Department of Education

Internal Audit

Data Access Controls Review

Issue Date: November 2014

Report Number: FY2015-01

Department of Education
Data Access Controls Review

Executive Summary

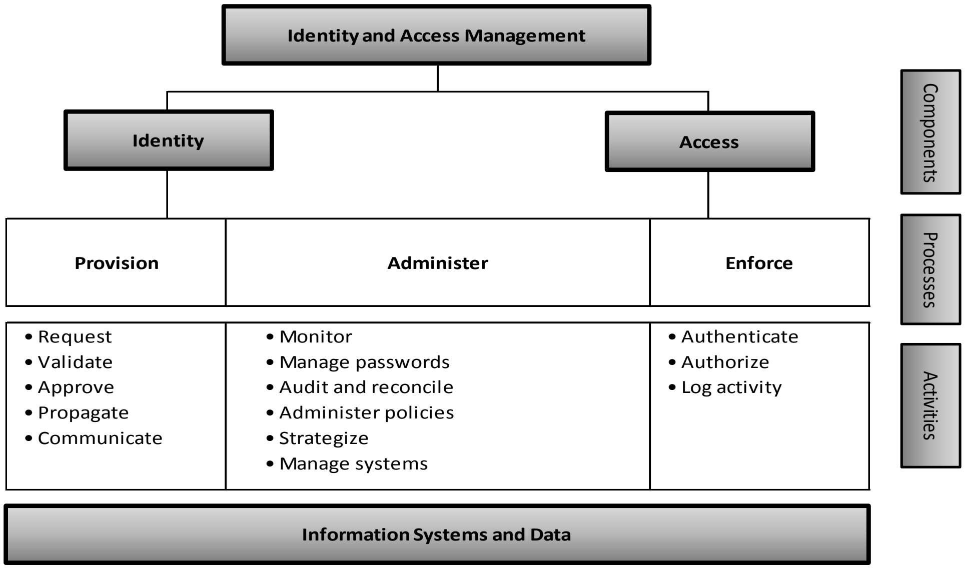
AUDIT OF:	**DATE:**	**AUDIT RATING:**
Data Access Controls Review	Fieldwork performed July 2014 – November 2014	Acceptable [ ] Marginal [X] Unacceptable [ ]

INTRODUCTION:
In connection with the Department of Education's (DOE) Updated Risk Assessment and Internal Audit Plan approved on August 5, 2014, Internal Audit (IA) performed a *"Data Access Controls Review."* The purpose of this project was to review access controls of select systems and/or records to ensure (1) only authorized individuals are permitted to request or approve access; (2) access provided aligns with job responsibilities; and (3) individuals are disabled or removed from the system when they no longer require access.

BACKGROUND:
As stated in the Global Technology Audit Guide, identity and access management (IAM) is a process of managing who has access to what information over time. IAM processes are used to initiate, capture, record, and manage the user identities and related access permissions to the DOE's proprietary information. Although this is usually viewed as an information technology (IT) function, IAM affects every office throughout the DOE.

There are several stages of the IAM process: provisioning, administration, and enforcement. Provisioning refers to an identity's creation, change, termination, validation, approval, propagation, and communication. Administration or identity management includes the establishment of an IAM strategy, administration of IAM policy statement changes, establishment of identity and password parameters, management of manual or automated IAM systems and processes, and periodic monitoring, auditing, reconciliation, and reporting of IAM systems. Enforcement includes the authentication, authorization, and logging of identities as they are used within the organization's IT systems.

Below is a depiction of IAM and its related components:



The DOE collects data with two goals in mind: 1) To provide an evolving snapshot of the academic and social health of the public education system, and 2) To create real-time feedback for teachers and administrators to help them regularly assess student performance, and create learning interventions when and where students need them. Some of the main data systems in the DOE include:

Student Information Systems

- **Accountability System** - Compiles scores from the state assessment (and alternate and Hawaiian language versions), student scores from quarterly assessments, and School Quality Survey results.
- **ARCHdb Database** - Provide schools with secure access to their student rosters that will be used to calculate Adequate Yearly Progress (AYP). The student-level data reflects the requirements of No Child Left Behind.
- **Blackboard** - Database of formative assessments for teachers.
- **Curriculum Development & Learning Management System** - Data for formative assessments, grades, attendance, and instructional & curricular management.
- **Data for School Improvement (DSI)** - Provides assessment items for the classroom teacher and is part of the formative assessment strategy in the Hawaii DOE's strategic plan to provide data to inform and adjust instruction to address student needs.
- **Electronic Comprehensive Student Support System (eCSSS)** - Includes student information relating to special education, English Language Learners, behavior assessments, progress monitoring, intervention and Response to Intervention (RTI) management, along with support program data, action plans for at-risk students, and early warning system.
- **Electronic Student Information System (eSIS)** - Includes student biographical data, attendance, elementary homeroom class lists, school master schedule, student and teacher schedules, grades/marks/report cards, enrollment, parent information, emergency contacts, diploma types available, projected graduation date, student credit accumulation, Career Technical Education progress, student health information, and homelessness.
- **eSchool** - Standards-based, online classes for students enrolled at any Hawaii public school (including charter schools).
- **Hawaii Growth Model, aka SchoolView** - Data on achievement and growth. This private (staff) view of the Hawaii Growth Model website drills down to protected student-level data.
- **Hawaii Statewide Assessment Portal (HSAP)** - The official site for the Hawaii State Assessments, the Hawaii State Alternate Assessments, and the End-of-Course Exams, with secured sites for teachers, test administrators, test coordinators, principals, complex area superintendents, and other DOE employees.
- **Hawaii Virtual Learning Network** - Online courses for Hawaii's students, WebEx services.
- **Longitudinal Data System (LDS)** - Provides reports and dashboards where teachers and administrators can access data about student academic progress and performance. The LDS enables teachers and administrators to customize existing reports by selecting specified report filters on student demographics, staff, etc., and develop what's known as Response to Intervention (RTI) - custom supports designed to meet the specialized learning of the student. LDS data are compiled along a continuum that begins with early education and continues through K-12.
- **Migrant** - Database with student-level data for students eligible for migrant services.

- **Roster Verification — Battelle for Kids** - Validates teacher-student linkages within a specific time period and attributes Student Growth Percentile (SGP) data to teachers for evaluation purposes.
- **Statewide Student Enrollment System (SSES)** - DOE's student enrollment system

Employee Information Systems

- **Electronic Human Resources (eHR) System** - Human resource system for DOE employees where employees can apply for jobs and modify online resumes.
- **Kronos** - Time and attendance tracking system.
- **PDE3** - Accounts for staff professional development (courses taken and completed) along with teacher evaluation data.
- **Project Inspire** - Online professional development credit program to assist teachers in the integration of technology to a standards-based curriculum.

Financial Systems

- **Budget – HyperAccess Program** - Repository for service verification and budget data.
- **Financial Management System (FMS)** - Automated, integrated, multi-user accounting and financial system which performs financial and school based accounting functions. FMS applications cannot be accessed off the DOE Network.
- **Financial Reporting System (FRS)** - DOE's financial reporting system.
- **Student Activity Fund (SAF) System** - DOE's accounting and financial system for non-appropriated funds.

Other Support Systems

- **DOE Intranet** - Staff-only website for internal communications, resources, key forms, and more.
- **DOE Memos and Notices** - Online searchable/sortable database of the Department's memos and notices to staff.
- **Facilities** - Data about school facilities, space and infrastructure. (The Department also hosts a separate external application, FacTrak, to manage the pipeline of the state's Capital Improvement Projects for schools).
- **Factrak** - Track Repair & Maintenance and Capital Improvement Projects.
- **Lotus Notes Webmail** - Access DOE webmail, calendar, address book online
- **Maximo** - Tracks work order and inventory
- **Official Enrollment Count** - Official enrollment count for all schools used for WSF funding
- **Password Self-Service System** - Allows employees to set their password for applications using the DOE Internet Password.
- **School Bus Transportation** - Real-time data about bus transportation and routes. Manages applications and accounting for student bus passes.
- **SMS Food Services** - Produces data resulting from the Free and Reduced Price Lunch program.
- **Virtual Private Network (VPN)** - extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it is directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network.

For new employees, a Form 5 is generated and automatically places the employee on a Lotus Notes database as well as a Microsoft Active Directory (Directory). To process any requests to grant new employees access to other applications (i.e. Kronos, LDS, etc.), program administrators use this Directory to authenticate that the employee is, in fact, a legitimate DOE employee.

For current DOE employees, access to various systems is generally requested through the business owners (i.e. Office of Fiscal Services (OFS), Office of School Facilities and Support Services (OSFSS), etc.) who then will contact the program administrators in the Office of Information Technology Services (OITS) to set up access.

David Wu is the Assistant Superintendent and Chief Information Officer of OITS. His management staff includes Tom Gerrish, Director of Enterprise Systems Branch (ESB) and Dean Horiuchi, Director of Enterprise Infrastructure Services Branch (EISB). Different branches in OITS are responsible for different systems.

Policies and procedures are posted in various sources including DOE Memos and Notes in Lotus Notes and the DOE Intranet. Through research, IA identified Chapter 487N of the Hawaii Revised Statutes (HRS), regarding security breach of personal information as the main regulatory governance.

SCOPE and OBJECTIVES:

The scope of our review included an examination of the data access controls processes in the DOE. We reviewed the design and operating effectiveness of the existing control procedures in place. The scope of our review specifically focused on the processes related to the following systems that IA deemed as high risk:

- Kronos
- LDS
- eSIS
- Password Self-Service System (Single Sign-On)
- FMS
- VPN

For the purpose of this review, we identified the program administrators in OITS as the process owners in regards to data access controls of the selected systems. However, with the exception of eSIS and VPN, each system is owned by different offices/branches outside of OITS. OFS is the business owner of Kronos and FMS. Data Governance and Analysis Branch is the business owner of LDS. Password Self-Service System (Single Sign-On) is directly linked to eHR, which is owned by the Office of Human Resources (OHR).

The scope of the detailed testing covered fiscal year 2013-2014 and fiscal year 2015 up to fieldwork date. This review excluded detailed testing of data access controls for eHR as it was covered by the *"eHR Post-Implementation Review"* issued by IA in July 2013.

The objectives of our review included the following:

1. To review, evaluate, and test the design and operating effectiveness of the process to revise (i.e. add, change, or remove) employee access privileges.
2. To review, evaluate, and test the design and operating effectiveness of the process to monitor user/employee access levels to ensure:
   a. Employee's access privileges align with the employee job responsibilities;
   b. Adequate segregation of duties exist; and
   c. Employee/user IDs are valid.
3. To review, evaluate, and test the design and operating effectiveness of the process to ensure that only authorized employees are assigned 'administrator' access and such access is only used to perform authorized activities.

OBSERVATIONS:

Based upon our review, we found the DOE's controls related to data access controls are functioning at a "marginal" level. A marginal rating indicates that there may be a potential for loss to the auditable area and ultimately to the DOE. Some improvements are necessary to bring the unit to an acceptable status, and if weaknesses continue without attention, further deterioration of the rating to an unacceptable status may occur.

Please refer to the Risk Ratings section of this report for a complete definition of the ratings used by IA and the Observations and Recommendations section for a detailed description of our findings.

We discussed our preliminary findings and recommendations with management and they were receptive to our findings and agreed to consider our recommendations for implementation.

Each observation presented in this report is followed by specific recommendations that will help to ensure that control gaps are addressed and, if enforced and monitored, will mitigate the control weaknesses. In summary, our observations are as follows:

1. Lack of proper monitoring over access controls
2. Lack of data access control policies and procedures when employees separate from the DOE
3. Inefficiencies result from requests to terminate user access through each respective system

Note: For the purpose of this review, separated employees include employees that retired, resigned, or was terminated from the DOE.

PLANNED FOLLOW UP BY MANAGEMENT AND INTERNAL AUDIT:

IA will follow up with management on their progress of completion for their action plans and report accordingly through the audit committee quarterly updates.

OVERALL RATING SCALE	
Acceptable	No significant deficiencies exist, while improvement continues to be appropriate; controls are considered adequate and findings are not significant to the overall unit/department.
Marginal	Potential for loss to the auditable unit/department and ultimately to the DOE. Indicates a number of observations, more serious in nature related to the control environment. Some improvement is needed to bring the unit to an acceptable status, but if weaknesses continue without attention, it could lead to further deterioration of the rating to an unacceptable status.
Unacceptable	Significant deficiencies exist which could lead to material financial loss to the auditable unit/department and potentially to the DOE. Corrective action should be a high priority of management and may require significant amounts of time and resources to implement.

OBSERVATION RATING SCALE	
High (1)	1 - The impact of the finding is *material*[1] and the likelihood of loss is probable in one of the following ways: • A material misstatement of the DOE's financial statements could occur; • The DOE's business objectives, processes, financial results or image could be materially impaired; • The DOE may fail to comply with applicable laws, regulations or contractual agreements, which could result in fines, sanctions and/or liabilities that are material to the DOE's financial performance, operations or image. *Immediate action is recommended to mitigate the DOE's exposure*
Moderate (2)	2 - The impact of the finding is *significant*[1] and the likelihood of loss is possible in one of the following ways: ➢ A significant misstatement of the DOE's financial statements could occur; ➢ The DOE's business objectives, processes, financial performance or image could be notably impaired; ➢ The DOE may fail to comply with applicable laws, regulations or contractual agreements, which could result in fines, sanctions and/or liabilities that are significant to the DOE's financial performance, operations or image. *Corrective action by management should be prioritized and completed in a timely manner to mitigate any risk exposure.*
Low (3)	3 - The impact of the finding is moderate and the probability of an event resulting in loss is possible. *Action is recommended to limit further deterioration of controls.*

[1] The application of these terms are consistent with the guidelines provided by the Institute of Internal Auditors

Observations

The detailed observations noted herein were based on work performed by IA through the last date of fieldwork and are generally focused on internal controls and enhancing the effectiveness of processes for future organizational benefit.

Obs. No.	Description	Page #
1	Lack of proper monitoring over access controls	8-11
2	Lack of data access control policies and procedures when employees separate from the DOE	12-13
3	Inefficiencies result from requests to terminate user access through each respective system	14

Observation Number: 1

Observation: Lack of proper monitoring over access controls **Rating: High**

Each system selected for testing has different access controls procedures. We interviewed all six (6) system administrators for each respective system and performed detailed testing. We noted that some systems require manual processes to add and remove users from the respective system while other systems are automated based on an employee's employment status with the DOE. Access for vendors and non-DOE employees are manually added and removed from each respective system. Each system has the ability to maintain security by user and role (user assigned to a role). The following table summarizes the exceptions noted during our review indicating inefficiencies and errors resulting from lack of proper monitoring over access controls.

System(s)	Summary of Observations Noted
Lack of Reviews	
➢ Kronos	➢ Lack of reviews performed including: periodic reviews performed where management traces access permissions to access request forms, reviews performed to monitor user/employee access levels for the system, and no verification and reconciliation processes performed to identify misaligned access rights.
Lack of Policies and Procedures	
➢ Kronos	➢ There is a lack of documented policies, procedures, flowcharts, or other documentation in regards to access controls.
Users with Improper Access Rights	
➢ Kronos	➢ Five (5) out of 858 users with active access where the user is no longer with the DOE but still had active access to Kronos. Management has terminated the accounts since the finding.
➢ LDS	➢ Six (6) out of 12,803 users with active access where the user is no longer with the DOE but still had active access to LDS.
➢ eSIS	➢ 236 out of 17,649 users with active access where the user is no longer with the DOE but still had active access to eSIS.
➢ FMS	➢ For six (6) of the 286 active users selected for detailed testing, the user is no longer with the DOE but still had active access to FMS.
➢ VPN	➢ For three (3) of the 60 active users selected for detailed testing, the user is no longer with the DOE but still had active access to VPN.

System(s)	Summary of Observations Noted
Users with Improper Access Rights (continued)	
➢ eCSSS, eSIS, FMS, Lotus Notes	➢ For seven (7) of the 20 employees selected for testing that were separated during the testing period, employees still had access to the respective systems. Four (4) of the seven (7) requested for revocation of employee's access after IA had informed the schools of the finding.
➢ Kronos	➢ One (1) out of 858 users with active access where the user transferred to a different office but still had access to the previous office. Management has terminated the accounts since the finding.
➢ Kronos	➢ One (1) out of 42 super-users had two (2) active accounts in use. One (1) account is no longer in use and should have been terminated. Management has terminated the accounts since the finding.
➢ Unknown to IA	➢ For three (3) of the 20 employees selected for testing that were separated during the testing period, user access could not be verified due to lack of response from schools.
User Access Change Requests	
➢ LDS	➢ For three (3) of the 40 active users selected for detailed testing, user access change requests could not be verified due to no responses from schools.
➢ VPN	➢ For two (2) of the 40 active users selected for detailed testing, no approval signatures were on the "DOE VPN Access Request Form."
Unique User IDs Not Used	
➢ FMS	➢ 3,595 out of 3,881 active users in FMS (93%) did not have unique user IDs for IA to perform detailed testing.

These observations indicate a weakness with the data access controls procedures. Based on discussions with system administrators, IA noted that the main factor attributed to the findings is that there is no automated process to remove users from the respective system. In the past, some business owners of the respective systems did not want an automated process to remove users based on OHR databases of employment status. That resulted in the manual process of removing users when notified by the school/office. See the effects of a manual process in Observation Number 2 and 3 as it relates to the lack of an automated process.

Impact

Lack of proper monitoring over access controls may lead to:

- Improper permission rights given to users.
- Improper access which may allow users to manipulate data in system.
- Inaccuracy of information which may lead to financial loss to the DOE.
- Inconsistencies between practices and policies and procedures.
- Improper access to systems which may lead to fraudulent acts and financial loss to the DOE.
- Improper access to confidential records by unauthorized users which may lead to possible violation of confidentiality laws.

Recommendation

Recommendations to address the lack of proper monitoring over access controls include:

- Management should work with OHR to develop an automated process to remove separated employees' access to respective systems.
- If business owners do not want an automated process, then business owners should be responsible for performing reviews on data access controls for their respective systems.
- Reminders should be sent out to the field to inform system administrators when separated employees no longer need access to respective systems.
- Reminders should be sent out to DOE sponsors to inform system administrators when consultants no longer need the access to the system.
- Business owners should notify system administrators to remove active users from the system if they receive no responses from the schools/offices regarding user access change requests.
- System administrators should periodically, on a test basis, check that active user accounts are valid.
- Periodic reviews should be performed by system administrators to trace access permissions to access request forms, monitor user/employee access levels, and identify misaligned access rights for Kronos.
- Management should develop policies and procedures for Kronos access controls and revisit these policies and procedures for any changes or updates.
- Management should enforce the proper completion of forms.
- Unique user IDs in FMS should be created in the system to accurately identify the users of the system.

Management Plan

ESB Management Plan:

The following actions are to be taken to remediate the findings noted above.

- OITS and key business leads will meet to confirm who has the responsibility to ensure personnel are removed from each business system in a timely manner. ESB will coordinate.
- The eHR, TSEAS, and Casual payroll are the base systems for all employees. ESB will develop an automated process that will compare all users in these systems with all other systems. This script will run automatically on a regular scheduled basis and develop a report that will show users who should be removed from all systems noted above.
- OITS and OHR will meet to discuss developing a workflow process to address those users who are transferring within the DOE but have different responsibilities and terminations that need immediate attention.

- Each business owner should develop a review process for each system they own that will act as an internal audit on a regular basis. OITS will provide technical assistance when requirements have been developed.
- All offices will be sent a list of FMS IDs and asked to identify who is using each ID with a deadline for response. After the deadline passes, DOE will either send non-respondents another list (if there are a large number) or contact each office to obtain the information. DOE will seek assistance from the complex areas for those offices that repeatedly fail to respond.

Contract Person: Tom Gerrish, Director
Enterprise Systems Branch
Office of Information Technology Services

Anticipated Completion Date: December 31, 2015

EISB Management Plan:

The joint review of the Data Access Controls with EISB and the IA Office has been very productive and informative. EISB designed, installed, and manages the DOE virtual private network (VPN) access. During the review EISB acknowledges accuracy of the IA Office finding. EISB proposes the following management plans to address these findings.

- The three (3) users that should have been removed from the active access list were vendors/ consultants to OITS staff (sponsors) working on OITS systems. These users are only given access for a limited time. Based on this finding, EISB will review and emphasize with the OITS sponsors the importance of managing their active list of vendors/consultants.
- The two (2) VPN users without approved signatures were part of the initial group of VPN users added before the implementation of the "DOE VPN Access Request Form." EISB has reviewed all VPN accounts for proper authorization and approvals. Going forward EISB plans to convert the paper forms into an electronic process to better manage these accounts.

Contract Person: Dean Horiuchi, Director
Enterprise Infrastructure Services Branch
Office of Information Technology Services

Anticipated Completion Date: August 31, 2015

Responsible Manager
Tom Gerrish, Director, Enterprise Systems Branch, OITS Dean Horiuchi, Director, Enterprise Infrastructure Services Branch, OITS

Observation Number: 2

Observation: Lack of data access control policies and procedures when employees separate from the DOE **Rating: Medium**

Based on discussions with system administrators/school personnel and test work performed, IA noted that for most of the systems selected for testing, user access is removed upon notification. System administrators have to rely on schools, district/state offices, and other departments to communicate the separation of employees/vendors before they can remove users from the respective systems. If information is not communicated, some of the system administrators have no way of knowing when to remove user access to the respective systems.

Based on testing performed for access removal for separated employees, IA noted that five (5) out of 17 schools/offices that responded to our questionnaire did not terminate access for employees that had left their respective school/office as they had an understanding that OHR would terminate access to the IT systems. However, OHR did not notify the respective system administrator of the employment statuses. In addition, based on discussions with various schools/offices, there are no consistent policies and procedures in regards to data access controls when employees separate from the DOE.

Impact

Lack of data access control policies and procedures when employees separate from the DOE may lead to inconsistencies between practices and policies and procedures. Such inefficiencies may result in wasted resources and financial loss to the DOE.

Recommendation

Recommendations to address the lack of integrated systems include:

- Management should work with OHR to develop an automated process to remove separated employees' access to respective systems.
- If business owners do not want an automated process, then business owners should be responsible for performing reviews on data access controls for their respective systems.
- Management should provide guidance to the field to explain the process to remove separated employees from each respective system.
- Reminders should be sent out to the field stating that schools/offices are responsible for contacting each respective system administrator to remove access for separated and transferred employees.
- Management should create a standardized checklist for the field to track each respective system an employee is given access to.

Management Plan

Please see Management's Plan in Observation #1.

Contract Person: Tom Gerrish, Director
Enterprise Systems Branch,
Office of Information Technology Services

Anticipated Completion Date: December 31, 2015

Contract Person: Dean Horiuchi, Director Enterprise Infrastructure Services Branch Office of Information Technology Services Anticipated Completion Date: August 31, 2015
Responsible Manager
Tom Gerrish, Director, Enterprise Systems Branch, OITS Dean Horiuchi, Director, Enterprise Infrastructure Services Branch, OITS

Observation Number: 3

Observation: Inefficiencies result from requests to terminate user access through each respective system **Rating: Low**

As noted in Observation Number 2, most system administrators have to rely on schools, district/state offices, and other departments to communicate the termination of employees/vendors before they can remove users from the respective systems. If information is not communicated, some of the system administrators have no way of knowing when to remove user access to the respective systems.

Based on the testing performed, IA noted inefficiencies related to the termination of user access to systems. Schools and offices have to contact different system owners to remove a separated employee's access to respective systems. The DOE does not have a centralized department that handles the termination of user access when an employee/vendor is no longer with the DOE.

Impact

Inefficiencies resulting from requests to terminate user access through each respective system may lead to inconsistencies between practices and policies and procedures. Such inefficiencies may result in wasted resources and financial loss to the DOE.

Recommendation

Management should work with OHR and business owners to develop an automatic process to remove separated employees' access to respective systems without having schools/offices to contact each system the separated employee had access to.

Management Plan

Please see Management's Plan in Observation #1.

Contract Person: Tom Gerrish, Director
Enterprise Systems Branch,
Office of Information Technology Services

Anticipated Completion Date: December 31, 2015

Contract Person: Dean Horiuchi, Director
Enterprise Infrastructure Services Branch
Office of Information Technology Services

Anticipated Completion Date: August 31, 2015

Responsible Manager

Tom Gerrish, Director, Enterprise Systems Branch, OITS
Dean Horiuchi, Director, Enterprise Infrastructure Services Branch, OITS

Acknowledgements

We wish to express our appreciation for the cooperation and assistance afforded to the review team by management and staff during the course of this review.