

Delegation of Authority (DOA) – Phase II
Final Audit Report
Report Nr. 11/10
August 27, 2010

Distribution:

To: President & CEO
Senior Vice President & Chief Financial Officer
Senior Vice President, Legal Services & Secretary
Senior Vice President, Insurance
Senior Vice President, Business Solutions & Technology
Senior Vice President, Human Resources
Vice President & Corporate Controller
General Counsel & Senior Assistant Secretary
Vice President & Chief Risk Officer
Vice President, Portfolio Management
Vice President, Insurance COE & CARD
Vice President, Credit Insurance Underwriting
Vice President, Human Resources, Client Services
Vice President, Organizational & Employee Development
Vice President & CIO
Assistant Secretary and Legal Counsel, Corporate Secretariat
Director, Asset Management
Director, CARD
Director, Financial Institutions
Director, Enterprise Portfolio Management
Director, RAPM
Director, Loans Services
Director, Cash Management, Taxation and Corporate Insurance
Manager, Business Solutions Insurance
Senior Purchasing Advisor, Purchasing

CC: Senior Vice President, Business Development
Senior Vice President, Financing Products Group
Vice President, Strategic Planning & Corporate Communications
Director, Planning & Government Relations
Manager, IT Business Management
Principal, Office of the Auditor General
Director, Office of the Auditor General

Audit Team:

N. Bylen
A. Lowe
L. Schoutsen
F. Tian
T. Wilson

Vice President Internal Audit

M. Ryan

Introduction

In accordance with our FY 2010 Audit Plan, EDC Internal Audit performed an audit of Delegation of Authority (DOA). Delegation of authority within EDC is established and governed through the Export Development Act, EDC By-Laws, and GEN-002. Specifically, Section 8(2) of the Export Development Act assigns authority to the President and CEO of EDC for all matters that are not explicitly reserved to the Board of Directors. Section 19 (1) of the EDC By-Laws outlines the transactions the Board of Directors reserves the right to authorize. Authority for all other transactions rests with the President & CEO of EDC. EDC's GEN-002 outlines the process for assigning this DOA. The appendices to GEN 002 detail the approved DOA levels by transaction type. The following table provides a list of DOA appendices in scope and whether DOA is captured manually or electronically within a business application. For those cases where DOA is performed electronically the name of the business application is provided.

GEN-002 Appendix	Electronic/Manual	System Used to Capture DOA
Appendices C/C1 & C/C1(LTP): Credit Granting Authority and Credit Granting Endorsement- Financing, Insurance, Guarantees and Equity	Electronic	CAS, Globex, FIRM, MBC
Appendix C2 - Asset Management	Manual	Not Applicable
Appendix C4 - Risk Transfer	Manual	Not Applicable
Appendix C5 - Credit Granting Commitment Extension	Manual	Not Applicable
Appendix I - Financial Accounting Division	Electronic	ACBS
Appendix K - Human Resources' Activities	Manual	Not Applicable
Appendix G- Treasury Division	Manual	Not Applicable
Appendix G2 - Asset & Liability Management	Manual	Not Applicable
Appendix N - Procurement Policy	Manual	Not Applicable
Appendix O - Claims and Recoveries	Electronic	CRS
Funding Approval for Technology Projects*	Manual	Not Applicable

* The Funding Approval for Technology Projects has historically been applied as a DOA in practice but is not currently within the scope of GEN-002. We included it in the above list and in the scope of our audit as efforts are currently underway to incorporate the funding approval as an Appendix to GEN-002.

Audit Objectives & Scope

The DOA audit has been conducted in two phases. Phase I of the audit was completed in 2009 and resulted in a *Well Controlled*¹ opinion on the design effectiveness of the DOA controls. This report addresses the results of Phase II of the audit. The overall objective of Phase II was to perform detailed testing of the DOA controls to ensure they are operating as intended.

The scope of the audit included the following GEN 002 appendices:

- Appendices C/C1 & C/C1(LTP): Credit Granting Authority and Credit Granting Endorsement Financing, Insurance, Guarantees and Equity
- Appendix C2 - Asset Management
- Appendix C4 - Risk Transfer
- Appendix C5 - Credit Granting Commitment Extension
- Appendix I - Financial Accounting Division
- Appendix K - Human Resources' Activities
- Appendix N - Procurement Policy

¹ 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.

- Appendix O - Claims and Recoveries
- Funding Approval for Technology Projects (not in GEN 002)

The Treasury Appendices (G, G2) were under revision and therefore were not included in the scope of this audit. In addition, changes were being made to the MBC DOA table applicable to medium and long-term Financing and therefore we did not test that component of Appendix C/C1. Testing of these areas will be completed by the end of Q4 2010. In examining the DOA process, the audit addressed the following risk elements of EDC's ERM framework: compliance, system, and transaction processing risk. Audit fieldwork was performed between March and June 2010.

Internal Audit Opinion

In our opinion, application of the DOA levels outlined in the Appendices of GEN-002 included in the scope of this audit is *Well Controlled*. Specifically, the results of our detailed testing confirm that transactions are being approved in accordance with the levels specified in the following appendices of GEN-002:

- Appendices C/C1- Credit Insurance
- Appendix C2 - Asset Management
- Appendix C4 - Risk Transfer
- Appendix C5 - Credit Granting Commitment Extension
- Appendix I - Financial Accounting Division
- Appendix K - Human Resources' Activities
- Appendix N - Procurement Policy
- Appendix O - Claims and Recoveries

Moderate² areas for improvement were identified and are outlined in the following section.

Audit Findings & Recommendations

1. DOA Table Maintenance

The audit included a testing of the controls surrounding the maintenance of DOA tables within Globex, CAS, FIRM, ACBS and CRS. Specifically whether:

- Write access to the DOA tables is assigned on an "as needed" basis;
- Segregation of duties (SOD) principles are respected by ensuring those responsible for updating the DOA table are independent of transaction processing;
- Changes are made based only on approved requests that are consistent with the relevant appendix of GEN 002; and
- There is an annual review of the DOA table to validate that DOA levels continue to match GEN 002.

² 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.

We found the above controls were operating as intended for CAS, ACBS and CRS. However, with the exception of SOD, we found that the above controls are not being applied consistently to the maintenance of the Globex and FIRM DOA tables. As noted in the Application Access Controls Audit (Report #15/09), write access to the Globex and FIRM DOA tables are excessive. We also found that the changes made to the Globex DOA table are not always supported by an approved request, while FIRM does not maintain a transaction trail of the changes made to the DOA table and therefore, we were unable to test changes to the DOA table. A periodic review of the Globex and FIRM DOA tables is not performed and as a result we found that some employees change roles but continue to have DOA authority in Globex or FIRM and/or have DOA levels in excess of what is allowed under the relevant GEN-002 appendices. It should be noted however, that detailed testing of both Globex and FIRM transactions confirms that transactions are being approved in accordance with GEN-002.

Excessive write access to the FIRM and Globex DOA tables and change management are being addressed through previous audit recommendations. We recommend that the DOA tables be reviewed on a periodic basis (annually as a minimum) to ensure DOA is removed from employees who change roles and to ensure assigned DOA levels continue to respect limits outlined in GEN 002.

Rating of Audit Finding – Moderate

Action Owners - Business Solutions Insurance in conjunction with System Owners

Due Dates – Q1 2011

2. Clarity of DOA Appendices

Appendix C-1 (Section 5) describes automatic approvals of credit commitments for insurance products in CAS via the decision support model as being considered “*duly authorized*”. The language in this section of C-1 also allows for such automated DOA credit commitment approvals to apply to any “*current or future equivalent system*”. The FIRM system also employs automated DOA approval of TFO policies via the Fast Track process. In 2009, approximately 60% of the TFO policies were approved via the Fast Track Process. FIRM does not use automated DOA approvals for granting credit to obligors. We recommend that consideration be given to clarifying the wording in Appendix C-1 to cover documentation implementing any credit commitment through automated DOAs such as those performed in FIRM. We also recommend that consideration be given to outlining the Fast Track and DSM DOA limits in the Appendix C Table.

The Claims and Recoveries System (CRS) also employs an automated DOA feature that results in automatic approval of claims below \$5000 via the “Exprog” profile (Express Claims Authorization). The wording of Appendix O of GEN-002 does not currently provide for this automated DOA. Accordingly, we recommend that the wording in Appendix O be updated to specifically provide for automated DOAs, and that consideration be given to incorporating automated DOA limits in the Appendix O Table.

Rating of Audit Finding – Moderate

Action Owners - Corporate Secretariat, Director CARD in conjunction with Legal Services

Due Dates – Q2 2011

3. Controls Around the Use of DOA Delegates in CRS

There are a number of CRS users who have delegation up authority and/or delegation down authority in CRS. Delegation up authority refers to the ability to approve a transaction in the system on behalf of someone with a higher DOA limit. Delegation down authority refers to the ability to approve a transaction in the system on behalf of someone with a lower DOA limit. Accordingly, the scope of audit included an examination of whether:

- Delegation up authority was recorded in CRS only after verifying that the transaction had been manually approved by the proper DOA authority;
- Delegation up authority was granted to a limited number of users with the explicit approval of the individual with the higher DOA limit;
- A transaction trail of the use of both delegation up or down authority is maintained and reviewed periodically.

We tested a sample of transactions approved in CRS via the delegation up authority and found that in all cases, the approval in CRS was recorded after verifying that the transaction had been manually approved by the proper DOA authority. A process does not currently exist, however, to formally assign delegation up authority based on the DOA authority's consent. There is also an opportunity to reduce the number of users with delegation up authority. CRS has been configured such that a delegate assumes the identity of the DOA authority when approving transactions on their behalf. As a result, the transaction appears as if it were approved by the DOA authority versus the delegate. We recommend that a process be established to assign delegation up authority based on the explicit approval of the DOA authority and that the number of users with delegation up authority be limited. We also recommend that a CRS report be created to enable periodic monitoring of the use of delegation up authority.

Rating of Audit Finding – Moderate

Action Owners – Director CARD in conjunction with Legal Services

Due Dates – Q4 2010

4. Application of the Funding Approval for Technology Projects

EDC's "Guidelines for the Approval and Monitoring of Designated Expenditures" requires that designated expenditures in excess of \$5M CAD be approved by the Board of Directors prior to management entering into related commitments. Technology projects greater than \$5 M CAD are an example of a designated expenditure. Accordingly, BS&T has developed a document entitled "Funding Approval for Technology Projects" outlining the incremental approvals required based on the dollar value of a technology project up to approval by EDC's Board of Directors as a Designated Expenditure. This approval document has been embedded and applied as part of BS&T's Engagement Delivery Model and is in the process of being incorporated into GEN-002 as a formal DOA document. Although it is not yet a formal DOA policy we included it in the scope of our audit as it is being applied as a DOA in practice and its application represents an important process prior to seeking Board approval of a Designated Expenditure.

We found that the correct level of approval is not always being obtained for technology projects. Although formal approvals were not obtained, it was clear that business sponsors were aware of and supported the project. However, we recommend that the requirement for timely formal approvals be reinforced to ensure business sponsors support the value of the project relative to its cost. Consideration should be given to reinforcing this concurrent with the rollout of the *Funding Approval for Technology Projects* as a formal DOA.

We also noted that there is inconsistency in defining the start and end of a technology project. For example, in some cases the selection and implementation of a business application is broken down into several projects such as Requirements Definition, Vendor Selection and Implementation. Approval is sought based on the budget of each of these projects rather than the total cost through implementation which is used as the basis for obtaining approvals on other technology projects. We recommend that clarification be included in the formal DOA policy regarding the definition of a technology project (i.e. start and end) to ensure consistent application of the DOA policy.

Rating of Audit Finding – Moderate

Action Owner – Director, Enterprise Portfolio Management

Due Dates – Q4 2010

Conclusion

The audit findings and recommendations have been communicated and agreed to by management, who has developed action plans that are scheduled for implementation no later than Q2 2011.

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