THE REGENTS OF THE UNIVERSITY OF CALIFORNIA
OFFICE OF ETHICS, COMPLIANCE AND AUDIT SERVICES

1111 Franklin Street, 5th Floor • Oakland, California 94607-5200 • (510) 987-0479 • FAX (510) 287-3334

Sheryl Vacca
SENIOR VICE PRESIDENT
CHIEF COMPLIANCE AND AUDIT OFFICER

April 20, 2012

DIRECTOR BITTLINGMEIER

Subject: Final Advisory Report No. P12A007, Review of Virtual Desktop Deployment

Attached please find the final report for: Advisory Project P12A007: Review of Virtual Desktop Deployment. With the issuance of this final report, please destroy any previous draft versions. We very much appreciate the assistance provided to us by you and members of your staff during our review. If you should have any questions, please feel free to contact me at 510-987-9646 (e-mail: Matthew.Hicks@ucop.edu).

Matt Hicks
Audit Director

Attachment
cc: SVP Vacca
CIO Weiss
Manager Loo
Contractor Unhavane

UNIVERSITY OF CALIFORNIA
ETHICS, COMPLIANCE AND AUDIT SERVICES
OFFICE OF THE PRESIDENT
ADVISORY SERVICES

REVIEW OF VIRTUAL DESKTOP DEPLOYMENT

Advisory Service No. P12A007
April 2012

Work Performed by:
Varsha Unhavane, Contractor

Executive Summary

Introduction

UCOP is currently evaluating the efficacy of a Virtual Desktop (VDI) for its IT needs. By migrating the desktop computing function to a centrally hosted service provider, UCOP hopes to increase the efficiency and value of its IT environment. A small device, known as a thin client, is deployed out to the workstations along with a monitor, keyboard and mouse. All the computing power is performed on the back-end servers and the user is presented with a desktop with the same look and feel they have today. The purpose of this advisory service is to provide a third-party assessment of the Virtual Desktop Infrastructure (VDI) deployment process.

Objectives and Scope

The primary objective of this review was to evaluate the deployment process for the Virtual Desktop (VDI) project. Given that the VDI project is inherently complex, Internal Audit approached the project from a high-level perspective. The review team structured its evaluation using a top-down approach, helping to identify broad areas of risk and potentially adverse impacts to the IT environment. The three (3) following areas were examined as part of the Virtual Desktop Infrastructure (VDI) review:

1. *Technology Overview*
    a. *Software Provider and Vendor Selection*
    b. *IT Security Risks and Implications*
2. *Business Case*
    a. *Proof of Concept and End User Experience*
3. *Financial Feasibility*
    a. *Costs and Expenditures*
    b. *Return on Investment*

Procedures Performed

In November 2011, the advisory team performed the following procedures to assess the overall health and stability of the quality assurance function:

- Obtained the following documentation to gather information surrounding the deployment process:

    a. *Virtual Desktop Infrastructure (VDI) Proof of Concept - Executive Summary*
    b. *Desktop Virtualization Feasibility Analysis*

- Interviewed key personnel to gather further information regarding the Virtual Desktop Infrastructure (VDI) deployment process.
- Reviewed documentation in conjunction with employee interviews to identify broad areas of risk associated with the deployment.
- Developed observations and noted possible opportunities for improvement.
- Discussed review findings with key stakeholders to validate issues and recommendations

Overall Conclusion

Based on the work performed, Internal Audit found that the process for the Virtual Desktop Infrastructure (VDI) deployment was generally adequate. Internal Audit noted several opportunities for improvement regarding UCOP's deployment methodology. For a detailed discussion on these issues, please refer to the subsequent pages of this report.

Opportunities for Improvement and Action Plans

1. **Prevent and Monitor Personal Use**

   IT security policies should be designed or updated to ensure that end users are not retaining personal information on a company machine. UCOP management should enforce these policies to mandate that UCOP's computers be used only for business purposes. Since information is managed from a centrally hosted service provider, continued personal use of company machines may increase the likelihood of many IT risks. These risks, which include data corruption and a massive loss of information, may adversely impact business processes and day-to-day operations. If these policies are already in place, enforcement should also be considered to help mitigate these risks. In addition, a communication plan for the Virtual Desktop Infrastructure (VDI) rollout should encourage users to clean all personal data prior to implementation.

2. **Compare Cost Benefits to Potential Risks**

   Return on Investment (ROI) is calculated on an ongoing basis as more and more users migrate to the Virtual Desktop Infrastructure (VDI) platform. Although cost savings are expected to increase as the number of new users grow, the deployment may come to a standstill should the project economics deteriorate. This may lead to a hybrid system, in which few users are on the new platform, and the remaining employees continue to use physical machines. Such a hybrid system may complicate the organization's technical infrastructure and IT administration. In addition, a hybrid system may increase the likelihood of cost and several IT risks, including security violations, data loss, and system failure. The project's heavy reliance on budgetary matters requires a careful consideration of these latent risks.

3. **Formalize Security Controls**

   Although security controls have been considered a part of the Virtual Desktop Infrastructure (VDI) project, they were not officially covered in the Proof of Concept phase. Interviews with key personnel indicate that the security piece has been contemplated on an informal basis. This consideration represents an important step in the deployment process, but should be supplemented with a formalized suite of security controls, in addition to the specific risks that they mitigate. As part of the advisory service, Internal Audit suggests that the following security features be formally considered and documented before implementation:

   a. *User Management and Administration*
   b. *Data Backup and Business Continuity*
   c. *Compliance with Security Policies and Procedures*
   d. *Encryption and Remote Access*
   e. *Monitoring and Corporate Governance*