

**Application Access Controls  
Audit Report  
Report Nr. 15/09  
December 4, 2009**

**Distribution:**

To: President & CEO  
Senior Vice President & Chief Financial Officer  
Senior Vice President, Business Solutions & Technology  
Senior Vice President, Human Resources  
Senior Vice President, Financing Products Group  
Senior Vice President, Insurance  
Vice President & Corporate Controller  
Vice President & Chief Information Officer  
Vice President, Insurance COE & CARD  
Vice President Human Resource Services  
Vice President Client Services  
Vice President, Corporate & International Trade Intelligence  
Assistant Controller, Corporate Finance & Control  
Director Cash Management, Taxation & Corporate Insurance  
Director Business Solutions Delivery  
Director CARD  
Director Financial Institutions  
Director Financing COE & International Relations  
Program Delivery Manager, Finance  
Program Delivery Manager, Financing  
Program Delivery Manager, Insurance  
Program Delivery Manager, HR/Legal/President's Group  
Manager, Client Services Centre  
Manager, Financial Reporting  
Credit Standards Manager  
Manager, Credit Standards & Scoring  
Manager, Accounts Payable  
HRIS Lead  
Business Analyst, Loans Services COE  
Business Analyst, CARD  
Accounts Payable Coordinator

**Audit Team:**

S. Slechta  
H. Klosevych  
N. Bylen

**Vice President, Internal Audit**

M. Ryan

CC: Senior Vice President, Corporate Secretariat & Legal Services  
Senior Vice President, Business Development  
Vice President & Treasurer  
Director Loans Services  
Program Delivery Manager, Business Development  
Manager, Insurance Accounting & Canada Account  
Project Business Lead Loan Services  
Vice President, Strategic Planning & Corporate Communications  
Director, Planning & Government Relations  
Principal, Office of the Auditor General

## Introduction

In accordance with our 2009 Audit Plan, EDC Internal Audit performed an audit of Application Access Controls.

## Audit Objectives & Scope

The overall objective of this audit was to evaluate the effectiveness of the controls in place to ensure access to business applications is appropriately restricted in order to ensure the on-going integrity of application data. Specific areas of examination included controls to ensure:

- ▶ Access is properly authorized;
- ▶ Access is assigned on an as needed basis and is not excessive relative to the employee's job function;
- ▶ Segregation of duties is maintained;
- ▶ Timely removal of access when an employee leaves or changes roles; and
- ▶ Access by BS&T System Administrators to the production environment is restricted.

In examining these areas the audit addressed the following risk elements of EDC's Enterprise Risk Management (ERM) framework: system risk, compliance risk, information security risk, and transaction processing risk. The scope of the audit included: PS FIN, CAS, ACBS, Globex, CRS, MBC, FIRM, PS HR, MTIP, C3, GAS, and UFS. Audit fieldwork was performed during October and November 2009.

## Internal Audit Opinion

In our opinion, *Opportunities Exist to Improve Controls*<sup>1</sup> surrounding access to business applications. We found that access is not being granted on an as needed basis for eight of the twelve business applications included in our scope. As a result, we noted excessive access to super user and security administrator profiles. Security administrators do not always have the information needed to determine if access requests are valid. Periodic review of access is not being consistently performed across all the business applications included in our scope. As a result, user access is often excessive in relation to roles. We have recommended that super user access be removed and granted on a temporary basis as needed. Security administrator profiles should only be granted to those responsible for performing this function. We have also recommended that the security administrator role be performed by the business. Finally, access to critical business applications should be reviewed on a periodic basis to ensure it remains commensurate with user roles.

---

<sup>1</sup> Our standard audit opinions are as follows:

- **Strong Controls:** Key controls are effectively designed and operating as intended. Best in class internal controls exist. Objectives of the audited process are most likely to be achieved.
- **Well Controlled:** Key controls are effectively designed and operating as intended. Objectives of the audited process are likely to be achieved.
- **Opportunities Exist to Improve Controls:** One or more key controls do not exist, are not designed properly or are not operating as intended. Objectives of the process may not be achieved. The financial and/or reputation impact to the audited process is more than inconsequential. Timely action is required.
- **Not Controlled:** Multiple key controls do not exist, are not designed properly or are not operating as intended. Objectives of the process are unlikely to be achieved. The financial and/or reputation impact to the audited process is material. Action must follow immediately.

## Audit Findings & Recommendations

### 1. Access to Privileged Accounts

Super user and administrator type profiles allow users to make changes directly to production data without being subject to the normal transaction processing controls. We noted that privileged accounts have been granted on a permanent basis to BS&T users in all systems with the exception of MTIP, UFS, GAS and ACBS. Processes are not in place to monitor/review changes made by users holding these profiles. We recommend that privileged accounts be assigned to a limited number of BS&T individuals on a temporary basis as needed. In situations where permanent access cannot be removed, the risks and business rational for specific users having this profile should be approved by senior management.

Rating of Audit Finding - Major<sup>2</sup>

Action Owner - Security Administrators & BSD Managers

Due Dates - Q2 2010

### 2. Access to Security Administrator Profiles

The security administrator profile enables the holder to grant any valid network user access to system profiles including super user type profiles. We found that, in several applications, the security administrator profile has been granted on a permanent basis to BS&T and/or business users who are not responsible for security administration (PS FIN, CAS, CRS, Globex, MBC, FIRM, and PS HR). In addition, there is no periodic review of the user profiles for several applications to ensure access is being granted on an as needed basis. We recommend that the security administrator profile be removed from all users who are not responsible for security administration. In addition, we recommend that processes be implemented to review access to critical business applications on a periodic basis.

Rating of Audit Finding - Major

Action Owner - Security Administrators & BSD Managers

Due Dates - Q2 2010

### 3. Periodic Review of Access to Application Systems

Processes are in place to periodically review the appropriateness of access to the following systems: UFS, PS FIN, MTIP, ACBS, CAS, and C3. However, there is no periodic review of the appropriateness of access to Globex, CRS, MBC, FIRM, PSHR and GAS. As a result, several instances were noted by where user's access was no longer required, excessive or created inappropriate segregation of duties. We recommend that a periodic review of access to the production environment be implemented. This should include validation of user/BS&T access with user managers and system owners.

Rating of Audit Finding - Major

Action Owners - Security Administrators

Due Dates - Q2 2010

---

<sup>2</sup> The ratings of our audit findings are as follows:

- **Major:** a key control does not exist, is poorly designed or is not operating as intended and the financial and/or reputation risk is more than inconsequential. The process objective to which the control relates is unlikely to be achieved. Corrective action is needed to ensure controls are cost effective and/or process objectives are achieved.
- **Moderate:** a key control does not exist, is poorly designed or is not operating as intended and the financial and/or reputation risk to the process is more than inconsequential. However, a compensating control exists. Corrective action is needed to avoid sole reliance on compensating controls and/or ensure controls are cost effective.
- **Minor:** a weakness in the design and/or operation of a non-key process control. Ability to achieve process objectives is unlikely to be impacted. Corrective action is suggested to ensure controls are cost effective.

#### 4. Client Service Center - Facilitator vs. Security Administrator

The Client Service Center ('CSC') acts as a facilitator in granting access to application systems by serving as a single point of contact for access requests and obtaining the necessary approvals. In addition to this facilitator role, the CSC also performs the security administrator role for CRS, Globex, FIRM and MBC. As security administrator, the CSC is responsible for determining whether a user should be granted access and whether the requested access is appropriate in relation to the requestors job function. However, we noted that the CSC is not always provided the information needed to make this decision. When acting as a facilitator the CSC does not always obtain and provide approvals to the security administrators in the business. We recommend the role of the CSC be limited to facilitating security administration. Explicit approvals should be captured via emails or sign-off on the access request form. Approvals should be forwarded to the security administrator in the business to ensure that approval is captured prior to granting access.

Rating of Audit Finding - Major  
Action Owners - Client Service Center & System Administrators  
Due Dates - Q2 2010

#### Conclusion

The audit findings and recommendations have been communicated to and agreed by management, who has developed action plans that are scheduled for implementation no later than Q2 2010.

We would like to thank management for their support throughout the audit.