Decentralized IT General Controls Review: Student Affairs Systems Group

December 2015 **FY15 - #13**

Submitted to:

Kasandra Kay Urquidez, Vice President, Enrollment Management/Student
Affairs Advancement and Dean, Undergraduate Admissions
Timothy B. Edwards, Director, Student Affairs Systems Group

Copies to:
Institutional Audit Review Board
Audit Committee, Arizona Board of Regents
Andrew C. Comrie, Senior Vice President for Academic Affairs and Provost
Jon Dudas, Senior Vice President, Senior Associate to the President and Secretary of the University
Gregg Goldman, Senior Vice President for Business Affairs and Chief Financial Officer
Laura Todd Johnson, Senior Vice President, Legal Affairs and General Counsel
Melissa Vito, Senior Vice President for Student Affairs and Enrollment Management, and Senior Vice Provost for Academic Initiatives and Student Success
Karen Ann Williams, Interim Vice President for Information Technology and Chief Information Officer
Duc D. Ma, Interim Associate Vice President, Financial Services Office

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

This page left blank intentionally.

Summary

Our review of the Information Technology ("IT") General Controls for the Student Affairs Systems Group ("SASG") decentralized IT unit was included in the approved Fiscal Year ("FY") 2015 Audit Plan. This audit supports the University of Arizona ("UA") Never Settle Strategic Plan's Synergy strategic priority through the optimization, expansion, and alignment of IT capacity. This is our second audit of IT general controls within a decentralized IT unit.

Background:
The University is similar to many large organizations in that it 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 economies of scale. Central services assist the University in meeting its mission, goals and also in meeting regulatory, and legal obligations in a cost effective manner. Decentralized services often include application development, server room/data center, and end user support. Decentralized IT services can provide timely, customized support to departments with a justifiable need that would be difficult for centralized IT to provide.

Organizations that support centralized and decentralized IT service typically have strong IT Governance in place to support decisions regarding IT risk and investment. ISACA[1], a leading industry expert in IT Governance and IT controls, defines IT Governance as*:*

"IT Governance is the responsibility of the Board of Directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives."

IT Governance at the University is focused on the IT systems and services provided by University Information Technology Services ("UITS"). The current state of governance does not provide for IT oversight and risk assessment for the decentralized IT units.

The University's Chief Information Officer ("CIO") has direct authority over UITS and the Information Security Office ("ISO"). The CIO's office enables collaboration for the decentralized units in the form of committees and shared initiatives but does not have authority over the decisions made by the decentralized units. Decentralized units are not required to participate in the collaborative committees or to accept decisions regarding technical direction made by the CIO, UITS, or the committees.

[1] Formerly the Information Systems Audit and Control Association

Decentralized IT General Controls

Currently, departments and colleges can construct and manage data centers/server rooms, develop applications using any desired development tool and platform, manage decentralized email services, and implement remote access and authentication services (providing access to the University's network).

Validation is not required to justify cost, duplication of effort, or information security risk. Services such as data center/server room and application development can be costly and can present high levels of risk depending on the type of data managed and the criticality of the application to the University's operation. Since confidential[2] and regulated[3] data is stored on many of the decentralized servers, there is risk that information security controls may not meet University policy or regulatory and legal obligations. Likewise, units that develop and manage applications considered critical to the mission of the University may be at risk for continuity, vulnerability, product quality, and long term maintenance.

In March of 2015, the University updated policy regarding data classification (IS-2321). The new policy indicates that confidential data must be stored in the central data center. Policy requirements for regulated data are not as clear; the policy requires a review by IT staff prior. According to IS-2321, confidential data includes FERPA[4] data, and data related to applicant, alumni, parent, citizen, and immigration status. Regulated data includes social security numbers.

For most large organizations, controls for regulated/confidential data and mission-critical systems require a high level of maturity and optimization. This type of IT environment is expensive to maintain and therefore is typically not duplicated within organizations. The University has invested in an extensive information security infrastructure for enterprise systems and data located in the central data center and has an agreement with Amazon Web Services. However, this same level of security infrastructure may not in place within the decentralized server rooms. Application development practices related to information security (specifically vulnerability testing), remote access, authentication, network and firewall services are not consistent and are not validated by the ISO or the CIO.

[2] University of Arizona 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.

[3] University of Arizona 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.

[4] Family Educational Rights and Privacy Act ("FERPA")

Decentralized IT General Controls

IT is often further decentralized within the larger departments and colleges. Student Affairs and Enrollment Management and Academic Initiatives - Student Success (“SAEM-AISS”) supported the operation of seven IT units at the time of this review. The SASG IT unit is the largest of the units. SASG, is managed by the Vice President (“VP) Enrollment Management & Student Affairs Advancement and Dean, Undergraduate Admissions.

A survey of the IT units within SAEM-AISS indicated duplication of effort as the units operate independently. SAEM-AISS provides diverse and mission-critical services to the University and its’ students. The areas of responsibility are listed below along with the number of IT units.

- Admissions & Enrollment (2 IT Units)
- Campus Support
- Health & Wellness (1 IT Unit)
- Student Advocacy & Learning Support
- Student Involvement
- Student Services (3 IT Units)
- Academic Initiatives (1 IT Unit)

The IT units are managed by the University BookStores, Campus Health Services, Residence Life, Marketing, Arizona Student Unions, UA South, and Enrollment (SASG). Additionally, some groups within SAEM-AISS use UITS for support.

SASG employs 23 staff that provide IT services to approximately 1700 internal users (staff and student employees) and 900 devices. They also provide application development services to external users and to University students. In FY 2015, the SASG budget was approximately $1.6 million and included funding for staff, hardware, and software. Funding sources include SAEM-AISS departmental funds, state funding, and user fees (per device). Since SAEM-AISS departments can choose to hire their own IT staff, the revenue from fees fluctuates as the user base changes. SASG indicated that departmental funding from SAEM-AISS has steadily decreased over time; therefore, the reliance on the fee revenue has increased.

Applications and websites developed by SASG support admissions and enrollment, financial aid, electronic transcripts, and the Online Campus. SASG indicated that the systems and websites are considered critical to the mission of the University. The systems contain FERPA data (confidential), regulated data and are used by external customers. Since mission critical systems, regulated/confidential data, and external users increase risk, the recommended maturity level for IT controls is also higher. The increased maturity level may require additional funding and risk management oversight.

The table on the next page indicates the services provided by SASG. Overlap in the services provided by SASG and UITS is indicated by the blue shading.

Decentralized IT General Controls

IT Service	Service Provided by SASG	Service Provided by UITS
Application Development (department systems)	√	
Authentication	√	√
Business Continuity/Disaster Recovery		
Data Backup	√	√
Data Center/Server Room	√	√
Email		√
Call Center		√
Help Desk/Desktop Support	√	√
Remote Access (VPN)	√	√
Server Operations (cloud-based or on-premises)	√	√

As stated earlier, departments and colleges often make independent decisions regarding IT services; a cost and risk assessment is not required by the University even if the same service is offered by UITS. The following areas of IT are considered to be high risk for information security and financial impact:

- Authentication/Local Data Security
- Application Development
- Server Operations
- Data Center Services
- Disaster Recovery
- Remote Access

There is financial risk that the University is funding duplicate services, has unknown information security risk, and that product quality is not at optimal levels. To effectively manage risk and cost, it is critical for the University's decentralized IT units to have effective controls in place.

Review Objective: Our primary objective was to perform a review of IT general controls based on the ISACA 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 current processes and controls for SASG IT that were in place from June 2015 to September 2015 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.

Decentralized IT General Controls

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

Methodology: Our review objective was accomplished by:

- Touring the SASG server room.

- Interviewing management within SAEM-AISS:
  - Senior Vice President
  - Associate Vice President
  - VP, Enrollment Management/Student Affairs Advancement and Dean, Undergraduate Admissions
  - Director Freshman Recruitment/Admissions

- Interviewing management and staff within SASG:
  - Director (former and current)
  - Associate Director
  - Senior IT Support Analyst
  - Senior Developer

- Interviewing management within the CIO's Office:
  - Deputy, Chief Information Officer
  - Former Information Security Officer

- Reviewing existing University policies and standards related to information technology operations and information security.

- Reviewing existing processes and standards in place within SASG.

- 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.

- Utilizing standard questionnaires and audit procedures developed for the COBIT-based decentralized IT general controls reviews.

Conclusion:

SASG is an established IT unit committed to providing quality IT service. A review of the IT general controls in place for SASG IT resulted in our opinion that the controls are in the Repeatable to Defined COBIT maturity range. See Exhibit A for detailed information regarding the COBIT maturity levels. We found that SASG has sufficient process in place for the size of the group, however since the group is responsible for University mission critical systems and regulated/confidential data, controls should be strengthened to aid in risk management.

Decentralized IT General Controls

The COBIT Align, Plan and Organize domain is focused on the assessment of controls related to the overall management of the IT operation within the business unit, SAEM-AISS. Improvement in oversight and risk assessment are needed at the department level specifically for mission critical systems and at-risk data. As with other decentralized University IT units, SAEM-AISS may not have the funding or enterprise level IT expertise to ensure that risk is managed at appropriate levels. Budget constraints present risk for the server room which houses equipment to support the admissions and enrollment systems and regulated/confidental data. To reduce risk, we recommend that the current funding model be reviewed by SAEM-AISS.

SASG demonstrated sufficient IT knowledge and experience, however, decisions regarding high risk areas should not be made independently by each unit. Since the University does not require that mission critical systems undergo assessment regarding redundancy, availability, and continuity or provide standards for data protection, we recommend that SAEM-AISS proactively discuss the risks with the CIO.

The COBIT Build, Acquire, and Implement ("BAI") domain is focused on managing solutions delivery and the technology environment. SASG manages a large number of development projects, however, project approval and project management processes are not in place. Prioritization at the department level within SAEM-AISS is inconsistent and a process is not in place to assess impact to projects when priorities are adjusted. We recommend implementing sufficient control processes for project initiation/approval and project management to reduce risk related to mission critical systems and to manage customer expectations.

Strengthening the controls in the areas described above will assist SAEM-AISS with managing risk related to mission-critical applications and regulated/confidential data.

According to the Institute of Internal Auditors ("IIA") 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.

Decentralized IT General Controls

Our assessment of these control objectives as they relate to the decentralized SASG IT unit is presented in the table below.

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.	Opportunity for Improvement	1	8
• Oversight of mission critical systems is in place and effective.	Opportunity for Improvement	1	8
• 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 are in place and effective.	Reasonable to Strong Controls in Place		
Effectiveness and Efficiency of Operations			
• Problem/Request Management, Application Development and IT operational processes exist and are effective.	Reasonable to Strong Controls in Place		
• Project Management, Business Continuity/Disaster Recovery Service Quality processes exist and are effective.	Opportunity for Improvement	1, 2	8,11
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.	Opportunity for Improvement	1	8

We appreciate the assistance of UA Staff during the audit.

/s/

Rosemary R. Casteel, CISA
Auditor-In-Charge
(520) 626-4235
casteelr@email.arizona.edu

/s/

Sara J. Click, CPA
Chief Auditor
(520) 626-4155
clicks@email.arizona.edu

Review Results, Recommendations and Responses

1. Process areas for the Align, Plan, and Organize (“APO”) domain require improvement to reduce risk.

Condition:

Processes related to risk assessment, technical architecture, service level management, planning, and strategy require improvement to reduce risk and ensure sufficient funding. SASG is responsible for systems considered mission critical to the University’s strategic goals and for managing and transmitting regulated/confidential data (e.g. Admissions website, Online Admissions, and Singularity) that require higher levels of information security. The systems directly support the admissions and enrollment, financial aid, and electronic transcripts business functions.

Criteria:

- ISACA’s COBIT Align Plan and Organize (“APO”) domain includes thirteen process areas related to managing IT from a business perspective. The process areas include managing the IT framework, strategy, budget, service quality and risk.

- ISACA’s Monitor Evaluate and Assess (“MEA”) domain includes three process areas related to non-IT department management evaluating and assessing the following areas: performance and conformance, the system of internal control, and compliance with internal/external requirements (University, Legal, Regulatory)

- University Information Security Data Classification and Handling Standard (IS-2321) states that confidential data such as FERPA data be stored within the University UITS data center environment and regulated data environments must undergo review.

Cause:

- Mature risk management processes are not in place for SAEM-AISS and the University does not track and manage mission critical systems within the decentralized units.
- IS-2321 was published in March of 2015; SASG had been managing confidential and regulated data prior to the policy change.

Effect:

- Confidential (FERPA) and regulated data could be at risk.
- Mission critical systems could be unavailable in the event of a facility incident, security incident or operational problem.
- Integration with other SAEM-AISS and enterprise systems may not be seamless and efficient; therefore, customer experience and data management may not be optimal.
- Innovation levels could be less than optimal due to budget constraint and inoperability with UITS and other IT units.
- Costs could be increased at the department or University level due to duplication of effort, lack of a strategic plan and goals, and technical architecture decisions.
- Sufficient funding may not be available to meet security and criticality requirements.

Recommendations:

The following improvements should be considered to reduce risk and manage IT related costs:

1. Confirm the availability requirements for University mission critical systems and services and develop a plan to meet the requirements (develop plans for continuity, funding, etc.).
2. Obtain documented approval from the Information Security Office regarding the protection requirements for the University mission critical systems, confidential data and regulated data. Develop a plan to meet the requirements provided (For example, controls for remote access and privileged access, as well as obtaining required funding, etc.).
3. Establish a (1-3 year) IT strategic plan with goals.
4. Implement consistent meetings (i.e. quarterly) with representation from the CIO and other SAEM-AISS IT groups along with non-IT management to monitor project progress, discuss risk, cost, and areas where duplication of effort could be reduced.
5. Review technical architecture and development platforms with the CIO to validate technical direction and alignment with that of central IT services.
6. Implement service levels and a program to collect metrics related to customer service and automate escalation of overdue requests and problems.
7. Review the funding model to ensure that revenue from fees can be relied upon to meet future budget requirements.

Management Response:

1. We are compiling a list of applications and services that SASG provides and will submit that to the SAEM-AISS leadership to determine the availability requirements for each item. Once that list is prioritized, SASG will begin to assess our current resources and plans to support the availability requirements. That plan will be submitted to the division leadership to determine if it is economically feasible and if necessary, accept the risk. This will be in place by March 2017.

2. We are working with the ISO staff to determine approval requirements for SASG's process for protecting the confidential and regulated data stored on behalf of our customers. We will obtain approval by the end of December 2016.

3. We are currently putting together a project portfolio that will be submitted to SAEM-AISS leadership for evaluation and approval. This, along with our capacity planning exercises, will form the foundation for SASG's IT strategic plan and goals. This will be in place by the end of April 2017.

4. We have met with the SAEM-AISS IT groups and are trying to establish recurring meetings. Our first meeting was held on October 6, 2016, with a second meeting to be hosted by Residence Life tentatively scheduled for November 16, 2016.

   To date, a number of working groups have been established to explore coordinating and sharing resources.

5. We have contacted the CIO team and are awaiting guidance. The Deputy CIO is currently reviewing the requirements and we anticipate a resolution prior to January 1, 2017.

6. We are expanding the memorandum of understanding for all of the departments supported by SASG to start including SLAs. This will be in place by the end of June 2017. Automatic escalation and metrics collection are more difficult tasks but there are options that are being explored and evaluated.

7. A proposal to revise the SASG funding model to meet any future application development requirements to ensure continuity is being developed. If that proposal is accepted and funding provided, we can revise the model. The desktop support funding model doesn't need to be revised, but will certainly be adjusted to eliminate redundant functions. As this will most likely have to be phased in and will require approval from SAEM-AISS division leadership, a concrete timeline for implementation can't be given at this time. SASG will work to have a proposal ready for discussion with division leadership by the end of June 2017.

2. Key process areas for the Build, Acquire and Implement ("BAI") domain require improvement to reduce risk.

Condition:
SASG internal customers can request projects without justification resulting in the management of many projects from year to year. Due to frequently changing priorities, some projects span multiple years. SASG cannot easily communicate the impact of the change to management and the customers. Additionally, the lack of project data does not allow for the computation of the total cost of a project or for planning for subsequent years.

Criteria:
ISACA's COBIT BAI domain includes ten process areas, the applicable areas related to the finding are project management and project initiation and approval.

Cause:

- Non-IT department management does not require user requests for application development to be justified and project management processes are not required to be used by SASG.
- Enterprise IT governance does not require the decentralized units to implement process and control based on risk.
- Application development costs are not managed by project.

Effect:

- Business management has little visibility of the cost, status, and risk related to projects.
- Some projects using expensive development resources may not have sufficient business justification.

Recommendations:
We recommend that SASG consider the following:

1. Implement a project initiation and approval process within the business units.

2. Implement a project management process to augment the SDLC so that issues, risks, and status are documented and reported consistently.

Management Response:

1. SASG has instituted a project management process that will move responsibility for prioritizing and approving projects to the division leadership level. As requirements are made known, the SASG business analysts will work with the customer to determine the extent of work required to complete the project. Any requests that involve more than 10 hours total SASG work will be sent to the appropriate division head for approval and prioritization. A copy of that assessment will also be sent to the other division heads to ensure the division leadership has visibility of the project impact on future and ongoing requirements. This will be discussed with division leadership with a projected implementation of June 2017.

2. SASG has refined its project tracking and management process to provide a single view of the status and risk for all projects. This document will be provided to the division leadership on a quarterly basis to ensure division-wide visibility and awareness of all ongoing projects is maintained. This will be implemented March 2017.

Exhibit A

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 Systems (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 is able to 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.	

This page left blank intentionally.

4.C.2

This page left blank intentionally.