SAN DIEGO: AUDIT & MANAGEMENT ADVISORY SERVICES
0919

August 24, 2015

PIERRE OUILLET
Vice Chancellor/Chief Financial Officer
0007

Subject: ***Information Technology Governance and Planning Project 2015-04***

The final audit report for Information Technology Governance and Planning Audit Report 2015-04, is attached. We would like to thank all members of the department for their cooperation and assistance during the audit.

UC wide policy requires that all draft audit reports, both printed (copied on tan paper for ease of identification) and electronic, be destroyed after the final report is issued. Because draft reports can contain sensitive information, please either return these documents to AMAS personnel or destroy them at the conclusion of the audit. We also request that draft reports not be photocopied or otherwise redistributed.

David Meier
Director
Audit & Management Advisory Services

Attachment

cc: Judy Bruner
Cheryl Ross
Sheryl Vacca
Min Yao

UC San Diego

AUDIT & MANAGEMENT ADVISORY SERVICES

Information Technology Governance and Planning
August 2015

Performed By:

Tessa Melendez, Auditor
Jennifer McDonald, Manager

Approved By:

David Meier, Director

Project Number: 2015-04

Information Technology Governance and Planning
Project 2015-04

Table of Contents

Information Technology Governance and Planning
Project 2015-04

I. Background

Audit & Management Advisory Services (AMAS) has completed a review of Information Technology Governance and Planning as part of the approved audit plan for fiscal year 2014-15. This report summarizes the results of our review.

Information Technology (IT) Governance is a framework for implementing policies, business processes, and internal controls to effectively support all of the services that an IT department provides. The prime focus is how an organization utilizes IT to support its business strategy and objectives while creating value and managing risk. Effective IT Governance involves determining how the IT department is functioning, what key metrics are used, and what return IT is providing on the investments made.

The IT Governance Institute (ITGI) has outlined five key IT Governance focus areas containing a number of best practices. These five areas are: Strategic Alignment, Risk Management, Resource Management, Performance Measurement, and Value Delivery. The Control Objectives for Information and Related Technology (COBIT) framework developed by the Information System Audit and Control Association (ISACA) (***Attachment A***), incorporates a set of guidelines and supporting toolset for IT Governance and defines the five focus areas as follows.

- *Strategic Alignment* – The way IT and business strategy are aligned to ensure maximum efficiency.
- *Risk Management* – Involves a risk framework to identify and manage risk while preserving value.
- *Resource Management* – Matches IT resources and capabilities with business needs.
- *Performance Management* – Measures business performance in order to redirect and realign activities based on results.
- *Value Delivery* – Determines if the IT deliverable and business value were successfully delivered as promised.

A maturity model is a tool used to help classify the current state of IT Governance. The COBIT model, based on the ITGI framework, applies a maturity assessment of initial, repeatable, defined, managed, or optimizing to each of the five focus areas (***Attachment B***). The ideal state is at or near "optimizing", with the understanding that achieving an optimized state is a continual process rather than a precisely defined end-point.

The UCSD IT environment is decentralized with a number of campus departments providing services to their respective areas, and at times to the broader campus community. These departments include, but are not limited to, Administrative Computing and Telecommunications (ACT), Academic Computing and Media Services, and the Office of Engineering Computing. ACT provides campus services to include

developing and supporting applications for UCSD business functions and processes, administering network services, providing email services for faculty and staff, hosting campus websites, managing IT security, maintaining the UCSD Data Warehouse, and managing the ACT Helpdesk in support of all ACT services.

The campus is in the process of an IT Unification effort to combine ACT with six campus administrative IT units: Chancellor's Complex, Human Resources, Business Financial Services (BFS), Housing Dining and Hospitality, Resource Management and Planning, and University Advancement. The unification plan was developed to support the Chancellor's Strategic Plan, which highlighted the need for an agile, sustainable, and supportive infrastructure. The plan received approval from the Chancellor's Cabinet in October 2014 and is currently in phase one of three, with phase three scheduled for completion at the end of Fiscal Year 2016-17. IT Unification is intended to streamline the IT organization in order to deliver efficient and effective IT services, provide a model that will invite participation from other campus departments, and create cost savings and cost avoidance through continual process improvement.

II. Audit Objective, Scope, and Procedures

The objective of our review was to evaluate the effectiveness of governance for IT resources in assuring that IT operations and projects are in alignment with UCSD's overall strategies and business objectives.

In order to achieve our objectives we completed the following:

- Interviewed campus senior leadership from Academic Affairs, BFS, Research, and Student Affairs;
- Interviewed the following ACT personnel:
    - Assistance Vice Chancellor (AVC);
    - Manager of Portfolio and Communications for the Project Management Office;
    - Director of Finance, Administration, and Helpdesk User Services;
    - Executive Director of Enterprise IT Operations;
    - Senior Director of IT Initiatives;
    - Director of Middleware & Identity Management Services;
    - Director of Enterprise Network and Telecommunications;
    - Director of the Campus Web Office; and
    - Executive Director of Enterprise Information Systems.
- Reviewed ACT's vision, mission, core values, and strategic direction;
- Reviewed the 2-year Financial Applications Roadmaps for Fiscal Years 2014-15 and 2015-16;

- Reviewed ACT's project portfolio, quality assurance framework, disaster recovery plan, governance committees, change management process, service governance proposal, campus newsletters, and bulletins;
- Reviewed IT Unification details and program road map;
- Reviewed campus IT workgroups and committees, members, and charges; and
- Evaluated and assessed IT Governance practices against the COBIT framework for both practices used and maturity state in the following areas:

    - Strategic Alignment
    - Risk Management
    - Resource Management
    - Performance Management
    - Value Delivery

The scope of our review focused primarily on administrative computing resources and corresponding campus management oversight.

III. Conclusion

Based on our review procedures, we concluded that IT Governance was generally effective in assuring that IT operations and projects were in alignment with UCSD's overall strategies and business objectives. A formal framework to address campus IT Governance has recently been developed in the form of the IT Unification project. The continuous development of business processes that support all five focus areas, and the progress of IT Unification will strengthen the maturity capabilities in each area. The external perspective on IT Governance was overall positive, although we did note opportunities for improvement in communication, defined objectives with committees, addressing aging business systems in a timely manner, and staffing resources.

Observations and supporting comments are provided in detail in the remainder of this report.

IV. Observations and Supporting Comments

External Perspectives on IT Governance

During our review, we interviewed senior leadership from Academic Affairs, BFS, Research, and Student Affairs, to gain their perspective on IT Governance and how it was administered to support the Campus Strategic Plan.

We noted that communication with ACT was conducted through a number of informal and formal arrangements ranging from one-on-one meetings with various members of ACT senior leadership to participation in IT-related campus-wide workgroups and

committees. We noted overall satisfaction with the services provided by ACT and the accessibility to senior ACT leadership either via formalized committees or informal discussions on an as-needed basis.

In communicating their satisfaction with ACT, and in an effort to bring greater awareness to the campus, a number of respondents indicated their desire for ACT to more effectively communicate its mission and goals to those in the University who many not interact as closely with ACT. This communication would ultimately bridge the gap for those in the greater campus community who may not be aware of ACT and the services it provides. We noted that ACT has worked to continually update and reach the campus community in a number of ways, through biannual campus newsletters communicating project highlights, and email notices with pertinent and timely information affecting the campus systems and IT processes. The newsletters also include a message from the AVC and other campus-related IT news. Newsletters are posted online and mailed to executive staff, campus technical leaders, Provosts, and other ACT campus colleagues.

We heard a few concerns with the number of committees in place and the effort associated with being a member. While many customers were satisfied with the productivity and progress of various campus IT work groups and committees, others felt the number of groups and time requirements could lead to meeting fatigue and impact forward progress, especially if the following criteria is not defined: a committee purpose, a requisite reporting authority, or a specified outcome for the group. Feedback highlighted past committee recommendations that were created from work groups and tiger team reports but were never implemented, or implementation efforts were not reported out. We did note five ACT Policy Committee (ACTPC) subcommittees were created very recently to provide a focused direction for campus IT needs.

Concerns were also expressed regarding the long term campus plans for the Integrated Financial Information System (IFIS) and the Integrated Student Information Systems (ISIS). IFIS and ISIS have been updated using layers of add-on programming aimed to provide continued service in the short-term, but both systems were nearing the end of their useful life. Additionally, as staff with the specific knowledge required to update and maintain these layered add-ons leave UCSD, the systems would eventually become difficult to support. While ACT's strategic direction included evolving both IFIS and ISIS from current legacy applications to more modern technologies, the general consensus was that a defined action plan for system replacement and a specified timeline had not yet been identified. While a Student Information Systems Executive Committee (SISEC) did exist, it had not yet provided any specific details related to replacing ISIS.

Several positive remarks were given regarding ACT's customer service, such as their increased focus toward a more client-oriented environment and their assistance in providing timely data and information during external audits. However, some shared experiences in which ACT staffing resources may have impacted the opportunities to

expand the in-house knowledge base. For instance, outsourcing projects created missed opportunities for UCSD personnel to become familiar with integral project development, which may result in the inability to support the departments as effectively if the project was completed with ACT personnel. Customers also indicated that delays had sometimes occurred as a result of contractors leaving employment prior to project completion.

We noted that since the AVC's arrival, much work had been undertaken to review the IT Governance structure with an effort to strengthen practices. This view was also reflected in our interviews.

ACT's Comments

While a taskforce has not yet been formed to review and recommend a new student information system, co-chairs of the SISEC are aware of the business risk associated with the aging legacy system, ISIS. The risks and concerns for maintaining both ISIS and IFIS have been communicated to UCSD's Chief Financial Officer. The primary delay in moving forward with a replacement plan has been a result of the University of California's upcoming implementation of UCPath, a system-wide effort to align human resources and payroll processes and technology across campuses, medical centers, and research units. However, SISEC co-chairs have discussed a preliminary strategy for replacement of ISIS. Additionally, ACT will soon be working with IFIS stakeholders to develop a replacement strategy that will coincide with the ISIS replacement in an effort to minimize costs.

IT Governance Framework & Maturity Model

A formal campus-wide IT Governance structure was recently implemented with the IT Unification project. During our review, we noted a governance environment that included structured processes and appropriate leadership that ensured IT investments were aligned and integrated with the campus strategic plan. The IT organizational structure appeared appropriate for the current size and roles and responsibilities of ACT.

AMAS completed a maturity analysis for IT Governance based on the ITGI IT Governance model (***Attachment B***). Our analysis was intended to provide a snapshot of current-state capabilities that can be used as a benchmarking tool for future planning improvements as they are implemented. All areas were assessed to be above the initial maturity level (***Attachment C***). Of the five focus areas, one of the areas was at the managed level, two of the areas were defined, and two of the areas were repeatable. While none of the areas have attained a level of full optimization, all areas are projected to see direct benefit and increased maturity after IT Unification has been fully implemented.

- *Strategic Alignment*
  The IT Unification project was developed to align IT infrastructure with the Chancellor's strategic planning initiative. The Chancellor's Cabinet will oversee the IT Unification process with assistance from the Office of Strategic Initiatives, who will also help resolve issues. In addition, key strategic committees exist with project charters and reporting structures, appropriate memberships, and defined roles and responsibilities. These committees serve to align IT with the business strategy on a regular and continual basis. Further, five ACTPC subcommittees have recently been formed to provide oversight and expertise on a variety of campus IT initiatives. **Maturity Level: Managed**

- *Risk Management*
  Enterprise risk assessments are performed in support of the campus executive committee level via the Compliance, Audit, Risk and Ethics Committee, with IT participation. A detailed risk analysis was conducted, and mitigation plan identified, to address the risks associated with creating a shared IT services model through the unification plan. We did note that risk assessments were not formally performed within ACT for current business processes. However, the ACT IT security director is involved in a ACTPC subcommittee to address security and privacy, and is active with several system wide committees to address security policy and incident response. ACT performs operational processes to address risk primarily through quality assurance reviews and disaster recovery plans. Risks are also identified and evaluated at the project management level. **Maturity Level: Repeatable**

- *Resource Management*
  Future state projections (IT Unification) are intended to further align the IT services with the business objectives by defining a campus wide IT service portfolio. Each service catalog will include costs for delivery and defining the appropriate funding approach for each IT service. The current ACT Organizational structure is defined with the current state addressing appropriate activities and needs at the project management level. A comprehensive project portfolio is in place to manage projects and several committees have been identified to address outsourcing services, such as cloud based computing. **Maturity Level: Defined**

- *Performance Management*
  The IT Unification effort will seek to establish clear expectations that can be measured and managed. Service quality and transparency will be addressed by establishing service level agreements (SLA) for all ACT services and using metrics to measure performance in order to realign activities based on results. A standard practice for performance measurement did not appear to be in place, however; ACT uses the annual staff at work survey to measure customer service.

ACTPC subcommittees are in place to identify operational and strategic metrics, and provide oversight and expertise on a variety of campus IT initiatives. **Maturity Level: Repeatable**

- *Value Delivery*
  The IT Unification effort will seek to establish clear expectations that can maximize value. The effort will align resources to support the campus mission; reduce service overhead for the campus community; streamline funding for strategic initiatives; and eliminate redundant business processes. Currently, a structured framework appeared to be in place to ensure that campus projects are delivered on time and within budget. Change management practices are in place to ensure the integrity and accuracy of processes and projects. Quality Assurance reviews are used to provide guidance, technical expertise, and control to the project development teams, to ensure that customer requirements are met and value is maintained. **Maturity Level: Defined**

IT Governance continues in its maturity and is well positioned to leverage the governance structure to further enhance ACT's initiatives in supporting the campus strategic plan.

COBIT Framework (Based on the IT Governance Institute (ITGI))	**Strategy Alignment**	**Risk Management**	**Resource Management**	**Performance Measurement**	**Value Delivery**
Objectives	Maximize opportunities for the business use of IT while providing transparency and assurance that IT objectives are being achieved.	Address legal/regulatory compliance needs and understand/manage key operational risks.	Appropriately align IT capabilities with business needs.	Utilize real-time data to continuously improve IT delivery.	Optimize return on IT investments.
Key Considerations	Define IT Value Proposition	Determine Risk Appetite / Tolerance	Optimize IT Resources (e.g., people, technology)	Measure Strategy Implementation	Deliver Against Benefits Strategy & ROI
	Aligning IT strategy with the business strategy	IT Risk Awareness	Optimize Investment in Resources	Measure Value Delivery to IT Value Proposition	Meeting Business Requirements
	Deliver Value to Products and Services	Assuring investors and shareholders that a 'standard of due care' around mitigating IT risks is being met by the organization/Transparency	Optimize Knowledge (training, career development)	IT Service Level Agreements	Execute the IT Value Proposition
	Increase Managerial Effectiveness	Identify Risk Exposures	Providing organizational structures that facilitate the implementation of strategy and goals	Identify Operational and Strategic Metrics	Projects are delivered On Time / Within Budget
	Assist in Competitive Positioning	Risk Accountability	Co-sourcing / Outsourcing	Reporting	Integrity & Accuracy of Information
	Cascading IT strategy and goals down into the enterprise	Risk Tracking / Trending	Asset Management	Communication/Board & Executive Awareness	Obtaining value from IT investments
*Measurements	Strategy Definition & Planning/IT Oversight Functions (e.g., steering committee)	Risk Assessments and Mitigation Plans	Program, Project and Portfolio Management	Reporting tools and documents	IT Operational Processes (e.g., change management, service provisioning, continuity, security, etc.)

*Identified Measurements were used during audit development as assessment criteria

COBIT Framework (Based on the IT Governance Institute (ITGI))

Maturation

	Strategy Alignment	Risk Management	Resource Management	Performance Measurement	Value Delivery
Optimizing	IT is integral to achieving key business strategy objectives. IT proactively identifies and presents solutions to address strategic business challenges.	Risk management is a continuous process coordinated by the Board and senior management. The IT and enterprise level of risk tolerance is widely known.	IT resources are deployed strategically, considering internal and external sourcing models, and are based on defined evaluation criteria linked to business strategies.	A balanced scorecard approach is used to continuously monitor IT effectiveness. The scorecard is presented to the Board and other key executives.	IT is viewed as a strategic business partner. Solutions are presented to the business for review, are delivered on time/budget, and achieve the specified scope / objectives.
Managed	The Board and/or executives regularly evaluate alignment between IT and business strategies. Long- and short-term (or tactical) IT plans are mapped to business strategies.	Annual IT risk assessments are completed according to accepted methodologies. Preventative controls and monitoring mechanisms help to validate that key risks are appropriately managed.	IT project, purchasing, asset, and resource management processes are integrated and regularly measured for effectiveness.	IT fully understands the operational performance indicators for the enterprise, and these are regularly measured, monitored, and reported / summarized to IT stakeholders.	IT cost-effectively delivers high- quality services that meet the needs of the enterprise. Communication is frequent and structured. IT proactively seeks to enhance business value.
Defined	A formal process is used to evaluate and prioritize potential IT projects. Established criteria are consistently applied to facilitate cross-functional committee decisions.	IT risks are known, prioritized, and re-evaluated on a regular basis. Mitigation activities are defined for each risk and some monitoring structures are in operation.	IT skill set inventories are maintained and gaps are proactively identified. Formal processes exist to deliver IT personnel and assets to projects and maintenance efforts, as needed.	IT Service Level Agreements (SLAs) with the business are defined and tracked. A formal process exists to review, monitor, and communicate SLA results / performance.	IT is viewed as an enabler of business processes. There are activities in place to confirm requirements are being met, budget is kept, and goals are being achieved (e.g., ROI).
Repeatable	IT maintains existing systems but is viewed primarily as an order taker by the business units. Project decisions involve business personnel and require business cases.	IT risks have been identified and are being tracked with some mitigation activities in place. IT adequately responds when an incident occurs, but procedures are informal.	An organization-wide organization chart exists and is maintained. A list of applications and infra-structure assets can be generated, but it may not be reliable or current.	Some measures are regularly assessed across IT and are consistently communicated. There are gaps between what is measured by IT and what the business would like to have measured.	IT is viewed as a consistent utility provider. IT-business communication is fairly consistent, but interaction is typically issues-focused. There is little formal analysis of goal achievement.
Initial	IT projects and services may inconsistently align with business needs / objectives. Project decisions are made unilaterally or without established criteria.	IT lacks understanding of the risks that may exist across the entire company landscape. Risk assessment activities occur occasionally or in response to an incident.	IT reporting lines and skill sets are known by management, but they are not inventoried or organized. IT asset management is informal.	Some measures are assessed within a few IT areas. Results may be informally communicated and data are not used to source or proactively address issues.	Communications between IT and the business are irregular and/or ineffective. Projects are often delayed; do not deliver specified scope, and/or are over budget.

Capability Maturity Model	COBIT Framework (Based on the IT Governance Institute (ITGI))	**Strategy Alignment**	**Risk Management**	**Resource Management**	**Performance Measurement**	**Value Delivery**
	Objectives	Maximize opportunities for the business use of IT while providing transparency and assurance that IT objectives are being achieved.	Address legal/regulatory compliance needs and understand/manage key operational risks.	Appropriately align IT capabilities with business needs.	Utilize real-time data to continuously improve IT delivery.	Optimize return on IT investments.
	Key Considerations	Aligning IT strategy with the business strategy; Cascading IT strategy and goals down into the enterprise.	IT Risk Awareness; Identify Risk Exposure, Accountability, and Tracking.	Optimize IT Resources, Investments, and Knowledge. Providing organizational structures that facilitate the implementation of strategy and goals.	Identify Operational and Strategic Metrics; Provide Communication & Executive Awareness.	Meeting Business Requirements; Obtaining value from IT investments.
Optimized	*Continually improving process performance through incremental and innovative technological changes and improvements.*					
Managed	*Management can effectively control the IT processes without measurable impact to quality and services.*	IT Unification is the first strategic attempt to align IT function with organizational need. Additional committees are in place with senior leadership and IT representatives, which serve to align IT with the business strategy.				
Defined	*Standard processes are in place and used to establish consistency of process performance across the organization.*			Organizational structure is defined with the current state addressing appropriate activities and needs. Future state projections (IT Unification) further align the IT services with business objectives.		Activities are in place to ensure requirements, budget and goals are being achieved. Future state projections (IT Unification) support new strategic capabilities and IT needs of the campus.
Repeatable	*Some processes are repeatable, possibly with consistent results. Process discipline is unlikely to be rigorous, but where it exists it may help to ensure that existing processes are maintained during times of stress.*		Risk assessments are performed at an external level (CARE, Chancellor's Cabinet) with IT participation. IT operational processes are in place to identify, prioritize and mitigate risk.		ACTPC subcommittees are formed to provide oversight and expertise on a variety of campus IT initiatives. Annual surveys are used to measure customer service.	
Initial	*Processes are typically undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled and reactive manner by users or events.*					

Yellow = Current State