

The background of the slide is a blurred image of a document. The word "monitor" is prominently displayed in bold, lowercase letters. Above it, the word "ORIGIN" is visible, and below it, the word "warn" is partially visible. Other words like "thing", "duties", and "picture" are also faintly visible in the background.

# GoC IT Security Compliance (MITSS)

Wendy E. Stewart  
Project Manager for MITSS at PHAC

# Overview

- Definitions
- Impacts
- Implementation Issues and Challenges
- Levels of Compliance
- Evidence of Compliance

# Definitions

- Departments interpret standard's statements differently
  - What is a MITSS "must"?
  - What is an "audit"?
  - What is an "IT Security Policy"?
  - What is my baseline security level?
  - What level of compliancy is reasonable for my department?
- Project priorities dependent on department's mandate and objectives
  - Departmental policy, standards and processes
  - Defined program
  - Critical systems and perimeter security
  - Active defense strategy
  - Incident response

# Impacts

- **Size and Complexity**
  - Does MITSS really expect me to perform TRAs and C&As on every application and system we have?
  - What's going on in the other branches and regions?
- **Organization**
  - How does IT Security fit into the corporate risk management framework?
  - How can I promote IT Security and be responsible for compliance when I have limited authority and ability to influence my organization?
  - Governance does not support MITSS
- **Culture**
  - What am I - Police or consultant?
  - How can I get to know what's going on before the project's ready to deploy?
  - Lack of awareness and support

# Issues

- Information assets are not known
- Information is not categorized (Protected, Classified)
- Business owners have not defined concept of operations
- Security is considered a barrier to programs, instead of an enabler
- Executives do not encourage security awareness or support compliance
- IT Security is not part of risk management framework
- People are too busy to support the changes introduced by the project
- Concentrate so much on attaining compliance and documentation that security actually suffers!

# Challenges

- Short timeframes
- Lack of funding
- Not enough trained staff available to support project deliverables
- Competing priorities
- Changing environment (e.g. common & shared services being implemented)
- Variation is what “compliance” means within the organization and the government
- Little or no executive influence

# IT Security (MITSS) Project Purpose

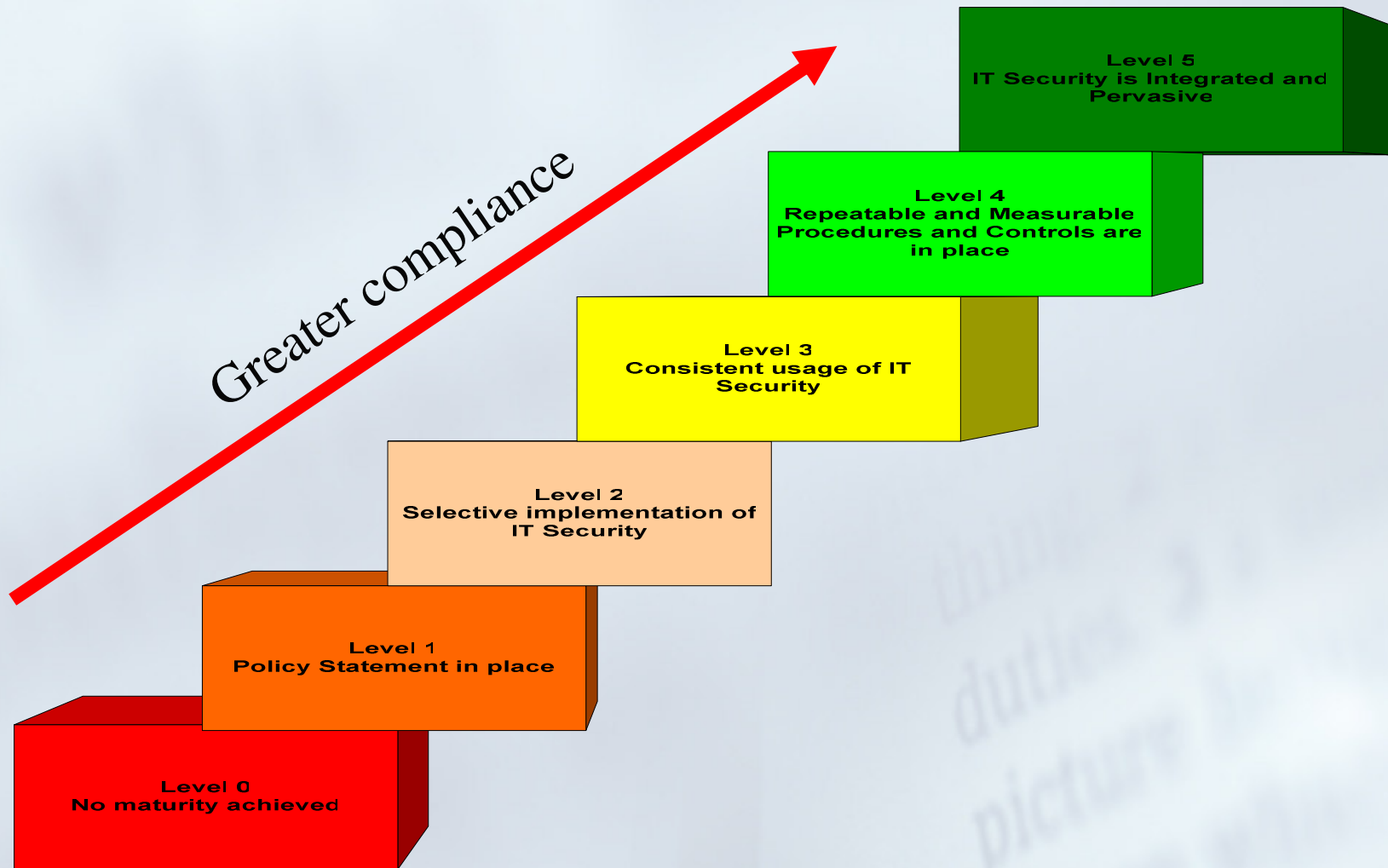


Establish an ongoing risk-based IT Security Program to fulfill TBS' mandated Management of Information Technology Security Standard (MITSS) compliancy by December 2006 and support the department's risk posture.

# Project Approach

- **Iterative phases**
  - Initial high level plan, with next phase's detailed planning during prior phase
  - Phase deliverables approved before next phase begins
- **Concurrent activities**
  - Policy development occurs while training, processes and tools are defined
  - Policy implemented while tools are implemented
  - IT Security program is gradually introduced, as staff are available and trained to take over from consultants
- **Flexibility**
  - As TBS publishes new standards applicable to IT Security, the project adapts and applies new standards to its deliverables
  - As common service offerings become available and mandated, the project takes advantage of such services

# Security Capability Maturity Model



# SCMM – Level Descriptions

Level	Definition	Description
0	No maturity achieved	Level 1 points have not been achieved.
1	Policy in place	Policy or policy statements (or standards) exist and are approved by Senior Mgmt committee and/or DM, with responsibilities and authority assigned.
2	Selective implementation of IT Security	IT Security Policies and Standards are well documented and acknowledged by employees and managers. Security measures are selectively implemented only to satisfy selected requirements.
3	Consistent usage of IT Security	IT Security Polices and Standards are implemented across the dept to varying levels, with compliance randomly assessed.
4	Repeatable and measurable procedures and controls in place	IT Security Policies and Standards are used routinely with consistent and repeatable results. IT security management is an integral part of departmental service implementation cycle. Work is being undertaken to surpass baseline requirements.
5	IT Security is integrated and pervasive	IT Security Policies and Standards are consistently applied/used across the organization. Dept. surpasses many or all GoC baseline security requirements.

# Applying the Maturity Model

- As with other maturity models, one level must be completed before the next one begins, in order to build on reusable results
- To attain compliancy for a maturity level, all requirements for that level must be met
- Maturity levels can vary by grouping systems and products by organizational criticality

# Strategy for Compliancy?

- Action Plan submission to TBS stated the following goals for December 2006:
- Continue to improve towards SCMM Level 5 beyond December 2006
- Full compliancy may never be reached
  - Cost
  - Labour and time commitments
  - Risk mitigation
  - Value / return on investment
  - Pervasive change (common services, program demands)

# Compliance ?

- Going through the motions of the risk management model (SoS, TRA, C&A) does not mean that compliance has been achieved
- Documentation is not enough; processes must be documented, measured and repeatable (fewer well-done are better than many that are not applied)
- Clearly defined deliverables that are accepted and supported by entire organization

# Evidence of Compliance

- Level 1:
  - IT Security Program
  - IT Security Policy
  - Security Sanctions
  - ITS Operational Tools and Supporting Processes
- Level 2:
  - Governance
  - Awareness Program
  - Statement of Sensitivity for critical applications
  - Contract Reviews
  - SA/SLA Reviews
  - Security Patching & Configuration Management
  - Backup, Restore and Archive Handling
  - Logging and Monitoring
  - Segregation of Duties (Operations)
  - MOU Reviews
  - Self-Assessment Process
  - Portable Device Management
  - Remote Access
  - Incident Response
  - Intrusion Detection
- Level 3:
  - IT Security Policy Compliance
  - IM/IT Continuity Planning
  - ITS Support Development, Implementation & Training
  - System Development Life Cycle
  - Ongoing Operational Support
  - ITS Project Toolkit
  - Segregation of Duties (Data Owners)
  - Data Classification, Labelling, Storage & Disposal
  - Wireless Safeguards
  - Physical Security for Telecom
  - Personnel Screening
  - Identification & Authentication
  - Cryptography
  - ITS Architecture
  - System Hardening

# Evidence of Compliance (continued)

- Level 4:
  - ITS Program Review, including penetration testing
  - Certification & Accreditation
  - Program Planning
  - Audit Follow-up
  - Business Continuity
  - Active Defence Strategy
  - Malicious Code Prevention
  - Security Incident Response
  - Continuous Improvement of Incident Response
- Level 5:
  - SDLC Compliancy
  - Government-wide Incident Handling
  - Vulnerability Management
  - Self-Assessment
  - Active Incident Monitoring
  - Impact Assessments
- Some variations on levels may be required, as Levels 2-4 may not reflect risk-based approach
- Complete Levels 2-3 for critical applications and perimeter systems before beginning non-critical systems

# Recommendations for Success

- Enhance the IT Security Section that includes policy and continuous process improvement, led by dedicated IT Security Coordinator
  - To support project and to evolve ongoing program for corporate history, knowledge exchange and continuity of objectives
  - Build the IT Security Program by gaining cooperation from IM/IT experts
- Establish Technical Architecture Review Board, incorporating IT Security and Privacy as risks that influence IM/IT decisions
- Ensure that all IT-related projects and programs use the approved IT Security System Development Life Cycle process before going into production (including TWF projects), which includes SoS, TRA, C&A and, if required, PIA completion
- Make IT Security Awareness training mandatory for all personnel through the corporate Security Policy, beginning with new employee orientation and executive training
- Encourage establishing a Corporate Risk Officer that looks at all risks and influences decisions, based on organization-wide risks and supports the Integrated Risk Management Framework
- Provide DM-level executive support and funding to achieve MITSS compliancy to the program
- Ensure that organization is addressing its security needs, not just compliance to policies and standards by providing regular audits which include vulnerability assessments and penetration testing, without informing the ITS operational staff, to test response processes as well as layered security defense.

# Questions?

- Wendy E. Stewart  
[wendy\\_stewart@phac-aspc.gc.ca](mailto:wendy_stewart@phac-aspc.gc.ca)

[weastewart@sympatico.ca](mailto:weastewart@sympatico.ca)

613-825-9470/851-2059