NEVADA SYSTEM OF HIGHER EDUCATION
SYSTEM COMPUTING SERVICES
CLOUD COMPUTING MANAGEMENT
Internal Audit Report
January 1, 2016 through June 30, 2016

GENERAL OVERVIEW

Cloud computing is a method of suppling network and computing resources in a utility like model that allows for greater flexibility and scalability. Service models include: Infrastructure as a Service (IaaS); Platform as a Service (PaaS); and Software as a Service (SaaS). IaaS encompasses fundamental computing resources such as processing, storage and network assets. PaaS allows the deployment of applications – either created or purchased onto cloud based platforms. SaaS provides the ability to use the provider's software on cloud infrastructure. There are also hybridized versions of the various models. There are several benefits to the customer with the cloud model, including, provisioning resources dynamically to meet demand, focusing resources on core issues rather than IT operations and skillsets, and containing cost. The risks of applications processed in the cloud are similar to outsourcing; however, there are additional risks with cloud operations. Some of the more salient concerns are greater reliance on third parties, increased complexity in regulatory and legal requirements, and security concerns. NSHE has made a significant shift and commitment to the cloud environment with recent projects. In addition, institutions have begun utilizing cloud based services and self-provisioned cloud services such as Evernote, Dropbox, and Google Drive, and are being utilized on a wide range of devices across NSHE.

SCOPE OF AUDIT

The Internal Audit Department has completed a review of Cloud Computing Management at the System Office of the Nevada System of Higher Education. We conducted our review between January and June of 2016.

Our review was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors, and included interviews of System Office personnel, reviews of contracts and records, and other auditing procedures as we considered necessary. The testing included, but was not necessarily limited to the following.

1. Reviewing policies and procedures regarding Cloud Computing governance and oversight.
2. Reviewing Cloud Computing contracts for key provisions.
3. Reviewing organizational plans and strategies related to Cloud Computing.
4. Interviews with key personnel with knowledge of cloud contracts and security risks.

In our opinion, we can be reasonably assured that the management of Cloud Computing at the System Office is functioning in a satisfactory manner, with the exception of the areas mentioned below. We believe that implementation of the following recommendations would help mitigate risks and improve Cloud Computing processes within the System Office and across NSHE.

GOVERNANCE AND OVERSIGHT

There has been a lack of oversight and governance with regard to the evaluation, planning and implementation phases of cloud computing projects. Without the checks and balances of the governance process, issues that can be addressed in project evaluation and

planning could become costly later in the project life cycle. While NSHE has some policies and procedures regarding information security and oversight/governance, they have not been applied at the IT project level. Chapter 4 Section 9 of the Board of Regents Procedures and Guidelines manual discusses an interim information security plan, but this plan is specific to Graham-Leach-Bliley act targeted data. In NSHE's case, this means Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA). For projects that do not touch on those data types, there are no governance guidelines.

We recommend that NSHE as a system (including all Institutions) select and implement a comprehensive governance model for IT projects that includes proper representation across the system and involvement of the Information Security Officers from each campus and the System Security Officer.

Institution Response:

We agree with this finding. NSHE is in the process of implementing an Information Security Governance model that includes representation from each institution and System Computing Services. The proposed Information Security Officers Council will be uniquely positioned to engage in the security aspects of all NSHE-wide IT projects. This new model should be fully in place by April, 2017.

Follow-Up Response:

NSHE has established an Information Security governance model consisting of an Information Security Officers Council, Information Security Steering Committee, and Internal Audit. These groups are currently engaged and will be engaged in all future large NSHE-wide IT projects. We ask that this item be closed.

SECURITY

Our review of projects noted an opportunity to enhance the evaluation of security considerations during the early stages of a project. The lack of a proper security evaluation at the outset could mean exposure to unnecessary risk with regard to potentially sensitive information

being made available in the public domain. For specific projects, the design of the security is being led by an outside consultant. The System Security Officer and Information Security Officers from the institutions should be considered when projects are being evaluated and as noted above, there is no overall framework for project governance that should include such security vetting.

We recommend that information technology projects include a proper evaluation of the security considerations during the evaluation phase of the project. We further recommend that security design components of such projects have major involvement of SCS/NSHE personnel.

Institution Response:

We agree with this finding. NSHE is in the process of implementing an Information Security Governance model that includes representation from each institution and System Computing Services. A change in IT leadership has placed greater emphasis on security oversight on current and future projects and will continue to embed security early in the IT project lifecycle.

Additionally, the proposed Information Security Officer's Council, a component of the overall governance model, will be tasked with providing an NSHE-wide, security-focused working group for earlier security vetting of NSHE IT projects. System level project management will be required to include this security group as part of the overall project lifecycle.

Follow-Up Response:

NSHE has established an Information Security governance model consisting of an Information Security Officers Council, Information Security Steering Committee, and Internal Audit. The NSHE Chief Information Security Officer is involved in early planning with NSHE-wide IT projects and the Security Officers Council is currently engaged and will be engaged in all future large NSHE-wide IT projects. We ask that this item be closed.

CLOUD COMPUTING POLICIES - NSHE

We noted system-wide policies do not exist that address Cloud Computing contracts or the use of self-provisioned cloud services. Uniform and knowledgeable guidance in this area could significantly mitigate risk, which includes but is not limited to entering into unfavorable

contracts for cloud services, loss of data if the cloud provider were to fail, sudden loss of service and/or data, loss of control of NSHE data to unsecure services, and unauthorized data exfiltration. The development of such policies would be beneficial across NSHE in establishing minimum requirements and guidance in this area.

We recommend that Cloud Computing policies be developed for inclusion in the Board of Regents Handbook and/or the NSHE Procedures and Guidelines Manual. We recommend the policies address general guidelines/best practices for establishing and administering Cloud Computing contracts.

Institution Response:

We agree with this finding. As stated, NSHE is in the process of implementing an Information Security Governance model that includes representation from each institution and System Computing Services.

A component of this governance model is the Information Security Officers Council whose members will be tasked with developing and proposing policies related to cloud computing and use of self-provisioned cloud services. It is anticipated that the newly formed group will address this topic by the end of FY2017 and produce a draft policy for review in this time frame.

Additionally, this group will be engaged in developing strategies to educate the NSHE user community on the appropriate use of cloud services.

Follow-up Response:

An initial discussion of a Cloud security policy was discussed with the Information Security Officers Council and the Information Security Steering Committee at their quarterly meetings. This is such a broadly defined and dynamic arena of computing that any policy needs to be based on data classification and appropriate use rather than technology.

In discussions, the Information Security groups have determined that a prerequisite to any Cloud Computing policy is the establishment of an NSHE data classification. Any such standard must encompasses work already done by some of our Institutions to prevent rework while providing enough guidance for other Institutions. This, in itself, is a major undertaking. Once completed and approved, a policy detailing the acceptable uses of Cloud Computing resources can be started.

It is anticipated that this type of widely sweeping policy especially in an area as ubiquitous as "cloud computing" will take at least a year after the data classification standard is established. A reasonable target for to complete this, considering the prerequisite work required and the requirement to included consensus among all Institutions, will be late 2018 – early 2019.

The Internal Audit Department appreciates the cooperation and assistance received from SCS during this review.

Reno, Nevada
August 17, 2016

/-----SIGNATURE ON FILE-----/
Grant Dintiman
IT Auditor

/-----SIGNATURE ON FILE-----/
Joseph Sunbury
Chief Internal Auditor