THE UNIVERSITY OF ARIZONA

Decentralized Unit IT General Controls Review: Facilities Management

Report FY16 - #10
Issued March 8, 2022

Submitted to:
Christopher M. Kopach, Associate Vice President, Facilities Management
Kevin D. Williams, Director, Facilities Management Information Technology

Copies to:
Institutional Internal Audit Review Board
Audit Committee, Arizona Board of Regents
Robert C. Robbins, President
Jon Dudas, Senior Vice President, Senior Associate to the President and
Secretary of the University
Liesl Folks, Senior Vice President, Academic Affairs and Provost
Laura Todd Johnson, Senior Vice President, Legal Affairs and General Counsel
Lisa N. Rulney, Senior Vice President and Chief Financial Officer, Business Affairs
Barry T. Brummund, Chief Information Officer
Ryan H. Goodell, Vice President, Facilities, Operations and Campus Planning
Mary Beth Tucker, Interim Chief Compliance Officer
Stacey Lemos, Assistant Vice President/Comptroller, Financial Management

Issued by: Sara J. Click, CPA, Chief Auditor
Internal Audit Department

Decentralized Unit IT General Controls: Facilities Management

Summary

Our review of the Information Technology (IT) General Controls for the Facilities Management (FM) decentralized IT unit was included in the approved Fiscal Year (FY) 2016 Audit Plan. This audit supports the University of Arizona (University) Never Settle Strategic Plan's Synergy strategic priority through the optimization, expansion, and alignment of IT capacity. This is our third audit of IT general controls within a decentralized IT unit, and our first specifically related to FM IT.

Background: The University, like many large organizations, supports both centralized and decentralized IT services. It is common for large organizations to centralize infrastructure services such as file server, network, and call center to gain efficiencies. Decentralized IT services often include application development, server room/data center, and end-user support. Decentralized IT services typically provide timely, customized support to departments that would be difficult for central IT to provide; however, the customized support increases IT costs and can impact data and system integration.

Oversight for the FM IT unit is provided by the Assistant Vice President for Facilities Management.[1] FM IT employs seven full-time staff and multiple students (equates to one FTE equivalent student position). IT services are provided to approximately 600 FM department users. Application development services are provided for systems servicing University staff and students. The FY 2015 budget was approximately $604,448 for hardware, software, and staff. Funding for the IT budget is provided by FM.

Applications and websites developed by FM IT support the FM department in their mission to provide services to the University and its students. FM IT supports the dedicated network supporting the University's utility plants. The components that make up this network are considered University level mission critical assets. A mission critical asset is defined as an IT system, component, application, or data that is critical to the University mission or daily operation. Since mission critical assets, confidential[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. (Note: Prior to report issuance, this standard was replaced by Information Resource Classification Standard ISO-400-S1 and Information Handling Standard ISO-400-S2.)

Decentralized Unit IT General Controls: Facilities Management

Review Objective: Our primary objective was to perform a review of IT general controls based on the ISACA[4] Control Objectives for Information and Related Technology (COBIT) framework. The COBIT framework has been used for previous IT general controls reviews to provide a level of consistency to the reader and objectivity for the reviews.

Scope: The scope of the review included processes and controls for FM IT that were in place from June 2016 to November 2016 for the following COBIT framework domains:

- Align, Plan, and Organize – Addresses the overall management of IT
- Build, Acquire, and Implement – Addresses application development and project management
- Deliver, Service, and Support – Addresses problem resolution, security management, and change management
- Monitor, Evaluate, and Assess – Addresses the strategic management review of IT

The fifth COBIT domain, Evaluate, Direct, and Monitor, is related to enterprise-level governance and does not address decentralized IT and, thus, was not within the scope of this review.

Methodology: Our review objective was accomplished by:

- Touring the FM IT server room;
- Touring the University Utility Plants to determine physical security controls and to assess the operational culture as well as the assets contained within the plants;
- Interviewing management within FM:
    - Assistant Vice President (AVP)[1]
- Interviewing management and staff within FM IT:
    - Assistant Director[5]
    - Application Development
    - Senior Systems Programmer
    - Systems Analyst
- Discussions with management within the CIO's Office:
    - Interim Chief Information Security Officer and Deputy Chief Information Security Officer
- Reviewing the *UA Cybersecurity Framework Risk Assessment* completed by FM;

[4] Formerly the Information Systems Audit and Control Association

[5] Director, Facilities Management Information Technology as of report issuance date.

- Reviewing existing University policies and standards related to information technology operations and information security;
- Reviewing existing processes and standards in place within FM IT;
- Reviewing industry standards related to logical and physical security from ISACA COBIT and the National Institute of Standards (NIST) 800-53 Rev 4 Moderate Baseline; and
- Utilizing standard questionnaires and audit procedures developed for the COBIT-based decentralized IT general controls reviews.

Conclusion: In summary, FM IT is effectively managed, and since they are a small group, many processes are informal. In some areas where risk is low, informal processes are sufficient; however, for mission critical assets and higher risk services and data, some processes such as change management require more maturity.

FM IT is an established department committed to providing quality service. The IT unit is small, consisting of seven staff responsible for providing support to FM, mission critical assets (the Utility Plant Network), and confidential data. FM IT demonstrated sufficient IT knowledge and experience.

The COBIT Align, Plan, and Organize (APO) and Monitor, Evaluate, and Assess (MEA) domains are focused on the assessment of controls related to the overall management of the IT operation. The FM AVP has implemented mature oversight and monitoring processes for FM as well as FM IT. The strong controls can be attributed to a 2013 Award for Excellence from APPA[6] for commitment to excellence in the field of educational facilities. FM actively collaborates with UITS regarding the Plant Network and recently had an external consultant review the security of the Plant Network. Our opinion is that the controls in place for the MEA domain were in the *Managed to Measurable* range on the COBIT maturity scale (see Exhibit on page 7), and controls for APO were in the *Repeatable to Defined* range.

Most IT operational controls in the remaining two COBIT domains were in the *Repeatable to Defined* COBIT maturity scale range. For IT units that support non-mission critical assets and lower risk data, this range would be sufficient in most cases. However, given the responsibility for mission critical assets and confidential data, some core processes require improvement to reduce risk. The recommended improvements are described below.

- The Build, Acquire, and Implement (BAI) domain is focused on managing solutions delivery and change to the technology environment. FM IT shares support responsibility with UITS

[6] APPA- Previously known as the Association of Physical Plant Administrators in the late 1960’s through the early 1990’s is known today as APPA: Leadership in Educational Facilities, and is most easily recognized and referred to as simply “APPA.”

for some components of the University Plant Network and is responsible for providing vendor access to the network. To manage risk, we recommend implementing an automated change management process as described on page 6.

- We observed controls and processes specific to the DSS, APO, and BAI domains that are considered low risk to the University, but may provide opportunities to gain efficiencies and reduce IT risk. Areas that could be reviewed/strengthened are application development practices and encryption requirements for managing and transmitting confidential data as specified in IS-2321. These areas were discussed with management during the audit.

According to the Institute of Internal Auditors International Professional Practices Framework, an organization is expected to establish and maintain effective risk management and control processes. These control processes are expected to ensure, among other things, that:

- The organization’s strategic objectives are achieved;
- Financial and operational information is reliable and possesses integrity;
- Operations are performed efficiently and achieve established objectives;
- Assets are safeguarded; and
- Actions and decisions of the organization are in compliance with laws, regulations, and contracts.

Our assessment of these control objectives as they relate to the decentralized FM IT unit is presented in the table on the following page.

General Control Objectives	Control Environment	Review Result	
		No.	Page
Achievement of the Organization's Strategic Objectives			
• A strategy and planning process exists that supports IT in attaining departmental goals and objectives.	Reasonable to Strong Controls in Place		
• Oversight of mission critical assets exists and is effective.	Reasonable to Strong Controls in Place		
• IT is managed (staff, budget, service, relationships, and vendors).	Reasonable to Strong Controls in Place		
Reliability and Integrity of Financial and Operational Information			
• Controls over financial/operational data exist and are effective.	Reasonable to Strong Controls in Place		
Effectiveness and Efficiency of Operations			
• Change Management, Problem/ Request Management, and Application Development exist and are effective.	Opportunity for Improvement	1	6
• Project Management, Business Continuity/Disaster Recovery Service Quality processes exist and are effective.	Reasonable to Strong Controls in Place		
Safeguarding of Assets			
• Processes for asset management exist and are effective.	Reasonable to Strong Controls in Place		
Compliance with Laws and Regulations			
• Regulated and confidential data are protected.	Reasonable to Strong Controls in Place		

We appreciate the assistance of University staff during the audit.

Sara J Click

Sara J. Click, CPA
Chief Auditor
clicks@arizona.edu

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

COBIT Maturity Model Rating Chart

5 -Optimized	An enterprise-wide risk and control program provides continuous and effective control and risk issue resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management, and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.	Mission Critical Assets (University) Regulated/Confidential Data Enterprise View/ Knowledge is Managed
4-Managed and Measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.	
3-Defined	Controls are in place and adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. While management can deal predictably with most control issues, some control weaknesses persist, and impacts could still be severe. Employees are aware of their responsibilities for control.	
2-Repeatable but Intuitive	Controls are in place but are not documented. Their operation is dependent on the knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritized or consistent. Employees may not be aware of their responsibilities.	Department Systems Internal/Public Data Instance View Dependent on Individual knowledge
1-Initial/Ad hoc	There is some recognition of the need for internal control. The approach to risk and control requirements is *ad hoc* and disorganized, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	
0-Non-existent	There is no recognition of the need for internal control. Control is not part of the organization's culture or mission. There is a high risk of control deficiencies and incidents.	