



Treasury Board of Canada
Secrétariat

Secrétariat du Conseil du Trésor
du Canada

Information Technology Security in the Government of Canada

ISACA Ottawa Valley Session
March 8, 2005

Linda Hunter
CIOB/TBS

Canada



ITS in the GOC

Today's Agenda

1. The Policy framework
2. Monitoring and oversight
3. The GOC “ITS Community”
4. Raising the profile of ITS
5. Yesterday, Today and Tomorrow



POLICY FRAMEWORK

- Government Security Policy (GSP)
- Policy on the Management of Government Information
- Privacy
- PKI
- Operational Security Standards
- MITS
 - Establishes baseline requirements
 - Compliance = At least, meets all the “musts” (i.e. baseline requirements)

...but implementation is department-specific, risk-based





Also need ...

- Technical guidance
 - Example CSE “red books”
 - TRA guidance
 - CSE, RCMP web site
 - PWGSC and Secure Channel
 - Common CA
 - PKI
 - ...

+ Department-specific policy, standards, guidance





Monitoring and Oversight

- Internal Audit
 - ITS
 - Security
 - Programs, systems and services
- OAG
 - 2002
 - Feb 2005
 - 2007??



ITS Self-Assessment

- Annual
- TBS to collect as requested
 - Validation needed – Internal Audit?
- Questions updated to reflect MITS
- Updates to continue to reflect more of the “hows” and as standards developed
- Departments should use to look at specific systems, small offices

▶ ITS Self-Assessment Results - 2004

- Of the 46 departments that completed responses, 1 met Maturity Level 1 and 2 requirements and 0 met only Level 1. A guesstimate would suggest that approximately 25% of the 45 who did not achieve at least Level 1, have a substantial amount of work in progress towards achieving at least Level 1.
- Of the 45 departments that did not achieve at least level 1, 22 were identified as having some classified information, 13 with some Protected C information and 28 with some Protected B information. Several departments indicated that 100% of their information has no designation or classification.



Results from IT Security Self-Assessment June 2004

1. 16% have no IT Security policy (or policy statements); 11% have no security policy – 33% of those who have a security policy indicate it has no formal management sign-off
2. 35% have no policy requirement to complete TRAs
3. 49 % have no policy requirements for contracts, MOUs, etc to include IT security statements; 36 % have no policy requirements for contracts, MOUs, etc to include security statements
4. 44% have no policy requirements for completion of the SRCL(Security Requirements Checklist); 63% of these do not require review by the DSO and ITSC
5. 2% do not have an ITSC



Results from IT Security Self-Assessment June 2004

6. 94% have requirements for departmental passwords
7. 85% include the identification of the C-I-A (Confidentiality, Integrity, Availability) as part of the SDLC (System Development Life Cycle)
8. 43% do not have / require formal, documented arrangements for sharing information with other governments including foreign, provincial, territorial and municipal, international educational and private sector organizations
9. 52% have no guidance in place clearly identifying what security statements should be covered in such agreements.
10. 12% do not have critical systems identified



Results from IT Security Self-Assessment June 2004

11. 25% do not have a policy requiring incident reporting
12. 26% do not have a policy requiring a BCP for critical systems and services
13. 20% reported they do not have a formal, consistent SDLC; of those that do have an SDLC, 38% do not incorporate IT Security requirements
14. 34% do not have a documented change and configuration management procedure
15. 19% reported they do not have clearly documented security responsibilities for IT security staff;
 - 28% do not have them for IT Operations staff;
 - 50% for program and service delivery managers;
 - 46 % for IT project managers and
 - 33% for all personnel



Departmental Monitoring

- A requirement in GSP
 - Departments are required to conduct active monitoring and internal audits of their security program.
- A requirement in MITS
 - Departments need to actively monitor their management practices and controls. As part of this responsibility, departments assess and audit IT security and remedy deficiencies where necessary.
- TRAs, VAs, Incident management, configuration management and change control, capacity planning, help desk
- Day-to-day operation (people, processes, technology)



The role of TBS and the Lead and Agencies

- Overview of the GoC as a whole
 - Performance Measurement
 - Status of critical systems, services
- Status of specific activities such as TRA, VA, Patch management, Access Control ...
 - Where do we need more / different direction and assistance
 - Priorities for action

The ITS Community

- **Departmental**
 - ITSC
 - Plus other security specialists
 - Technical specialists
 - LAN / network admin, help desk, account managers
 - CIO
 - Business / Information Owners
 - Senior Management
 - Audit
 - All employees
- **Central Agency**
 - TBS
- **Lead Agencies**
 - CSE, PSEPC, RCMP



Committees

- ITS Committee
- CIOC
- PKI-related (PMA, PAC...)
- NSP-related
- Audit
- SIMB
- Service Transformation
- Working Groups on standards
- MITS Implementation Coordination
- Business-related / stewardship ...



Raising the profile of ITS

- Is there a Problem?
 - OAG interviewees said:
 - a lack of money and people,
 - a lack of interest in IT security by senior management, and
 - IT security concerns were not part of the culture in their organizations
- What can we do?
 - More and improved awareness
 - Senior management
 - Business imperative
 - All employees

IT Security is not just about the mouse and keyboard

15



▶ **What can we do?** continued

- Communications
 - Speak the language of the business owner and senior management, not “tech-talk”
- Provide support, advice, assistance
 - Mutual problems, mutual solutions
- Focus on **BUSINESS RISK**

NOT Security or IT risk

- Senior Committees
 - Presentations, presence, ...



ITS in the GOC

Yesterday ...

Today...

Tomorrow ...

In the future...



Yesterday

- Y2K helped drive disaster recovery planning
- OAG 2002 caused us to look at where we were and evaluate our progress
- Relatively static environment, department-centric, limited common/shared, emphasis on technology solutions
- Internal Audits on IT Security rare
- Little discussion of performance measurement

▶ Today

- **National Security Policy 2004 emphasized Business Continuity Planning**
 - PSEPC to “audit”
- **MITS establishes the baseline requirements**
- **OAG 2005**
- **TBS and lead security agencies providing coordination and technical guidance and support**
 - More work with / between departments
 - Best practices, strategies shared
- **More common / shared**
- **Many departments have improved ITS programs**
- **More TRA, VA, C&A**
- **More business owners aware / involved**
- **More audits, more emphasis on performance measurement**



Tomorrow

- **MITIS Compliance**
- **OAG report plus TBS responses as driver**
- **Improved communication** (and understanding)
 - Within departments (security, IM/IT, audit, business, senior management, ...)
 - Between departments (best practices, incident information, threat and risk information)
- **Common/shared infrastructure and services**
 - Secure Channel
 - Some mandatory across GoC
 - Security built-in
 - VA (SPA), Incident management (DARI), threat info ...
- **Performance measurement across the GOC**
- **Communities of interest all involved**

20



In the future --- Personal Musings

- What are the attributes needed across the GOC and in individual departments to:
 - Have a consistent IT Security posture that meets expectations of citizens, business, international partners, ...
 - Get a more positive response on the next OAG report
- Where are we now? What are the gaps?
 - How do we close them?
 - How will we know when we are there?

We're all in this together !!!!!

In the future - - Personal Musings

- Focus on organizational network, not technical
- Driven by business needs, not technical requirements
- Protection of business, not technical, assets
- Business owners, all personnel accept security as a responsibility
- ITS community advises senior management, business, IM/IT, ...
- Integrated – it's a requirement of doing business
 - Compliance with standards more of a by-product
- ONE Risk management process – incorporates ITS +

22



In the future - - Personal Musings

- Measurable – clear, specific goals based on business goals, objectives, priorities
 - Defined targets, measurements + communicated
- People / process centric, not technology with business priorities as focus
- Active defence
 - maintain a common / consistent ITS posture
 - + ability to adapt to constantly-changing risk environment

In the future - - Personal Musings

- Overall approach
 - Enterprise based
 - Resiliency important attribute
 - Security as business enabler
 - Not reactive or a burden
 - Not just because of policy
 - Planned and integrated into overall GOC and departmental business planning and resourcing
 - Clearly defined, consistent
 - Repeatable, measurable, sustainable

In the future - - Personal Musings

- Emphasize critical assets and services
- Senior management support is
 - VISIBLE and ACTIVE
- Security adequately funded because it is a
 - Strategic, budgeted, capitalized investment
- Measurement is planned, on-going, qualitative and quantitative
 - One overall perspective including results of audit , VA, TRA, assessments,
 - MAF focussed

This means we would have:

- Regular TRAs and updates
- Security throughout the SDLC
- Critical assets and services identified and protected
- Departmental and GOC business agenda drives the priorities including ITS direction and strategy
- BCPs in place, tested, current
- Incidents tracked, managed, reported on
- Policy, standards, guidance current
- Job descriptions with security responsibilities included
- Senior management considers ITS risk
- Training for all
- Monitoring incl audits, assessments, technical tests, ...
- Access control, virus control, back-up and recovery, identification and authentication, clearances ... ETC

26





Where do we go from here....

- All - Build on the OAG 2005 report and use the recommendations and comments as a starting point
- Briefings planned
 - MITS forum
 - ITSC
 - DSO meeting
 - CIOC
 - ISSA, ITAC
- CIOB AVAILABLE TO BRIEF YOU, YOUR MANAGEMENT, YOUR DEPARTMENT, COMMITTEES...



Where do we go from here....

- Encourage your department to review and look inward at how well they would have done
- Brief within your department
 - (a detailed deck on the OAG report is available)
- We (collectively) need to do a better job on response and follow-up
- TBS is committed to providing support and leadership
 - **AND** Lead security agencies have indicated their willingness to provide continued support

A possible “project” plan *Short Term*

1. TBS coordination
2. Action plan requested in letter to DMs
3. Departmental response with action plans
4. Meet with departments to review, discuss – on request, during, after ...
5. Follow-up early 2006 – status report or reminder ...
6. Early 2007 – TBS “self-assessment”, with internal audit follow-up on approx 25%
7. Report to Secretary on departments that are compliant – early 2007



A possible “project” plan *Longer Term*

- A funded, resourced, recognized PROJECT
- Common goals, strategy
- Central oversight, coordination
- Departmental implementation
- All communities of interest included
- ITS Performance Measurement





QUESTIONS ??????

- Linda Hunter
(613)948-1135
hunter.linda@tbs-sct.gc.ca



Canada 