App
IT governance and priorities not aligned with institutional priorities	✓						
Failure to designate leadership (e.g., an individual or individuals) for institutional oversight and strategic direction for IT operations	✓						
Failure to designate leadership (e.g., an individual or individuals) for institutional oversight and strategic direction for information security activities	✓						
No succession plan for key institutional IT leaders (e.g., CIO, CISO, CTO, CPO, etc.)	✓						
Relevant stakeholders not included in important IT investment decisions (e.g., priorities, technologies, new applications)	✓						
IT assets (e.g., hardware, devices, data, and software) and systems not prioritized based on their classification, criticality, and institutional value		✓			✓		
IT assets (e.g., hardw are, devices, data, and softw are), systems, and services outdated, do not support institutional needs (admissions, academic, business operations, research, etc.)	✓						
IT management aims and directions not communicated to critical user areas	✓						
Lack of shared understanding by IT and business units that affects IT service delivery and projects	✓				✓		
IT projects not managed in terms of budget, scheduling, scope, priority, and delivery	✓						
No process for identifying and allocating costs attributable to IT services	✓						
No process for measuring and managing IT performance		✓					
No process for managing IT problems to ensure they are adequately resolved or for investigating causes to prevent recurrence		✓				✓	
Incorrect information on public-facing institutional resources (e.g., w ebsite, social media streams)					✓		
Critical institutional business and academic data (e.g., admissions, business operations, research, etc.) not available w hen needed						✓	
Loss of access—for an unacceptable period of time—to IT systems and services hosted by another organization				✓	✓		

IT communications and netw orks not protected from complete or intermittent failure					✓			
Areas housing critical IT assets (e.g., hardw are, devices, data, and softw are) or services physically inaccessible, inoperable, or unsuitable for human access					✓			
Failure to make adequate plans for continuation of institutional business processes (e.g., admissions, academic, operational activities, and research) in the event of an extended IT outage					✓			
No coordinated vetting and review process for third-party or cloud-computing services used to store, process, or transmit institutional data		✓			✓			
Failure to create and maintain sufficient and current policies and standards to protect the confidentiality, integrity, and availability of institutional data and IT resources (e.g., hardw are, devices, data, and softw are)						✓		
Data breach or leak of sensitive information (e.g., academic, business, or research data)						✓		
Inadequate cyber security incident or event response						✓		
Failure to control logical access and incorporate principles of least functionality to IT resources (e.g., hardw are, devices, data, and softw are) and systems						✓		
Failure to control physical access to data centers/facilities and areas housing critical IT resources (e.g., hardw are, devices, data, and softw are) and systems						✓		
Failure to follow organized life-cycle management practices (development, acquisition, use, transfer, repair, replacement, destruction) for institutional IT resources and systems		✓						
Failure to document institutional IT infrastructure architecture and to implement change-control processes (including creating, maintaining, and revising baseline IT system configurations)					✓		✓	
Institutional IT communication and data flow s not documented		✓					✓	
Licenses and permits for institutional IT systems and softw are not maintained	✓							
No process for ensuring institutional data remain complete, accurate, and valid during input, update, and storage			✓			✓		
Audit logs on critical IT systems and processes not maintained		✓				✓		
Too few IT staff to ensure continuous IT system operations	✓				✓			
Users (e.g., students, faculty, staff, administrators, third parties) do not follow legal and regulatory requirements regarding the operation/use of IT systems and the use of institutional data	✓					✓		
Users (e.g., students, faculty, staff, administrators, third parties) do not follow university policies regarding the operation/use of IT systems and the use of institutional data	✓					✓		
Degree to w hich the data centers are distributed increases risk					✓			