THE UNIVERSITY OF ARIZONA

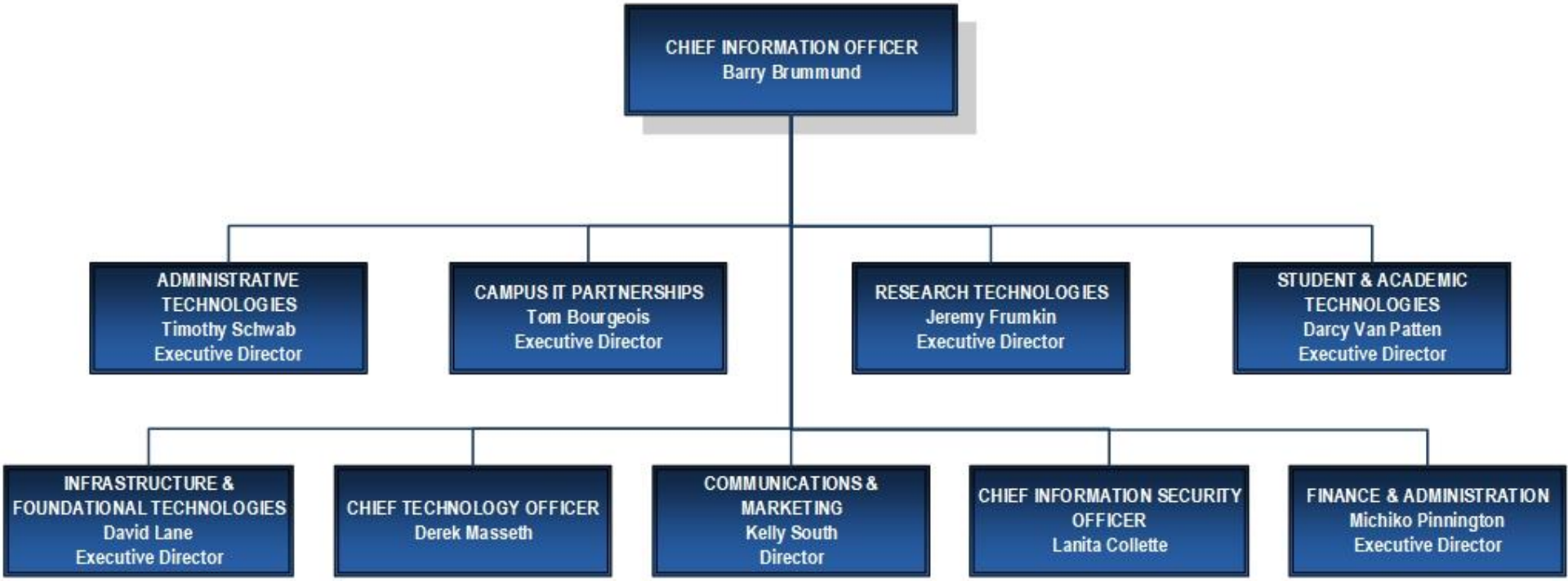
CABO Meeting

Barry Brummund
Chief Information Officer

June 13, 2018

UITS Organizational Structure

THE UNIVERSITY OF ARIZONA
University Information Technology Services



June 13, 2018

UITS Service Portfolio

Administrative Tech

UAccess Financials Employee, Learning, and Research; Docuware; Applicant Tracking Service; & Conflict of Interest

Campus IT Partnerships

Business Relationship Managers; Workgroup & Network Consulting; Campus Web Services; EAST; 24/7 IT Support Center; & Campus Switchboard

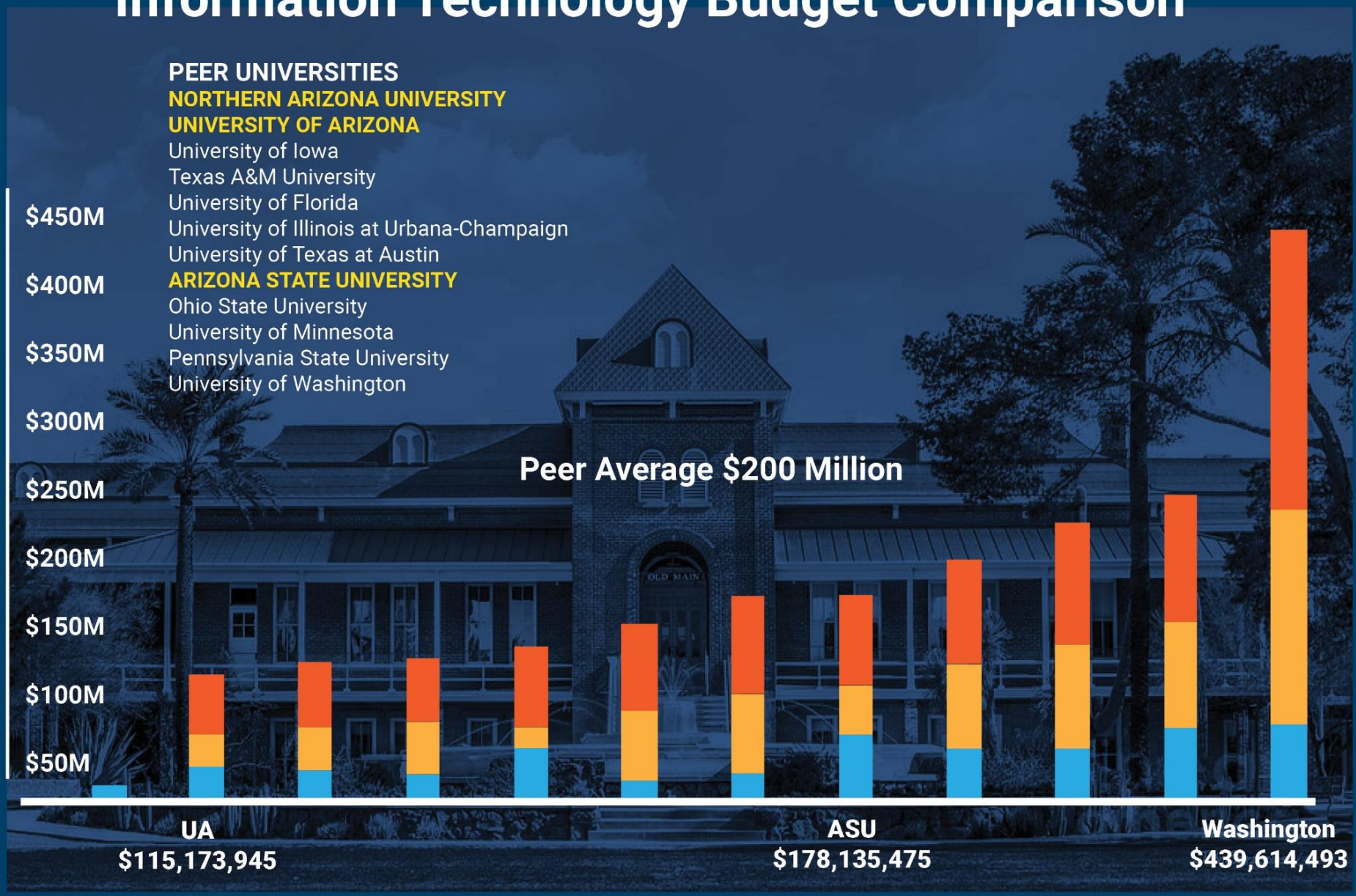
Research Tech

High Performance Computing Data Center; HPC Consulting; CUI; & Visualization Services

Student & Academic Tech

UAccess Student; Academic Technologies; Classroom Technologies; & Office of Student Computing Resources

Information Technology Budget Comparison



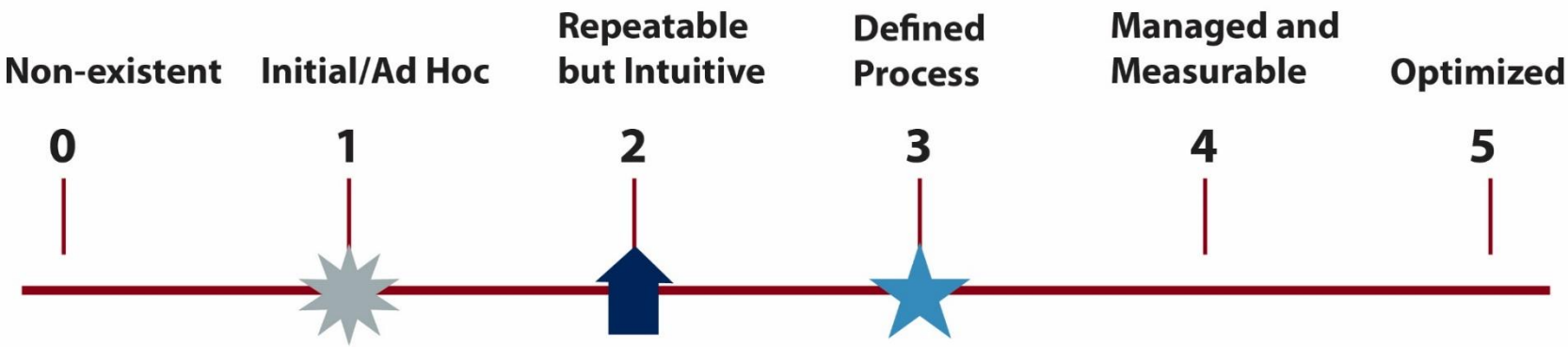

Q&A

Information Security Update

Final Summary of Facts – Performance Audit

- 60 page draft audit report
- Five findings and 23 recommendations
  - UA has low level of IT operation and process maturity.
- CIO has validated accuracy of audit findings.
- Final audit and news release will be published **June 22** by OAG.
- Media strategy developed with UA Communications.
- Action plan to address audit findings is in progress.

Figure 12 - Graphic Representation of Maturity Models



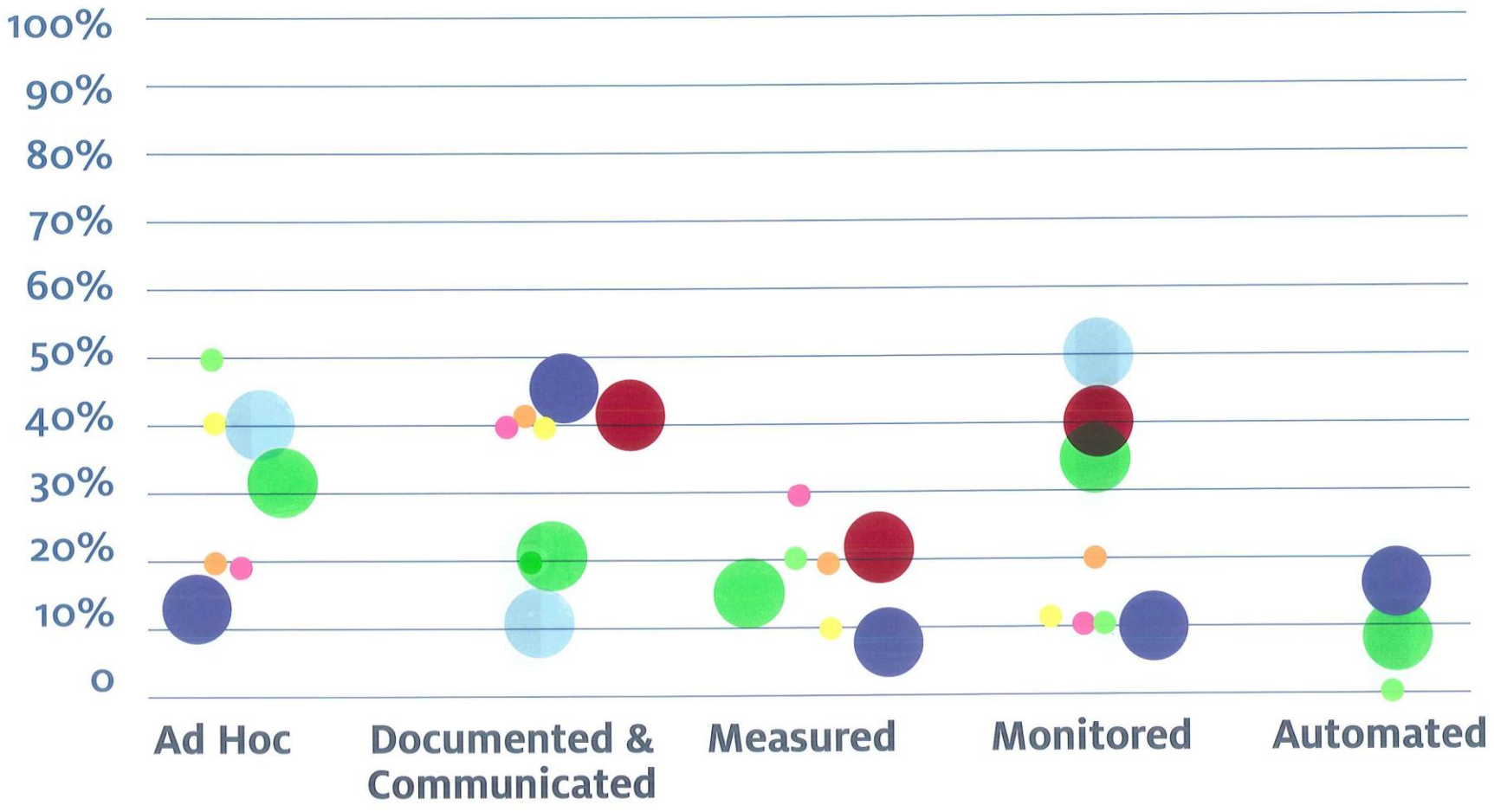
LEGEND FOR SYMBOLS USED

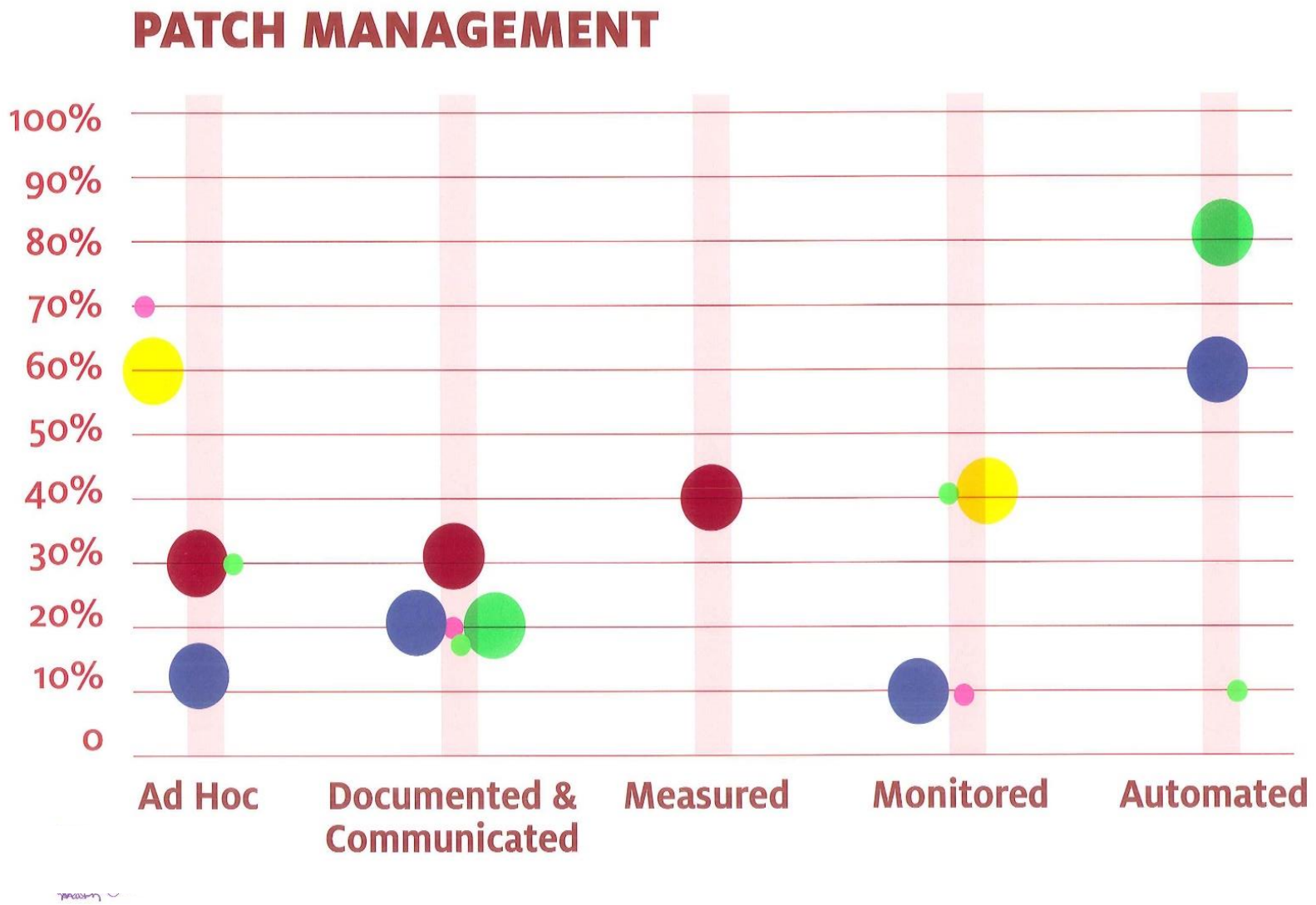
- Enterprise Current Status
- Industry Average
- Enterprise Target

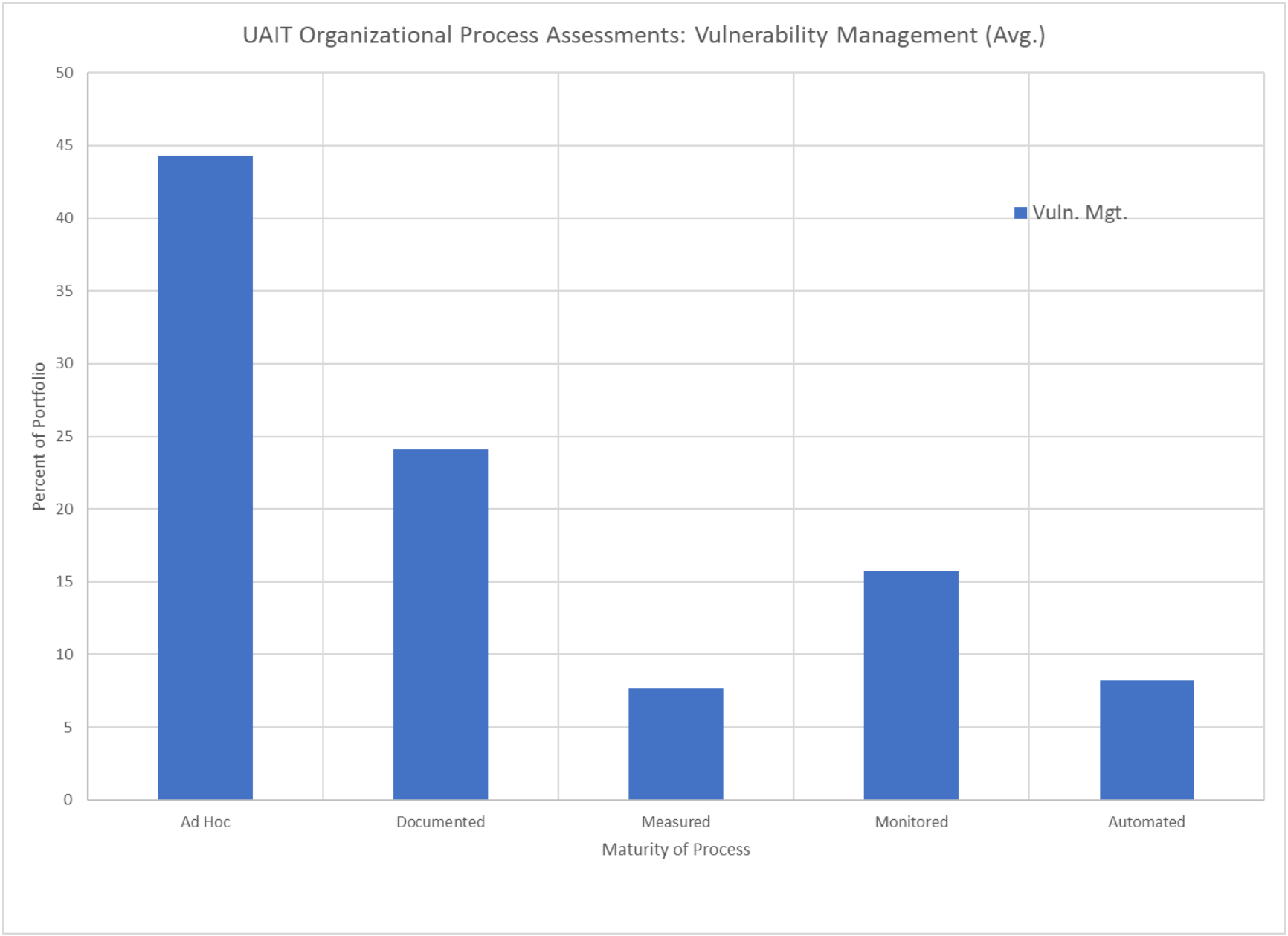
LEGEND FOR RANKINGS USED

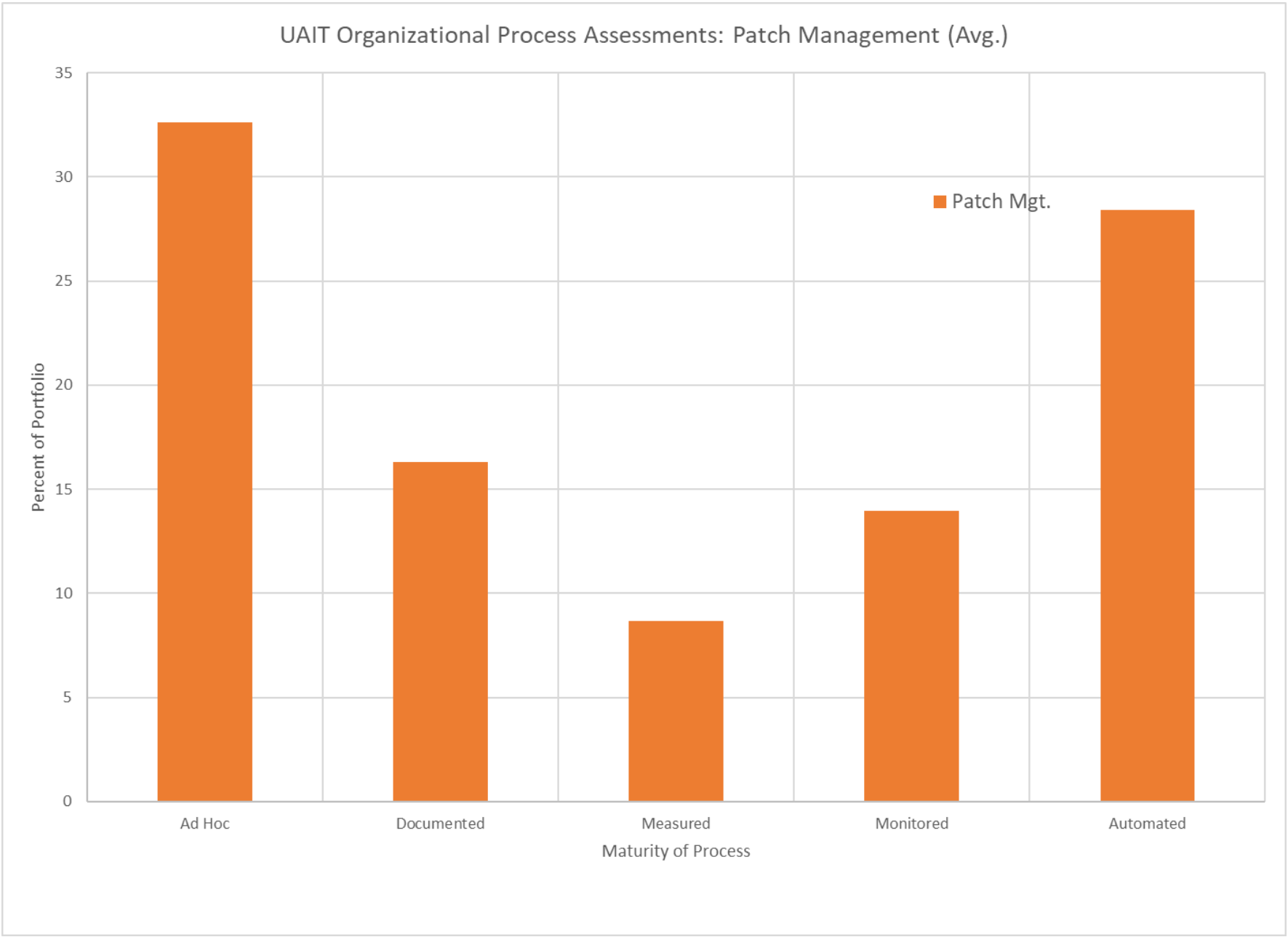
0 = Management processes are not applied at all.
1 = Processes are *ad hoc* and disorganized.
2 = Processes follow a regular pattern.
3 = Processes are documented and communicated.
4 = Processes are monitored and measured.
5 = Good practices are followed and automated.

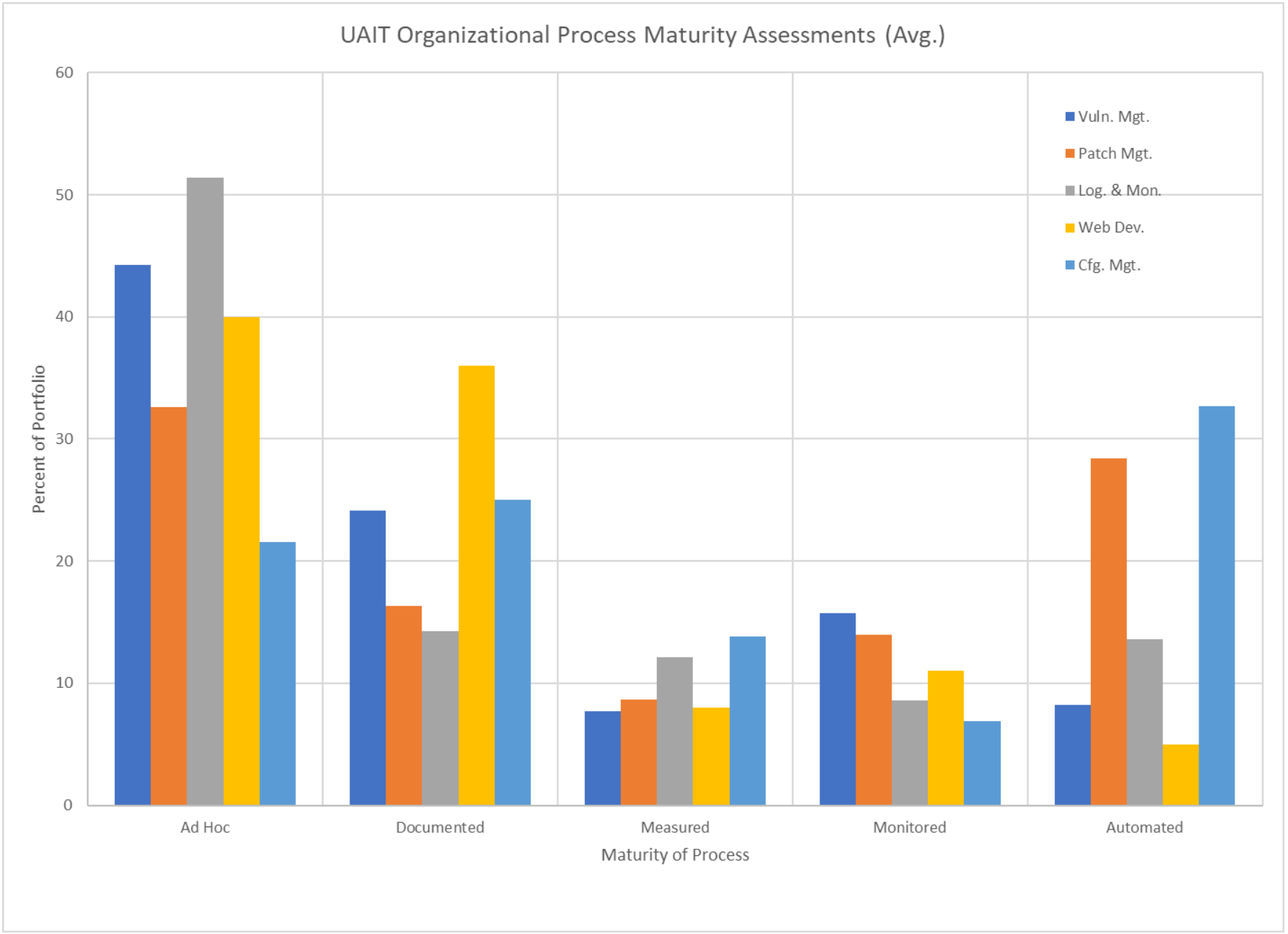
VULNERABILITY MANAGEMENT




PATCH MANAGEMENT
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0
Ad Hoc
Documented & Communicated
Measured
Monitored
Automated

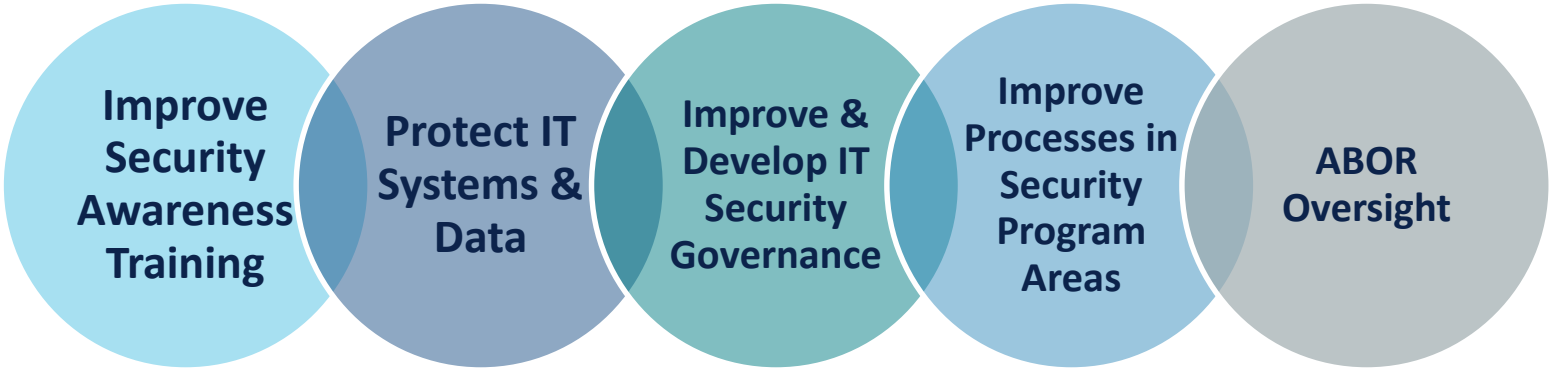

UAIT Organizational Process Assessments: Vulnerability Management (Avg.)
50
45
40
35
30
25
20
15
10
5
0
Percent of Portfolio
Vuln. Mgt.
Ad Hoc
Documented
Measured
Monitored
Automated
Maturity of Process


UAIT Organizational Process Assessments: Patch Management (Avg.)
35
30
25
20
15
10
5
0
Percent of Portfolio
Patch Mgt.
Ad Hoc
Documented
Measured
Monitored
Automated
Maturity of Process


UAIT Organizational Process Maturity Assessments (Avg.)
60
50
40
30
20
10
0
Percent of Portfolio
Vuln. Mgt.
Patch Mgt.
Log. & Mon.
Web Dev.
Cfg. Mgt.
Ad Hoc
Documented
Measured
Monitored
Automated
Maturity of Process

Audit Key Findings

- 23 recommendations in five areas:



- Positive highlights:
  - Recently hired CIO in April 2018
  - CUI environment that meets DoD security compliance
  - Better than the industry average against phishing attacks

Finding 1: Improve Security Awareness Training

- Implement security awareness training policy, procedures and automated tracking system to ensure compliance.
- Require annual security awareness training

Finding 2: Protect IT Systems & Data

- Develop and implement written policies and procedures for:
  - Vulnerability Management, Patch Management, Configuration Management, Web application Development, and Log Monitoring
- Develop and implement university-wide policies and procedures:
  - Aligned with best practices
  - For reporting identified noncompliance, evaluating instances of noncompliance, and correcting issues in a timely manner.

Finding 3: Improve & Develop IT Security Governance

- Develop and implement university-wide IT security strategic plan
- Policies to guide management and protection of IT systems and data
- Procedures for monitoring effectiveness of IT security practices and areas of noncompliance
- Policies and procedures to assess third parties for IT security requirements

Finding 4: Improve Processes in Security Program Areas

- Revise data classification policies and require units to develop IT systems inventory
- Regularly review and update data inventories
- Develop plan for ensuring units complete data inventories
- Revise IT risk assessment policies
- Fully implement IT risk assessment process for all units, compile and analyze data, and use results to establish university wide IT risk profile that is communicated to UA leadership.
- Develop procedures to train incident response personnel and assess if UA staff are complying with incident response policies

Finding 5: ABOR Oversight

- N/A for UA

Preliminary ISO Action Plan

	Audit Finding 1	Audit Finding 2				Audit Finding 3	Audit Finding 4		
ISO Project	Awareness & Training	Vulnerability & Patch Mgmt	Configuration Mgmt	Logging & Monitoring	Web App Development	Governance	Risk Assessment	Data Classification	Incident Response
Network Monitoring				X					X
Endpoint Security & System Management		X			X		X		X
Encryption Key Escrow							X	X	
Endpoint Malware Protection		X							X
Vulnerability Management		X			X		X		
Secure Internet Gateway		X							X
Cloud Access Security Broker							X	X	X
Advanced Threat Protection		X							X
Security Operations Center(SOC)	X	X	X	X					X
Log Management				X				X	X
Risk Assessment Program Improvements		X	X	X	X	X	X	X	X
Awareness/Training Program Improvements	X								
Departmental Security Plan Development	X	X	X	X	X	X	X	X	X
Mandatory NetID+	X					X	X		
ISO Service Catalog Development	X	X	X	X	X	X	X	X	X
Incident Response Plan Improvements	X					X			X
ISE Deployment		X		X				X	X
Network Segmentation		X		X			X		X
Security Policy Revisions and Additions	X	X	X	X	X	X	X	X	X
Metrics Development	X	X	X	X	X	X	X	X	X
Strategic Plan Development	X	X	X	X	X	X	X	X	X
Third Party Assess & Monitoring Program	X	X	X	X	X	X	X	X	X
Build Security Team	X	X	X	X	X	X	X	X	X

ISO Project Portfolio (DRAFT)

Finding	Project Status	Oct. 2017	Dec. 2017	Jan. 2018	Mar. 2018	Apr. 2018	May. 2018	Jun. 2018	Jul. 2018	Aug. 2018	Sept. 2018	Oct. 2018	Nov. 2018	Dec. 2018	2019+
2, 4	Network Monitoring														
2, 4	Endpoint Security														
2, 4	Endpoint Malware Protection - *solution in place*														
2, 4	Encryption Key Escrow - *Solution in place*														
2, 4	Vulnerability Mgmt.														
2, 4	Secure Internet Gateway														
4	Cloud Access Security Broker														
2, 4	Advanced Threat Protection														
1, 2, 4	Security Ops Center														
2, 4	Log Management														
2, 3, 4	Risk Assessment Program Impr														
1	Awareness Program & Training														
1, 2, 3, 4	Security Plan Development														
1, 3, 4	Mandatory NetID+														
1, 2, 3, 4	ISO Service Catalog														February
1, 3, 4	Incident Response Plan														Summer
	ISE Deployment														
1, 2, 4	Network Segmentation														August
1, 2, 3, 4	Policy Revisions and Additions														
1, 2, 3, 4	Metrics Development														
1, 2, 3, 4	Strategic Plan Development														
1, 2, 3, 4	Third Party Program														
1, 2, 3, 4	Build a Security Team														August
1, 2, 3, 4	Audit Process														

Protect

People

- Annual Information Security Awareness Training
- Two factor authentication

+

Systems

- Align central & campus IT workforce
  - Expand service desk & enterprise ticketing system
  - Operations as a Svc.
- Infrastructure Updates


Q&A