

**COMPREHENSIVE AUDIT OF
HRDC'S (SDC & HRSDC)
INFORMATION TECHNOLOGY
SECURITY**

**SOCIAL DEVELOPMENT CANADA
AUDIT & EVALUATION
DIRECTORATE**

ISACA Ottawa Valley Breakfast Session

Marriott Hotel, Ottawa

March 8 2005

INTRODUCTION

Audit Team

- ❖ SDC Internal Audit
Jim Blain, Paul LePage, Mike Winterburn, Ken Allen, F-M Brière
- ❖ Communication Security Establishment (CSE)
Edward Bleackley, Alain Di Stefano, Luc Dandurand
- ❖ Electronic Warfare Associates (EWA)
Jim Robbins, Rob Walters
- ❖ SDC Stakeholders
ITSS/Dave Beach, DSO/Serge Ash

Approved by HRDC's Audit & Evaluation Committee in Fall, 2003

Consultations with:

- ❖ Office of the Auditor General, IT Audit Services
- ❖ Treasury Board Secretariat (TBS), Government Operations Services
- ❖ TBS, Chief Information Officer Branch
- ❖ Royal Canadian Mounted Police, Technical Security Branch
- ❖ EWA
- ❖ CSE
- ❖ Minister, National Defence Approval
- ❖ Deputy Ministers' MOU – Security Posture Assessment

APPROACH

Three-Phased Audit

❖ **Phase 1: ITS Governance Framework**

(October, 2003 – March, 2004)

- SDC Internal Audit & EWA
- Conducted at NHQ (including Montréal & Belleville ITCs), and the Quebec, Ontario, Alberta/NWY/Nunavut, & BC/Yukon Regions

❖ **Phase 2: Internal ITS Vulnerabilities**

(February, 2004)

- SDC Internal Audit & CSE (Onsite Technical Vulnerability Assessment)
- OTVA: conducted inside the department on department premises

❖ **Phase 3: External ITS Vulnerabilities**

(March – August, 2004)

- SDC Internal Audit & CSE (Active Network Security Testing)
- ANST: conducted outside the department on CSE premises

PHASE 1 - OBJECTIVES

Phase 1: ITS Governance Framework (October, 2003 – March, 2004)

Assess ITS Controls: Management, Operational, Personnel and Technical

- ❖ Management Controls (e.g. 'ITS management structure should be documented, integrated into HRDC's programs, and supported by all levels of management')
- ❖ Operational Controls (e.g. 'ITS policies/procedures should describe HRDC's ITS roles, responsibilities and services')
- ❖ Personnel Controls (e.g. 'An HRDC ITS Awareness Program should be nationally implemented')
- ❖ Technical Controls (e.g. 'ITS safeguards (e.g. firewalls, anti-virus) should be maintained (where appropriate), monitored (e.g. ITS attacks) and adjusted (as warranted)')

PHASE 1 - OBJECTIVES

Document a network map of HRDC systems for Phase 2 (OTVA) and 3 (ANST) testing

Assess status of issues from previous ITS audits: 2002 OAG and 1999 Internal Audit

❖ **2002 OAG ITS Audit**

- better implement the ITS governance framework
- conduct broad-based risk assessments
- provide employees with adequate training in ITS awareness
- ensure that ITS is considered at the start of a system development life cycle
- carry out ITS audits/reviews (including technical vulnerability testing)

❖ **1999 IARMS ITS Audit**

- streamline HRDC's organizational structure/processes to manage ITS at all levels
- enhance the knowledge and awareness of all HRDC personnel regarding ITS

PHASE 2 - OBJECTIVES

Phase 2: Internal ITS Vulnerabilities (February, 2004)

- ❖ **Conduct an internal (e.g. employee) Vulnerability Assessment of HRDC's systems**

- ❖ **Onsite Technical Vulnerability Assessment (OTVA)**
 - Network/Host Scanning
 - Network Vulnerability Scanning
 - Router Assessment
 - LAN Switch Analysis
 - Wireless Access Point Discovery
 - Mobile Device Policy Review
 - Password Assessment
 - Dial-Up Discovery/War Dialing

PHASE 3 - OBJECTIVES

Phase 3: External ITS Vulnerabilities

(March – August, 2004)

- ❖ **Conduct an external (e.g. 'hacker') Vulnerability Assessment of HRDC's systems**

- ❖ **Active Network Security Testing (ANST)**
 - Network Scanning
 - Network Probing
 - Vulnerability Identification
 - Exploitation Research and Development
 - Exploit Activities

CLIENT PERSPECTIVE

- ❖ Importance of ITS audit (e.g. proactive vigilance, raising ITS awareness, etc.);
- ❖ Communication with auditors (e.g. understanding audit objectives/expectations, etc.);
- ❖ Liaising with (Systems) senior management (e.g. management support/cooperation, etc.);
- ❖ Responding to audit findings and implementing audit recommendations (e.g. Management Action Plan - prioritizing, timing, budgeting, risk ranking, etc.)
- ❖ Lessons learned (from a client (auditee) perspective)

LESSONS LEARNED

- ❖ Cultural Change
- ❖ IT Awareness – Everyone's Responsibility!
- ❖ Strategically Maintain ITS Enhancements
- ❖ Senior Management Support
- ❖ Comprehensive - Technical and Non-technical
- ❖ Continuous Client Liaison
- ❖ OAG (and Other 3rd Party) Liaison

For further information, contact:

Paul LePage (613 – 277 – 2479)

Paul.LePage@sdcdsc.gc.ca