Correctional Service Canada　Service correctionnel Canada

FUTURA RECIPERE

SAFETY, RESPECT
AND DIGNITY
FOR ALL

LA SÉCURITÉ,
LA DIGNITÉ
ET LE RESPECT
POUR TOUS

AUDIT OF LOGICAL ACCESS CONTROLS

Internal Audit Branch

378-1-240

Approved by Audit Committee

May 20, 2008

Canada

EXECUTIVE SUMMARY

CSC, as part of the criminal justice system and respecting the rule of law, contributes to public safety by actively encouraging and assisting offenders to become law-abiding citizens, while exercising reasonable, safe, secure and humane control. In order to meet its objectives, CSC relies on a number of internal information systems which contains sensitive information and/or are deemed mission critical to the Service. Considering that logical access controls (i.e. user ids and passwords giving users' access to the corporate network or corporate applications) is the foundation of IT security, these controls have to be seen as the primary means to protect CSC from unauthorized access to our corporate systems and the sensitive information within them.

As part of the 2007-08 internal audit plan, an audit of logical access controls at the Correctional Service Canada (CSC) was conducted by the Internal Audit Branch with the assistance of Deloitte.

The scope of this audit included an assessment of logical access controls for specific, key applications at CSC including: OMS – Offender Management System, IFMMS – Integrated Financial and Material Management System, HRMS – PeopleSoft) as well as the Data Warehouse (DW). In addition, Microsoft's Active Directory and remote access (Virtual Private Network) were included in the scope of this audit as these systems are "gateways" to other applications.

Logical access controls for these key applications have been evaluated against the COBIT control objectives "Plan and Organize" and "Ensure Systems Security". Specifically this audit evaluated the following objectives:

- *Plan and Organize - An IT risk management framework and risk assessment process has been developed and implemented to manage and assess logical access control risks; and,*
- *Ensure System Security - Applications are appropriately secured to prevent unauthorized use, disclosure, modification, damage or loss of data.*

Overall Conclusion

Plan and Organize - CSC has designed and implemented some key controls to assist with the identification and assessment of IT security risks. These controls include the use of a Threat Risk Assessments (TRA) approach for assessing risks and the use of the MITS assessment which management has used to identify gaps. However, CSC does not yet have a comprehensive CSC-wide IT risk management framework and risk assessment process to allow IT management to systematically identified and prioritize IT security needs. Further, the TRA for the applications in scope need to be updated.

Ensure System Security - For those applications in scope of the audit, controls are in place to ensure that new user's access is authorized and that IT security policies and procedures are communicated to these new users. In addition, security incident and monitoring activities for the OMS system have been designed and implemented. However, further efforts are required to design and/or implement controls to prevent unauthorized access to CSC's applications. [redacted] In addition, considerations should also be given to further integrate security responsibilities as well [redacted]. These measures could further enhance IT security and provide efficiencies if implemented.

Recommendations have been made to address the control deficiencies.

Senior management has reviewed, and agrees with, the findings contained in the report. The Management Action Plan which addresses the recommendations is included in Appendix C.