



Management of IT Security (MITS)

Implementation and Audit Approach

Presentation to ISACA

23 March 2006

Bruce Hunter, Treasury Board Secretariat



Outline

- Introduction and Context
 - MITS “Call for Action”
- MITS Overview
- MITS Implementation Approach
- Assessment and Audit

The Need is Real

- “The threat of cyber-attacks is real, ... consequences ... can be severe.”
 - National Security Policy 2004
- “Vulnerability assessments ... have revealed significant weaknesses that, if exploited, could result in serious damage to government systems.”
 - OAG February 2005
- “A weakness or a breakdown in federal government IT security would have serious implications for Canadians and the availability of all manner of services upon which they depend.”
 - PAC 14th Report 7 June 2005



Attention is Required

- “...the government has much work to do to translate its policies and standards into ... practices that will result in a more secure IT environment in departments and agencies”
 - OAG February 2005
- “...expects that (government) will assign urgent priority to ... ensuring that Canadians have secure, trustworthy electronic access to government programs and services.”
 - PAC 14th Report 7 June 2005

Senior Management Audience

- “senior management is not aware of security risks and does not understand how breaches could affect operations and the credibility of government. If ... allowed ... Canadians' trust in the government would be greatly eroded.”
 - OAG February 2005
- “IT security action plan should be approved by the deputy head or designated and reported to TBS.”
 - OAG February 2005
- “TBS develop and implement a plan for an awareness of the importance of IT security among senior departmental managers”
 - PAC 14th Report 7 June 2005



MITIS Overview





Management of IT Security (MITS)

- MITS defines baseline security requirements that departments must fulfill to ensure the security of information and information technology assets.
 - 144 mandatory requirements
 - Reflects commonly accepted best practice
- MITS implementation requires a risk management approach.
 - Flexibility for departments to implement MITS within the context of their corporate risk profile
 - Graduated application of management controls and technical and operational safeguards should be commensurate with the risks
- MITS emphasizes the need for “active defence” using the Prevent-Detect- Respond-Recover paradigm



MITs Key Requirements

- MITs focuses on the following key IT security management requirements:
 - Security Organization
 - Security Policy
 - Identify IT security resources in new services/systems
 - IT security throughout the System Development Life Cycle
 - Identification and categorization of information and IT Assets
 - Risk Management
 - Incident Management
 - Vulnerability Management
 - Business Continuity Planning
 - Audit & Assessment
 - Awareness & Training



MITs Key Requirements

- Security Organization
 - IT security requires IT security, DSO, CIO, IT, program and service owners, and senior management personnel working together in a concerted effort
 - To be successful, an effective organization must be in place early
- Security Policy
 - Security policy applies GSP/MITs in departmental context
 - Other measures are often dependent on policy
- Identify ITS resources in new services/systems
 - Resources must be driven by business needs
 - Lack of resources often cited as a key problem



MITIS Key Requirements

- System Development Life Cycle
 - A management framework is required to ensure security is applied at all stages of the SDLC
 - Security must be designed in: it cannot be bolted on after the fact
- Identification of Assets
 - Must identify most important services/systems to prioritize plans and mitigate highest risks first
- Risk Management
 - Risks must be understood and accepted by program owners, and included in the corporate risk profile
 - Threat and Risk Assessments; Certification and Accreditation



MITIS Key Requirements

- Incident Management
 - Recognizing the dynamic nature of threats and vulnerabilities, departments must detect and respond to incidents when they occur
- Vulnerability Management
 - Departments must identify new vulnerabilities, assess the risk, and take action (e.g. apply patches)
 - Number of vulnerabilities continues to grow and the time required to respond is decreasing
- Business Continuity Planning
 - Increased dependence on IM and IT must be reflected in Business Continuity Plans



MITIS Key Requirements

- Audit and assessment
 - Annual assessment of IT security program and practices
 - Supported by self-assessment tool
 - IT security must be included in departmental internal audit planning, priority for audit based on risks
 - Enhanced TBS oversight and monitoring
- Training and Awareness
 - Awareness is key to improve understanding of risks
 - Common understanding between IT security professionals, program owners and senior management



MITIS Implementation Approach





Background

- 2002 Government Security Policy & Auditor General report focus on standards-based approach
 - 47 standards proposed to PAC
- 2004 Publication of MITS
 - Compliance based
 - Implementation by December 2006
- 2005 Auditor General & Public Accounts Committee reports
 - Progress is unsatisfactory
 - TBS introduced the need for a broader strategy to address IT Security



Implementation Plan

- MITIS is key to GC-wide effort to improve IT Security
- Concentrated effort required to improve State of IT Security:
 - MITIS Action Plans reported to TBS: August 2005
 - TBS Analysis of Action Plans: December 2005
 - TBS intervention strategy: March 2006
 - Semi-annual status updates: June, December 2006
 - MITIS implementation target: December 2006
 - Government-wide assessment: 2007



Analysis shows

- Successes:
 - Almost all departments and agencies are actively improving their ITS programs
 - Senior management is engaged
 - TBS has a GC-wide view of the state of ITS security
 - Significant effort underway
- However:
 - A long way to go
 - Fundamentals not yet in place in some departments
 - Inconsistency across the GC
 - Many departments will not comply by Dec 2006



Way Ahead

- MITIS implementation by December 2006 remains a high priority
 - TBS intervention to accelerate MITIS compliance
- Development of IT security Strategy underway to design and implement a sustainable, whole of government IT security program in the longer term (post December 2006)



Assessment and Audit Plans

- While MITS compliance is the focus for December 2006, an enhanced performance measurement framework is required to support security assessments
 - Current approach is compliance based and lacks performance criteria based on effectiveness: The focus is “do we comply?” versus “are we secure?”
 - Enhanced performance measurement framework “under construction”. Compliance will be supplemented by performance metrics such as:
 - Satisfying business objectives
 - State of security (vulnerabilities, incident statistics, impacts, etc)
- IT security self-assessment tool “on hold” pending new performance measures



Assessment and Audit Plans

- Status update provided to Auditor General
- Many departments have planned Internal Audits in 2006/2007
 - Office of Comptroller General reviewing IT security audit plans
 - Update draft IT Security Audit Guide to reflect MITS requirements
 - Supplement compliance with security effectiveness metrics (e.g. Auditor General used vulnerability assessments)

Some References

- 2002 Report of the Auditor General of Canada: IT Security
<http://www.oag-bvg.gc.ca/domino/reports.nsf/html/0203ce.html>
- 2005 Report of the Auditor General of Canada: IT Security <http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20050201ce.html>
- 14th Report of the Standing Committee on Public Accounts: IT Security
<http://www.parl.gc.ca/committee/CommitteePublication.aspx?COM=8989&Lang=1&SourceId=119275>
- Government Response To The Fourteenth Report Of The Standing Committee On Public Accounts http://www.tbs-sct.gc.ca/report/gr-rg/2005/0921_e.asp
- Securing and Open Society: Canada's National Security Policy Apr 2004
http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_e.pdf
- Government Security Policy http://publiservice.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_12a/gsp-psg_e.asp
- Operational Security Standard: Management of IT Security (MITS)
http://publiservice.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/23RECON_e.asp
- Mid Term Report on the Government Security Policy Aug 2005
- Report to Secretary of the Treasury Board, TBS Action Plan to Support the Adoption of MITS
- The CSO' Security Compliance Agenda, Benchmark Research report,
www.securitycompliance.com
- Become Compliant (without breaking the bank), www.infosecuritymag.com





Canada 