# UNIVERSITY TECHNOLOGY ADVISORY COMMITTEE

WOU BOARD OF TRUSTEES

FINANCE & ADMINISTRATION COMMITTEE (FAC)

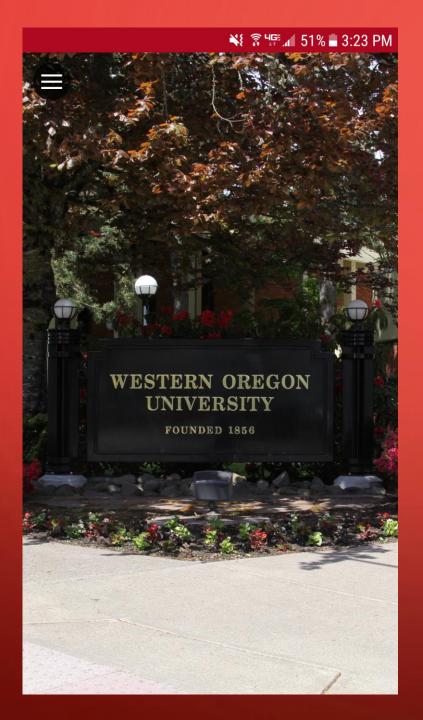
4/4/19

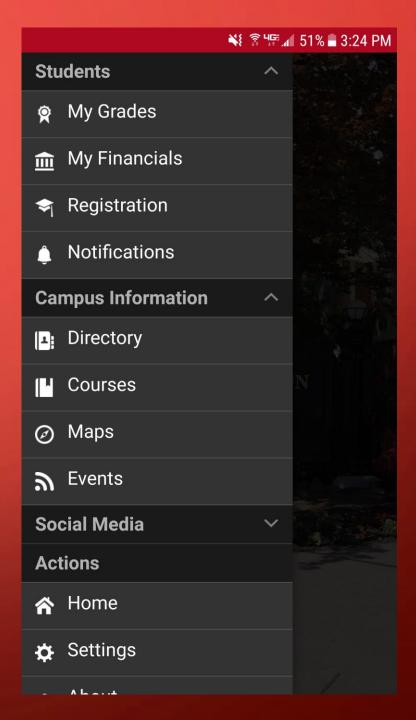
#### LMS REVIEW

- UTAC team (facilitated by Scott Carter)
- "Learning Management System"
  - Currently Moodle (open-source)
- Moodle satisfaction survey (sent March 2019)
  - Will do other market analysis/research
- Multiple LMS pilots (scheduled for Summer 2019)
- If a new LMS is selected, rollout tentatively Summer 2020

#### MOBILE APP

- UTAC sub-committee (chaired by Lisa Catto)
- "WOU App" can be downloaded here:
  - http://www.wou.edu/~mansot/mobileapp.html
- Current features:
  - Grades, Financials, Courses, Map, Employee directory, Social media
- Under final review by UTAC, then will be sent to Rex
- Goal: Launch in late May, available for SOAR





## DUO (MULTI-FACTOR AUTHENTICATION)

- Passwords are no longer sufficient
- DUO is an easy-to-use mobile application
- Rollout via Portal
  - #1: UCS staff members
  - #2: Banner (admin pages) users
  - #3: Faculty/Staff
  - #4: Students
- Hardware tokens available for campus members w/o a smartphone

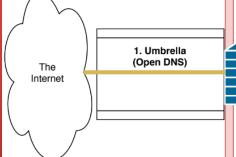
### UNIVERSITY TECHNOLOGY PLAN

- Currently reviewing Technology plans (content and layout) from other Universities
- Committee will continue to collaborate to build one for WOU, incorporating best practices from other Universities

## CYBERSECURITY

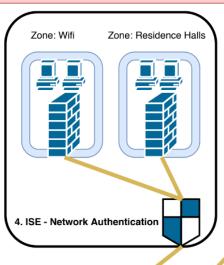
- Presentation at each UTAC meeting
  - 1/18: Layered security @ WOU (see next slide)
  - 2/22: CIS20 Framework
  - 3/22: DUO (multi-factor authentication)
- Developing a responsive security tool: redWOLF3

#### WOU: Layered Network Security



#### 8. External Support:

Penetration Testing (CoalFire)
Vendor Support
Vendor information sessions
Vendor product demonstrations
CIS 20 Framework
PCI education and testing





Zone: PCI (credit cards)



Zone: Other network zones



- 2FA: 2-factor authentication (Duo)
- System Logs (AP, LDAP, Portal, Web, Security, ...)
- OS Upgrades (Windows Server 2016, ...)
- App Upgrades (SQL Server, etc...)
- Group-based drive/file security
- SSL Always ON
- AccountLookup (password complexity)
- Internal PentrationTesting
- Network Drive Snapshots
- Sophos + InterceptX
- Email Security Appliances (+Archives)
- Physical Access Control & Survelliance
- Secure (VPN) access to Banner (local only)
- (Future): Custom log analysis system
- · Daytime monitoring of systems via 4k monitor



2. Border Firewall 3. FirePOWER (Internal Firewalls and Intrusion Protection: ~17k rules)

VPN: Remote Access











#### 7. User Security:

Information Security Training (Future)

Needed to educate WOU community about dangers of surfing "high risk" content or disabling security controls









6. Desktop Security:

- · Network login required
- Sophos + InterceptX
- . SCCM: Updates for Windows + Software
- JAMF: Updates for MacOS + Software
- · Limited admin privileges
- OS Upgrades (Windows 10, etc...)

Zone: Departments

Zone: Data Center

			PHASE1			
				DUE		
				BY		
		Overall completion %:	22.30	June 30		
			Initial review	% Data Center analysis complete	Data Center control in place	Data Center control automated
CIS Control 1: Inventory and Control of Hardware Assets				100.00		
	1.1	Utilize an Active Discovery Tool	Χ	Х		
	1.2	Use a Passive Asset Discovery Tool	Χ	X	Х	Х
	1.3	Use DHCP Logging to Update Asset Inventory	X	NA	NA	NA
	1.4	Maintain Detailed Asset Inventory	X	X		
	1.5	Maintain Asset Inventory Information	Χ	X		
	1.6	Address Unauthorized Assets	Χ	X	X	X
	1.7	Deploy Port Level Access Control	X	NA	NA	NA
	1.8	Utilize Client Certificates to Authenticate Hardware Assets	Χ	NA	NA	NA
CIS Control 2: Inventory and Control of Software Assets				10.00		
	2.1	Maintain Inventory of Authorized Software	Χ			
	2.2	Ensure Software is Supported by Vendor	Χ			
	2 3	Utiliza Saftwara Inventory Tools	Y			