Issued by:

[2]/regulated[3] data, and external users increase risk, the recommended maturity level for IT controls is also higher. The increased maturity levels may increase IT cost.

---

[1] Associate Vice President, Facilities Management as of report issuance date.

[2] University of Arizona Data Classification Handling Standard (IS-2321) – Confidential data is defined as data protected as Confidential by law, contracts, or third-party agreement, and by the University for confidential treatment. Unauthorized disclosure, alteration, or destruction of this data type could cause a significant level of risk to the University or its affiliates. (Note: Prior to report issuance, this standard was replaced by Information Resource Classification Standard ISO-400-S1 and Information Handling Standard ISO-400-S2.)

[3] University of Arizona Data Classification Handling Standard (IS-2321) – Regulated data is defined as data controlled by federal, state, local, and/or industry regulations. These data are affected by data breach notification laws and contractual provisions in government research grants, which impose legal and technical restrictions on the appropriate use of institutional information.

Decentralized Unit IT General Controls

Decentralized Unit

Decentralized

General Control Objectives	Control Environment	Review Result	
		No.	Page
Achievement of the Organization's Strategic Objectives			

Review Results, Recommendations and Responses

1. The current change management process requires strengthening to reduce risk for mission critical assets.

Condition: A documented, integrated, and automated change management process is not in place to track change and approvals related to mission critical systems and confidential data.

Criteria:

- ISACA's COBIT Deliver, Service, and Support (DSS) domain includes six process areas related to managing IT services. The process areas include managing IT security services and business process controls.

- ISACA's COBIT Build, Acquire, and Implement (BAI) domain includes ten process areas, including processes related to managing change.

Cause: The University does not require decentralized IT units to implement effective IT processes, including change management.

Effect: Unmanaged change can cause severe impacts to information technology systems, services, and data. The impacts can include downtime, loss of data, and potential security incidents. The impacts can be potentially damaging if the systems and services are mission critical, or if regulated and confidential data are compromised.

Recommendations:

1. Implement a change management process that includes impact assessment and the automated capability to document, approve, and track change to software and hardware related to mission critical systems and confidential data.
2. Strengthen the Patch Management Policy by adding steps for tracking, testing, and approving a change in the policy, or include the patch management process in an overall change management process.

Management Responses :

1. Implemented May 2017. Facilities Management will document, integrate, and automate a change management process to track changes and approvals related to mission critical systems and confidential data by May 1, 2017. The process will review managing IT security services and business process controls. Additionally, a Change Management Policy was adopted.
2. Implemented May 2017. Facilities Management will add steps for tracking, testing, and approving a change in policy, or include the patch management process in an overall change management process. Additionally, a Patch Management Policy was adopted.

Exhibit