STATE OF WISCONSIN
Department of Employee Trust Funds
Robert J. Conlin
SECRETARY

801 W Badger Road
PO Box 7931
Madison WI 53707-7931

1-877-533-5020 (toll free)
Fax 608-267-4549
etf.wi.gov

CORRESPONDENCE MEMORANDUM

DATE: June 3, 2014

TO: Audit Committee Members

FROM: John Vincent, Director
              Office of Internal Audit

SUBJECT: WEBS Access Termination Process Review (2013-10)

This report is for Audit Committee review and discussion. No action is required.

Attached is the Executive Summary of the WEBS Access Termination Process Review. The results of this review have been submitted and discussed with the Office of the Secretary, Department of Employee Trust Funds. The Executive Summary provides the review introduction, objective, scope, summary of findings, improvements, and recommendations. There are no recommendations in the report.

I will be available at the Audit Committee meeting to answer any questions.

Attachment: Executive Summary of the WEBS Access Termination Process Review

Reviewed and approved by Robert J. Conlin, Secretary

Electronically Signed 6/12/14

Board	Mtg Date	Item #
AUD	6.26.14	4B

CORRESPONDENCE MEMORANDUM

June 3, 2014

Robert Conlin, Secretary
Department of Employee Trust Funds

AUDIT REPORT

WEBS Access Termination Process Review
(2013-10)

The Office of Internal Audit submits the final report of the WEBS Access Termination Process Review.

The review was requested by the Secretary's Office, following the results of the Legislative Audit Bureau's (LAB) 2012 financial audit. During the audit, LAB found several instances where an employee's access to the Wisconsin Employee Benefits System (WEBS) remained after the employee had terminated. This review was to determine if additional controls could be added to improve the department's process to disable access upon termination.

The attached Executive Summary provides the background, audit objectives and scope, findings, and recommendations. <u>There are no recommendations in the report</u>.

We would like to thank all of the ETF employees who contributed to this review.

Respectfully submitted,

_____
John Vincent
Director, Office of Internal Audit

STATE OF WISCONSIN
Department of Employee Trust Funds
Robert J. Conlin
SECRETARY

_____

EXECUTIVE SUMMARY

WEBS Access Termination Process Review
(2013-10)

June 3, 2014

DEPARTMENT OF EMPLOYEE TRUST FUNDS

WEBS Access Termination Process Review
(2013-10)

EXECUTIVE SUMMARY

Introduction

In its 2012 financial audit, the Legislative Audit Bureau (LAB) found several instances of inappropriate Wisconsin Employee Benefits System (WEBS) access remaining after workers had terminated employment with the department. The department responded by immediately increasing security controls. Additionally, the Secretary's Office asked the Office of Internal Audit to review the new disable and delete security controls for workers' accounts using WEBS to determine if there were control or process improvements that might be recommended.

Audit Objective

Review WEBS access procedures to determine if any additional controls can be added to improve the disable and delete process for terminating workers.

Audit Scope

The scope of the audit is the WEBS access termination process involving the following:

- ETF employees that are in full-time, part-time, limited-term, and project positions who have WEBS access
- Consultants and contractors who have WEBS access
- Employees of third-party administrators (TPA), and other entities outside of the department, who have WEBS access
- Mainframe RACF[1], internal security, and DB2[2] application security processes used to control access to WEBS subsystems and screens
- Current and planned security processing that includes WEBS monitoring and follow-up for delayed implementation of security controls

Summary of Findings and Improvements

In response to the LAB report, the department has initiated a number of control measures and processes involving terminating or terminated department staff, consultants, contractors, and staff of third-party administrators. We reviewed the current process and changes that have been made and have not identified any additional improvements. The measures implemented have added controls, a more comprehensive monitoring process and a broader email distribution group to ensure necessary staff are notified of terminations for implementing appropriate security steps. It should be noted that internal audit discussed the establishment of an automated

---

[1] RACF – Resource Access Control Facility. An IBM program product that provides access control by identifying and verifying users to the system, authorizing access to various data types, logging detected unauthorized attempts to enter the system, and logging detected access to protected data.

[2] *DB2* -- a relational database management system from IBM.

workflow approach to deleting access. Such an approach will be part of the Benefits Administration System.

The department has put into place the following changes:

- Division of Management Services – Bureau of Information Technology
  - RACF ID's are scheduled to expire on the day an employee departs (similar to what is done with Active Directory accounts). Department security administration staff disable the account.

  - The annual review of third-party administrator (TPA) accounts is now a part of the annual review of WEBS access, which is completed during May. ETF security staff will contact the TPAs to review and identify accounts no longer needed.

  - On a monthly basis, ETF security staff generates reports of ID's that have not been used in the past 30 days for Active Directory and 60 days for RACF. Security staff conducts a follow-up with the appropriate ETF supervisors to ensure these accounts are still active. This will also help ensure deletion of TPA accounts that are no longer needed.

  - Addressing LAB's concern about two server administrator accounts:
    - A second account was created for all technical staff that have the need for any administrative access/privileges. These accounts are only used to perform administrative duties.
    - Technical development and support staff no longer have access to the production root ID and password. Administrative privileges needed to execute are given through the pseudo facility assigned to their normal ID.

- Division of Management Services – Human Resources
  - A email distribution group, "ETF Staff Setup-Disconnect," was established to provide supervisors with the contact point to inform IT, Facilities, Human Resources, SAM (Supplies & Mail Services Section) and procurement when a an ETF staff, LTE, project or contractor is terminating.

Another access control currently in development is a process to create reports that monitor administrative access. At this time, ETF security staff are developing an effective report that logs log in and log out times.

Recommendations - *None*