COLORADO
Secretary of Technology &
Chief Information Officer
Governor's Office of Information Technology

Suma Nallapati
601 East 18th Avenue, Suite 250
Denver, CO 80203

September 11, 2015

Dianne E. Ray, CPA
State Auditor
Colorado Office of the State Auditor
1525 Sherman St., 7th Floor
Denver, CO 80203

Dear Ms. Ray:

In response to your request, we have prepared an updated status report regarding the implementation of audit recommendations contained in the October 2014 Performance Audit of the Systems Backup and Recovery. The attached report provides a brief explanation of the actions taken by the Governor's Office of Information Technology to implement each recommendation.

If you have any questions, please do not hesitate to contact me at 303.764.7708 or by email at suma.nallapati@state.co.us.

Sincerely,

Suma Nallapati

Secretary of Technology and Chief Information Officer

AUDIT RECOMMENDATION STATUS REPORT

AUDIT NAME: Systems Backup and Recovery, IT Performance Audit, October 2014, Governor's Office of Information Technology
AUDIT NUMBER: 1403P
DEPARTMENT: Governor's Office of Information Technology

DATE OF STATUS REPORT: September 11, 2015:

SUMMARY INFORMATION

Rec. Number	Agency's Response	Original Implementation Date	Implementation Status	Revised Implementation Date (If applicable)
1a	Agree	July 2015	Implemented	N/A
1b	Agree	December 2016	Partially Implemented	N/A
2a	Agree	December 2016	Partially Implemented	N/A
2b	Agree	July 2015	Implemented	N/A
2c	Agree	December 2016	Partially Implemented	N/A
2d	Agree	December 2016	Partially Implemented	N/A
3a	Agree	July 2015	Implemented	N/A
3b	Agree	December 2016	Partially Implemented	N/A
3c	Agree	December 2015	Implemented	N/A
4a	Agree	July 2015	Implemented	N/A
4b	Agree	December 2016	Partially Implemented	N/A
5a	Agree	July 2015	Implemented	N/A
5b	Agree	December 2017	Partially Implemented	N/A
6a	Partially Agree	December 2016	Implemented	N/A
6b	Agree	July 2015	Implemented	N/A
7a	Agree	July 2015	Implemented	N/A
7b	Partially Agree	July 2015	Implemented	N/A

DETAIL OF IMPLEMENTATION STATUS

Recommendation No. 1:

Ensure that backup and recovery procedures for OIT-managed systems are in place and appropriate by:

A. Communicating the relevant backup and recovery policies to OIT personnel responsible for establishing, implementing, performing, and managing backup and recovery procedures and establishing a mechanism to hold IT staff accountable for implementing backup and recovery policies and procedures.

Current Implementation Status for Rec. 1, part a: Implemented.

Agency's Update:

OIT documented, published, and communicated The Colorado Information Security Policies, which include policies such as backup and recovery, access management, and data classification. In addition OIT established an agency specific operational checklist, as well as a Backup and Recovery policy and procedures in July 2015 to establish guidelines and a consistent reference point for ensuring backup process is followed. OIT also added performance measurements to annual staff plans requiring all OIT policies be reviewed. OIT has established multiple avenues to communicate policies to relevant staff such as a quarterly newsletter, trainings, operational managers meetings, etc.

B. Ensuring that backup and recovery procedures are developed and implemented in accordance with agency Disaster Recovery Plans. This would include coordinating with agency personnel to identify system backup and recovery requirements in agency Disaster Recovery Plans.

Current Implementation Status for Rec. 1, part b: Partially Implemented.

Agency's Update:

Implementing an enterprise wide backup and recovery solution for each application and system for each participating department within two years is an aggressive goal. OIT is fully committed to this goal and has already completed the initial backup and recovery assessment that required synthesizing a large amount of data such as backup windows, change rate, failures and reliability, client tuning, capacity, and retention for each application and system. OIT has secured additional funding to fully deploy an enterprise wide backup and recovery solution which, at a minimum, requires infrastructure build out (power and cabling at data centers, racks, etc.), offsite data replication, upgrade and expansion of network connectivity, procurement of disk hardware and software, procurement and deployment of data protection software, implementation of Load Balancer functionality, etc. Once the basic infrastructure is available, OIT will run test data through a failover and recovery process. Upon completion of successful testing of data recovery, critical and essential systems can be targeted for integration into the backup and recovery solution. While backup and restoration exist for Critical, Essential, and highly Important platforms

today, Disaster Recovery will be tested and incorporated for Critical and Essential platforms. Improving the existing Data Backup and Recovery operations, efficiency, standards, and centralization across the enterprise is required to reach Disaster Recovery and documenting feasible recovery plans with agency personnel as a final outcome. We will strive to implement this audit finding by its original implementation date of December 2016.

Recommendation No. 2:

Ensure that backup and recovery monitoring processes are effective by:

A. updating policies by adding monitoring requirements and standards that ensure the availability of information systems and data through backup and recovery.

Current Implementation Status for Rec. 2, part a.: Partially Implemented.

Agency's Update:

OIT documented, published, and communicated The Colorado Information Security Policies and procedures pertaining to Infrastructure Services Backup and Data protection, which include policies and procedures around monitoring. While the policies and procedures are in place, in order to ensure availability of information systems and data through backup and recovery it is imperative that required infrastructure and tools and technology are in place as well. As listed in recommendation 1.b this is a multi-year projects and which will ensure availability of information systems and data through backup, recovery, and disaster recovery.

B. establishing processes to communicate updated OIT backup and recovery policies to personnel responsible for managing monitoring processes and holding personnel accountable for implementing the policies.

Current Implementation Status for Rec. 2, part b.: Implemented.

Agency's Update:

OIT documented, published, and communicated The Colorado Information Security Policies, which include policies such as backup and recovery, access management, and data classification. In addition OIT established an agency specific operational checklist, as well as a Backup and Recovery policy and procedures in July 2015 to establish guidelines and a consistent reference point for ensuring backup process is followed. OIT also added performance measurements to annual staff plans requiring all OIT policies be reviewed and understood. OIT has established multiple avenues to communicate policies to relevant staff such as a quarterly newsletter, trainings, operational managers meetings, etc.

C. Correcting configurations on systems that can support automated backup and recovery notifications to notify appropriate personnel of backup status in a timely manner.

Current Implementation Status for Rec. 2, part c.: Partially Implemented.

Agency's Update:

OIT is re-evaluating all the existing infrastructure tools and techniques and working towards an enterprise wide solution as listed in rec 1.b. OIT's new Backup and Recovery policy identifies the requirements to establish automated alerting on failed backup processing. Through OIT's new Backup Colorado project, auto-alerting will be implemented for systems that are not currently utilizing the functionality

D. Ensuring that appropriate resources are cross-trained and allocated to perform manual backup monitoring processes.

Current Implementation Status for Rec. 2, part d.: Partially implemented.

Agency's Update:

OIT is re-evaluating all the existing infrastructure tools and techniques and working towards an enterprise wide solution as listed in rec 1.b. A As part of this project, OIT will evaluate cross-training requirements of personnel and make allocations, as required, based on the needs of the new enterprise-wide solution.

Recommendation No. 3:

Ensure that backup and recovery offsite storage requirements are met by:

A. Establishing processes to communicate OIT and agency backup and recovery policies to personnel responsible for managing offsite backup storage procedures and hold personnel accountable for implementing the procedures.

Current Implementation Status for Rec. 3, part a.: Implemented.

Agency's Update:

OIT documented, published, and communicated The Colorado Information Security Policies, which include policies such as backup and recovery, access management, and data classification. In addition OIT established an agency specific operational checklist, as well as a Backup and Recovery policy in July 2015 to establish guidelines and a consistent reference point for ensuring backup process is followed. OIT also added performance measurements to annual staff plans requiring all OIT policies be reviewed and understood. OIT has established multiple avenues to communicate policies to relevant staff such as a quarterly newsletter, trainings, operational managers meetings, etc.

B. Ensuring that personnel responsible for managing backup and recovery processes have the facilities to comply with offsite storage policy requirements.

Current Implementation Status for Rec. 3, part b.: Partially Implemented.

Agency's Update:

OIT is re-evaluating all the existing infrastructure tools and techniques and working towards an enterprise wide solution as listed in rec 1.b. As part of this project, OIT will evaluate the need for off-site storage facilities requirements and ensure that personnel responsible for managing backup and recovery processes have the adequate facilities or resources to comply with backup and recovery policies.

C. Developing and following a formal process to coordinate backup and recovery process changes with agency system owners.

Current Implementation Status for Rec. 3, part c.: Implemented.

Agency's Update:

OIT has implemented a formal change management process to coordinate backup and recovery process changes with agency system owners.

Recommendation No. 4:

Ensure that encryption is applied to backup and recovery media and systems appropriately by:

A. Establishing a process to communicate relevant OIT policies to personnel responsible for categorizing data according to policy requirements.

Current Implementation Status for Rec. 4, part a.: Implemented.

Agency's Update:

OIT documented, published, and communicated The Colorado Information Security Policies, which include policies such as backup and recovery, access management, and data classification. In addition OIT documented, published, and communicated procedures pertaining to Infrastructure Services Backup and Data protection. OIT established an agency specific operational checklist to hold IT staff accountable for implementing backup and recovery policies and procedures. OIT has established multiple avenues to communicate policies to relevant staff such as a quarterly newsletter, trainings, operational managers meetings, etc.

B. Developing and implementing a process to categorize all backed up data based on the OIT policies and establishing a mechanism to hold IT staff accountable for implementing data backup encryption processes, as appropriate.

Current Implementation Status for Rec. 4, part b.: Partially Implemented.

Agency's Update:

OIT is re-evaluating all the existing infrastructure tools and techniques and working towards an enterprise wide solution as listed in rec 1.b. While OIT already has a process to categorize all backed up data based on the data classification, deploying an encryption solution will be developed as part of the enterprise Backup Colorado project to meet backup encryption requirements.

Recommendation No. 5:

Ensure that system recovery policy requirements are met by:

A. Establishing processes to communicate OIT system recovery policies to personnel responsible for managing system recovery processes and holding personnel accountable for implementing the policies.

Current Implementation Status for Rec. 5, part a.: Implemented.

Agency's Update:

OIT documented, published, and communicated The Colorado Information Security Policies, which include policies such as backup and recovery, access management, and data classification. In addition OIT established an agency specific operational checklist, as well as a Backup and Recovery policy and procedures in July 2015 to establish guidelines and a consistent reference point for ensuring backup process is followed. OIT also added performance measurements to annual staff plans requiring all OIT policies be reviewed and understood. OIT has established multiple avenues to communicate policies to relevant staff such as a quarterly newsletter, trainings, operational managers meetings, etc.

B. Evaluating hardware needs and resources to adequately perform system recovery testing and providing the necessary hardware, based on availability of resources.

Current Implementation Status for Rec. 5, part b.: Partially Implemented.

Agency's Update:

OIT has evaluated hardware needs and resources to secure funding to support system recovery testing as part of the Backup Colorado project. The funding will help to fully deploy an enterprise wide backup and recovery solution which, at a minimum, requires infrastructure build out (power and cabling at data centers, racks, etc.), Tape Library Backup System, upgrade and expansion of network connectivity, procurement of disk hardware and software, procurement and deployment of data protection software, implementation of Load Balancer functionality, etc. Once the basic infrastructure is available, OIT will work run test data through a failover and recovery process. Upon completion of successful testing of data recovery, critical and essential systems can be targeted for integration into the backup and recovery solution. OIT will strive to implement this part of the audit finding by its original implementation date of December 2017.

Recommendation No. 6:

Ensure that OIT backup and recovery access management processes are effective by:

A. Updating policies to include access management requirements and standards to address the risks associated with lost or stolen access cards or tokens and to ensure that access to backup and recovery facilities are restricted appropriately.

Current Implementation Status for Rec. 6, part a.: Implemented.

Agency's Update:

OIT documented, published, and communicated The Colorado Information Security Policies (CISPs), which include policies such as backup and recovery, access management, and data classification. The CISPs and associated procedures address lost or stolen access cards or tokens. There are certain facilities where the access control management lies with agency or third party and they own the execution of access controls. OIT cannot enforce access management controls for the facilities that are not under OIT's authority. OIT has implemented this recommendation based on its role and responsibility.

B. Establishing a process to communicate access management policies to personnel responsible for managing these procedures and holding personnel accountable for implementing the policies.

Current Implementation Status for Rec. 6, part b.: Implemented.

Agency's Update:

OIT documented, published, and communicated The Colorado Information Security Policies, which include policies such as backup and recovery, access management, and data classification. In addition OIT established an agency specific operational checklist, as well as a Backup and Recovery policy in July 2015 to establish guidelines and a consistent reference point for ensuring backup process is followed. OIT also added performance measurements to annual staff plans requiring all OIT policies be reviewed and understood. OIT has established multiple avenues to communicate policies to relevant staff such as a quarterly newsletter, trainings, operational managers meetings, etc.

Recommendation No. 7:

Improve governance over backup and recovery processes by:

A. Creating a process for reviewing, updating, and communicating OIT backup and recovery policies to personnel responsible for managing IT backup and recovery processes and

establishing a mechanism to hold IT staff accountable for implementing backup and recovery policies and procedures.

Current Implementation Status for Rec. 7, part a.: Implemented.

Agency's Update:

OIT documented, published, and communicated The Colorado Information Security Policies, which include policies such as backup and recovery, access management, and data classification. In addition OIT established an agency specific operational checklist, as well as a Backup and Recovery policy and procedures in July 2015 to establish guidelines and a consistent reference point for ensuring backup process is followed. OIT also added performance measurements to annual staff plans requiring all OIT policies be reviewed and understood. OIT has established multiple avenues to communicate policies to relevant staff such as a quarterly newsletter, trainings, operational managers meetings, etc. Additionally, as part of ongoing compliance with state statute the OIT will review and update all Information Security Policies annually.

B. Finalize the ECSP that was due July 15, 2014, including backup and recovery roles and responsibilities within OIT.

Current Implementation Status for Rec. 7, part b.: Implemented.

Agency's Update:

OIT has documented and published the ECSP including backup and recovery roles and responsibilities within OIT.