Review of User Access to Kronos Enterprise Time and Attendance System

March 10, 2016 **Report No. 16-3**

Office of the County Auditor

Evan A. Lukic, CPA

County Auditor

Table of Contents

Executive Summary

This report presents the results of our review of user access to the Kronos Time and Attendance System. The objective of this review was to evaluate whether the access rights granted to employees were commensurate with job responsibilities and whether appropriate segregation of duties were enforced. Our review covered user access rights during the period October 1, 2014 to July 20, 2015.

We conducted interviews with appropriate County personnel and reviewed and analyzed Kronos security reports. Our review found instances of non-compliance with County policies and industry best practices:

- Kronos Administrators had access to all system functions without appropriate monitoring.
- Employee access to the Kronos application was not appropriately restricted based on employee job responsibilities.
- Terminated employees accounts were not deactivated from Kronos immediately upon termination as required by County policy.
- Changes to system integrated pay and work rules to process employee time transactions against labor union contract or other administrative business rules, and historical edits made to employee time cards after the end of the pay period were not reviewed for unauthorized or inappropriate activity.
- Kronos timecards were not consistently approved before payroll processing as required by County Procedures.

We recommend the Board of County Commissioners direct the County Administrator to:

1. Require that the permissions granted to the Kronos Administrators be reviewed with the vendor to reduce segregation of duties conflicts, and to ensure that appropriate monitoring controls are implemented since Kronos Administrators will continue to have access to sensitive and high risk functions.
2. Require a periodic review of all function access profiles to ensure that each agency periodically reviews the users to which these profiles are assigned to validate that user access remains commensurate with job responsibilities.
3. Review employee termination procedures to ensure that all terminated employee access is revoked immediately upon termination.

4. Design and implement a periodic review of system integrated pay and work rules changes, as well as historical edits to timecards, to ensure that each change is authorized and appropriate.

5. Require that the Broward County EasyPay timecard approval process be followed to enforce timecard workflow approval, and to require each agency to follow-up on timecards that were not approved prior to processing payroll to ensure that they were accurate.

Purpose and Scope

The purpose of this review was to evaluate whether the access rights granted to employees were commensurate with job responsibilities and whether appropriate segregation of duties were enforced. Our review covered user access rights and supervision and review controls during the period October 1, 2014 to July 31, 2015.

Methodology

To accomplish our objective we reviewed the:

- ❖ County Administrative Policy and Procedures, Volume 7: Enterprise Technology Services (ETS), Chapter 3: IT Administration

- ❖ United States Government Accountability Office, Federal Information System Controls Audit Manual

- ❖ National Institute of Standards and Technology Special Publication 800-53, Security and Privacy Controls for Federal Information Systems

In addition, we performed the following procedures to validate user authorization controls, segregation of duties controls, and supervision and review controls for the Kronos Time and Attendance System.

- ❖ User Authorization Procedures

    - ✓ Selected a sample of Function Access Profiles (FAP). For each FAP selected, we attempted to determine whether the users assigned the FAP require access for the performance of user job responsibilities.

    - ✓ Reviewed timecard activity logs to determine whether employee time is approved by each employee and the employee's supervisor prior to signoff by the department's payroll liaison.

- ✓ Selected a sample of new hires to determine whether access to the Kronos application was appropriately authorized and that access was granted as authorized.

- ✓ Selected a sample of terminated employees to determine whether system access was promptly terminated.

❖ Segregation of Duties Procedures

- ✓ Inspected user administration procedures and forms to determine whether access is granted based on employee job responsibilities.

- ✓ Interviewed selected management and information security personnel regarding segregation of duties.

- ✓ Reviewed the Kronos Service Organization Control Report for any issues related to segregation of duties.

- ✓ Reviewed Broward County's Kronos design and implementation documentation.

- ✓ Reviewed system reports showing permissions assigned to each function action profile to determine whether access is appropriate for job responsibilities and appropriate segregation of duties is enforced.

❖ Supervision and Review Procedures

- ✓ Interviewed management personnel and inspected supporting documentation to determine whether a periodic review of user access is performed to validate that user access is appropriate for user job responsibilities and appropriate segregation of duties are enforced.

- ✓ Interviewed supervisors and reviewed user activity logs for incompatible actions.

Background

Kronos Enterprise Time and Attendance System

On June 12, 2012 (Item No. 29), the Broward County Board of County Commissioners approved an agreement between Broward County and Kronos Incorporated for an Enterprise Time and Attendance System for an initial estimated cost of $2.2 million. The agreement provided for the purchase of an Enterprise Time and Attendance System for the Broward County workforce, for both salaried and hourly employees. The initial

purchase included hardware and software, professional and educational services, reimbursable expenses, system hosting, and maintenance. The Kronos implementation project was officially launched on August 22, 2012 and as of September 30, 2015, the County has incurred $2.4 million in expenses related to this project with the project 75% to 80% complete.[1]

Kronos replaced the previous manual paper process for managing time and attendance for hourly and salaried employees at all Broward County agencies.

Kronos is used for management and tracking of staff actual hours against a planned schedule including leave hours (annual, job basis, sick etc.). The system integrates complex pay and work rules to process employee time transactions against labor union contract or other administrative business rules. The County is responsible for managing access to the system and managing the pay and work rules. Kronos is responsible for supporting the system (change management, and operations).

The system has a combination of time-capture devices which includes, electronic time clocks and keyboard entry into a web-based system for employee self-check-in.

Employee Setup

When an employee is hired, the Agency completes a Personnel Action Form (BC102-102) which is approved by the Agency Director and Human Resources and then sent to Payroll for set up in the Cyborg payroll system. Once an employee is set up in Cyborg, the employee is automatically enrolled in Kronos and is granted default access which provides basic time entry and approval rights on the Kronos time clocks.

Access to the Kronos Time and Attendance System is granted via Function Access Profiles ("FAP"). Each employee is given access to one FAP which defines their capabilities on Kronos. FAPs are designed to limit access to Kronos based on an employee's job responsibilities with respect to time and attendance entry, approval, and monitoring.

Time Reporting and Approval

Hourly employees

Instead of filling out manual time-sheets, employees now electronically clock in and out and submit time-off requests via the electronic time clocks that are located across Broward County or on their computers using the web-based system. Employee hours are recorded on an electronic timecard maintained by the Kronos system.

[1] Estimated project completion status provided by Kronos Project Manager

Salaried Employees

Salaried employees submit time-off requests (annual, job basis, sick, etc.) electronically via the Kronos website instead of manually preparing a leave slip and routing it to the appropriate Supervisor for approval. Time-off requests are reviewed and approved electronically by assigned Supervisors, which automatically updates employee timecards maintained by Kronos.

Payroll Processing

At the end of the two-week payroll period, employees review and approve their time-cards for accuracy. The time-cards are then reviewed and approved electronically by Supervisors before sign-off by Payroll Liaisons. Approved hours are transmitted to the Cyborg system ("Cyborg") for payroll processing.

Cyborg is the system of record for payroll. Cyborg updates Kronos daily with employee information including new hires and terminations, while Kronos updates Cyborg bi-weekly with employee time information through an automated data transfer process.

On the Monday prior to each scheduled payroll, Supervisors are required to complete their review and approval of timecards by 10am. Payroll Liaisons are then required to ensure that employees and supervisors have approved timecards before they sign-off that timecards are ready for payroll processing.

If a change needs to be made to an employee's timecard after it is signed off by the Payroll Liaison and submitted to payroll, a historical edit will be necessary. Historical edits are processed by Payroll Central Managers, in the Payroll Section of the Accounting Division.

Employee Termination

When an employee is terminated a BC102-102 form is completed by Agencies and forwarded to the Human Resources Division. This form is used to update employee status information within Cyborg. Terminated employee accounts in Kronos are disabled daily through the automated data transfer process with Cyborg.

Findings

Finding #1: Kronos Administrators	*Kronos Administrators can perform all system functions without appropriate monitoring.*

An important preventive control is “segregation of duties,” which requires more than one individual to be responsible for completing a process or to have control over more than one phase of a transaction. National Institute of Standards and Technology (NIST) requires that no user should have the ability to perform (initiate, approve, signoff) all aspects of a transaction[2].

We reviewed the Kronos Administrator Function Access Profiles (FAP) and determined users assigned this profile have full access to the Kronos Enterprise Time and Attendance System. This allows them the ability to bypass segregation of duties controls over the time and attendance recording process affecting the County’s payroll. For example these Administrators have the ability to edit their own hours worked and leave balances without adequate monitoring.

Three County employees were assigned the Kronos Administrator FAP. The FAP was designed by Kronos to facilitate system, security, and user maintenance and support; however, full access to the Kronos application increases the risk of unauthorized or inaccurate time and leave reporting affecting the County’s payroll. Procedures have not yet been implemented to monitor the activity of users to which this FAP is assigned.

Recommendation #1

We recommend the Board of County Commissioners direct the County Administrator to require that the permissions granted to the "Kronos Administrator" FAP be reviewed with the vendor to restrict activity to only that required for the performance of job responsibilities and reduce segregation of duties conflicts. Since this FAP will continue to have access to sensitive and high risk functions, monitoring controls should be implemented to monitor the activity of these accounts.

Finding #2: Employee Access	*Employee access to the Kronos application was not appropriately restricted based on employee job responsibilities.*

The County’s IT Administration Policy[3] requires that all access rights must be consistent with the user’s current roles and responsibilities.

[2] NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, Control AC-5 Separation of Duties
[3] County Administrative Policy and Procedures, Volume 7: Enterprise Technology Services (ETS), Chapter 3: IT Administration, Section 4.3.

Each employee is given access to one Function Access Profile ("FAP") which defines their capabilities on the Kronos application. The FAP should limit user access to only the access required for the performance of job responsibilities.

We selected a sample of nine FAPs and reviewed the detailed permissions granted against the job function for which they were designed and noted that five (56%) FAPs reviewed had more access than that required for the job responsibilities for which they were designed.

We also reviewed all users with access to the Payroll Liaison and Supervisor FAPs which have access to sensitive functions within the Kronos application and noted the following;

- Three (8%) of 37 users tested with the Payroll Liaison FAP within the Kronos application did not require this access level for the performance of their job responsibilities.

- Three (6%) of 50 users tested with a Supervisor FAP did not require this access level for the performance of their job responsibilities.

Inappropriate access to the Kronos application increases the risk of unauthorized or inaccurate time and leave reporting affecting the County's payroll. Procedures have not yet been implemented to periodically review FAPs and the users to which these FAPs are assigned in order to ensure that user access remains commensurate with job responsibilities.

Recommendation #2

We recommend the Board of County Commissioners direct the County Administrator to require a periodic review of FAPs and assigned employees to ensure that user access remains commensurate with job responsibilities.

Finding #3: Terminated Employee Access	*Terminated employees accounts were not deactivated from Kronos immediately upon termination as required by County policy.*

The County's IT Administration Policy[4] requires that access rights must be removed upon termination of employment. Once a Human Resources Division, Personnel Action Form (BC102-102) is processed, the employee status is updated in Cyborg. Kronos is updated nightly through a data exchange with Cyborg to disable terminated employee accounts. We selected a sample of 37 terminated employees and reviewed Kronos user security reports to determine whether terminated employee accounts were disabled or removed immediately upon termination. We noted the following:

[4] County Administrative Policy and Procedures, Volume 7: Enterprise Technology Services (ETS), Chapter 3: IT Administration, Section 4.2.

- 33 (89%) of 37 terminated employees were not revoked immediately upon termination. We noted that, on average, terminated employee access was revoked 17 days from the date of termination within a range of 1 to 49 days.

- Two (5%) of 37 terminated employee accounts tested were not disabled as the Cyborg to Kronos data transfer process was not configured correctly to disable employee accounts with a leave of absence status at the time of termination.

Enabled terminated employee accounts on County systems increases the risk of compromise and inappropriate payroll payments to terminated employees. The current termination process is not consistently followed in a timely manner by County agencies.

Recommendation #3

We recommend the Board of County Commissioners direct the County Administrator to review employee separation procedures to ensure that all terminated employee access is revoked immediately upon termination as required by County policy.

Finding #4: Sensitive Transaction Review	*Changes to system integrated pay and work rules, and historical edits were not reviewed for unauthorized or inappropriate activity.*

User activity logs should be periodically reviewed by appropriate management personnel for incompatible actions and abnormalities as recommended by the United States Government Accountability Office[5].

Changes to system integrated pay and work rules to process employee time transactions against labor union contract or other administrative business rules and historical edits made to employee time cards after the end of the pay period can be performed by Kronos Administrators and Payroll Central Managers. The Kronos Time and Attendance system contains logs that record this activity; however, they were not periodically reviewed for unauthorized or inappropriate activity.

There is currently no procedure in place to perform periodic reviews of activity logs which increases the risk of unauthorized or inappropriate changes to pay and work rules, and historical timecard information affecting the County's payroll.

[5] United States Government Accountability Office, Federal Information System Controls Audit Manual (FISCAM), February 2009, Control Technique SD-2.2.5.

Recommendation #4

We recommend the Board of County Commissioners direct the County Administrator to design and implement a periodic review of user activity logs, based on risk, to ensure that high risk activity that occurs outside of the regular timecard approval process (pay rule changes, historical edits) is authorized and appropriate.

Finding #5: Timecard Approval Workflow	*Kronos timecards were not consistently approved before payroll processing as required by County Procedures.*

Broward County easyPay Time and Attendance procedures require that all employees (hourly and salary) approve their timecard before their Supervisor approves it. It also requires that Supervisors approve timecards so that Payroll Liaisons know that timecards are ready for processing.

We reviewed the timecard approval process and a sample of 23 timecards for one pay period to determine if the approval process was followed. We noted that the Kronos application does not automatically enforce the timecard workflow approval process and the process is not consistently enforced procedurally. As a result;

- 52% of the timecards tested had no employee approval
- 17% of the timecards tested had no supervisor approval

Payroll Central must run payroll according to the County's schedule and, as a consequence, processes payroll with or without the employee or supervisor approvals. There is no process or procedure to follow up on timecards that were not approved prior to processing payroll.

Inconsistent review and approval of employee time increases the risk of inaccurate payroll, and leave balances.

Recommendation #5

We recommend the Board of County Commissioners direct the County Administrator to require that Broward County easyPay timecard approval process be followed to procedurally enforce timecard workflow approval. In addition, we recommend that each agency be required to follow-up on timecards that were not approved prior to processing payroll to ensure that they were accurate.

County Auditor

Board Action
Agenda Item 33
April 26, 2016

COUNTY AUDITOR

33.

A. MOTION TO FILE Review of User Access to Kronos Enterprise Time and Attendance System (Report No. 16-3).

(This item was pulled by a member of the public.)

ACTION: (T-11:06 AM) Approved. (Refer to minutes for full discussion.)

VOTE: 9-0.

B. MOTION TO ADOPT County Auditor's Recommendations.

(This item was pulled by a member of the public.)

ACTION: (T-11:06 AM) Approved. (Refer to minutes for full discussion.)

VOTE: 9-0.

Attachments

Exhibit 1 - Review of User Access to Kronos Enterprise Time and Attendance System
Exhibit 2 - Management's Response