National Defence / Défense nationale

Chief Review Services / Chef - Service d'examen

CRS / CS Ex

Follow-up on Audit of Information Technology Security: Certification and Accreditation

July 2009

7050-33-6 (CRS)



Canada

Caveat

The results of this work do not constitute an audit of the IT certification and accreditation process. Rather, this report provides an update on the progress made regarding the Management Action Plan provided in response to the September 2007 Audit of IT Security: Certification and Accreditation.

Table of Contents

Reviewed by CRS in accordance with the *Access to Information* Act (AIA). Information UNCLASSIFIED.

Acronyms and Abbreviations

ADM(IM)	Assistant Deputy Minister (Information Management)
C&A	Certification and Accreditation
COS(IM)	Chief of Staff Information Management
CRS	Chief Review Services
DND/CF	Department of National Defence/Canadian Forces
Dir IM Secur	Director Information Management Security
FY	Fiscal Year
GSP	Government Security Policy
IM Gp	Information Management Group
IT	Information Technology
L1	Level 1
MAP	Management Action Plan
SA	Special Assistant
VCDS	Vice Chief of the Defence Staff

Introduction

As required by the Treasury Board Policy on Internal Audit, Chief Review Services (CRS) undertook an audit follow-up to assess the implementation of the management action plan (MAP) provided by the Vice Chief of the Defence Staff (VCDS) and Chief of Staff Information Management (COS(IM)) in response to the *Audit of Information Technology (IT) Security: Certification and Accreditation (C&A)* (September 2007).

The Government Security Policy (GSP) states that "departments must apply baseline security controls, continuously monitor service delivery levels, track and analyse threats to departmental IT systems, and establish effective incident response and IT continuity mechanisms."[1] The C&A process is the primary mechanism to ensure that baseline security controls are applied and additional controls are implemented to prevent compromise of the confidentiality, integrity and availability of Department of National Defence and Canadian Forces (DND/CF) information from internal and external threats. Director Information Management Security (Dir IM Secur) is the DND/CF IT security coordinator and is responsible for ensuring that DND/CF IT systems have been properly certified and accredited prior to operating.

The Department's ability to maintain public and international confidence, to comply with government statutes such as the *Security of Information Act* and the *Privacy Act*, and to support the successful completion of military operations and government initiatives such as audited financial statements, relies heavily on the confidentiality, integrity and availability of numerous information systems. The sensitivity of information in DND/CF is wide-ranging—public and commercial information, personal data, military operations, and national and international intelligence—and its confidentiality, integrity, availability and value to the Department needs to be preserved.

Methodology

This audit follow-up is not another audit of the same issues, but rather a review of documentation and evidence to assess progress made in implementing the MAP as at 15 April 2009. The following methods were used to determine progress made regarding the MAP:

- Interviewed Dir IM Secur and Dir IM Secur staff;
- Interviewed SA2/VCDS; and
- Examined policy documents, plans and reports related to the C&A process.

Overall Assessment

At the time of the follow-up, Assistant Deputy Minister (Information Management (ADM(IM)) was about to publish its "Certification and Accreditation Revitalization Plan" designed to reduce the C&A backlog ..... within the current C&A process. Besides clearly outlining the "C&A process" responsibilities of the Strategic Joint Staff, Level 1 (L1) system operational authority stakeholders, technical authorities and Information Management

[1] *Government Security Policy*, S10.12, February 2002.

Group (IM Gp) entities, the document categorizes the C&A priorities into four tiers from the highest to lowest priority networks, facilities and applications with the intent being to address the tier one highest priority items within the next 12-18 months.

Conversely, while the C&A Revitalization Plan represents a positive way ahead, progress has ..... however, an attempt to hire a contractor to carry out the planned in-depth C&A process study was unsuccessful. ...

MAP Implementation Progress

Certification and Accreditation

..... of the C&A process so as to ..... with the GSP and associated standards and guidelines, ... It was also recommended that departmental policies be updated and necessary resources be identified, funded and acquired in order to implement ..... Updated policies and additional resource requirements would be based on the results of this analysis, and were to be completed by June 2008. .....

Conduct of the in-depth C&A process study was to have been performed by a contractor, but in January 2009, the only bidder was deemed non-compliant. Dir IM Secur is currently considering other alternatives to meet this commitment.

In December 2008, Dir IM Secur allocated one full-time resource to gain a situational awareness on internal processes and inter-relationships with other IM Gp organizations. .....
.....
.....
.....
The results of these evaluations are to be coordinated with the C&A staffs and incorporated in the C&A study. In parallel, the Enterprise Information Security Environment Project is exploring longer-term options for an automated C&A approach starting with the development of approved security architecture and eventually rolling out software that could identify and flag non-approved configurations. This longer-term solution is envisioned to provide considerable processing and productivity improvements. .....
.....
.....
.....
.....

Attention is currently focussed on accrediting all DND/CF information systems that appear on Dir IM Secur's C&A system list ..... The accuracy of the C&A status has been verified for all designated domain information systems appearing on Dir IM Secur's list, ...
.....
.....

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

More progress has been made regarding the resource-related recommendations. Dir IM Secur has staffed most positions in the current establishment and 17 additional positions have been approved through the business planning process and the C&A Revitalization Initiative plan ...
.....
.....
.....
.....
.....
This increase would fund the additional salaries and a contract for nine Information System

Security Officers to assist operational authorities in completing the required C&A documentation. However, the FY 2009/10 Business Plan has not yet been given final approval and therefore the status of the funding request is unknown.

Residual Risk

An information system is accredited once the Operational Authority accepts the residual risk.
.....
.....
.....
.....
.....
.....
.....
.....
.....

.....
.....
.....
.....
.....
..... VCDS agreed and anticipated that initial actions to quantify and develop recommendations for senior executive management on the issue of IT C&A residual risk management would be completed by the end of March 2008; IM Gp staffs were to assist in this effort as required.

Although current DND/CF risk management policy does refer to the setting of risk tolerance levels and there are ongoing efforts to incorporate risk management practices into the defence planning and management process, ...
.....
..... Representatives from Deputy Provost Marshal Security, Dir IM Secur, Strategic Joint Staff Plans, and Director Intelligence Information Management did develop a proposal and a risk management matrix that addressed most of the report's recommendation, ...
..... The VCDS group is currently determining how best to address the report's recommendation, but will be looking at it from an overall risk acceptance perspective, rather than just as an IT requirement.