

# **Policy, Roles and Standards Security Enhancement Project**



**Privacy and Security Conference:  
Synergies in an e-Society**

**Project Lead: Brent Grover**

**February 9, 2005**



# Agenda

- **Purpose**
- **Goals and Objectives**
- **Organizational Maturity**
- **PRS Sub-Projects**
- **Wrap Up and Questions**



# Policy, Roles and Standards (PRS)

## Purpose

- To clarify and strengthen government's policies and standards around IT Security, while also clarifying roles and responsibilities.

## Carpe Diem

- Opportunity to create consistent, repeatable and documented processes for the Office of the CIO based on a structured policy framework.
- Policy Development Process

# Policy Development Process

**Defined Consultation Process**

**Policy Framework**

<b>Clusters</b>	<b>Instruments</b>
<b>Statutory Requirements</b>	<b>Legislation, Regulation</b>
<b>Policy Tools</b>	<b>Core Policy, Operational Policy/Procedure, Standard, Guidance</b>
<b>Communication Tools</b>	<b>Memo, Bulletin, Directive, Alert</b>

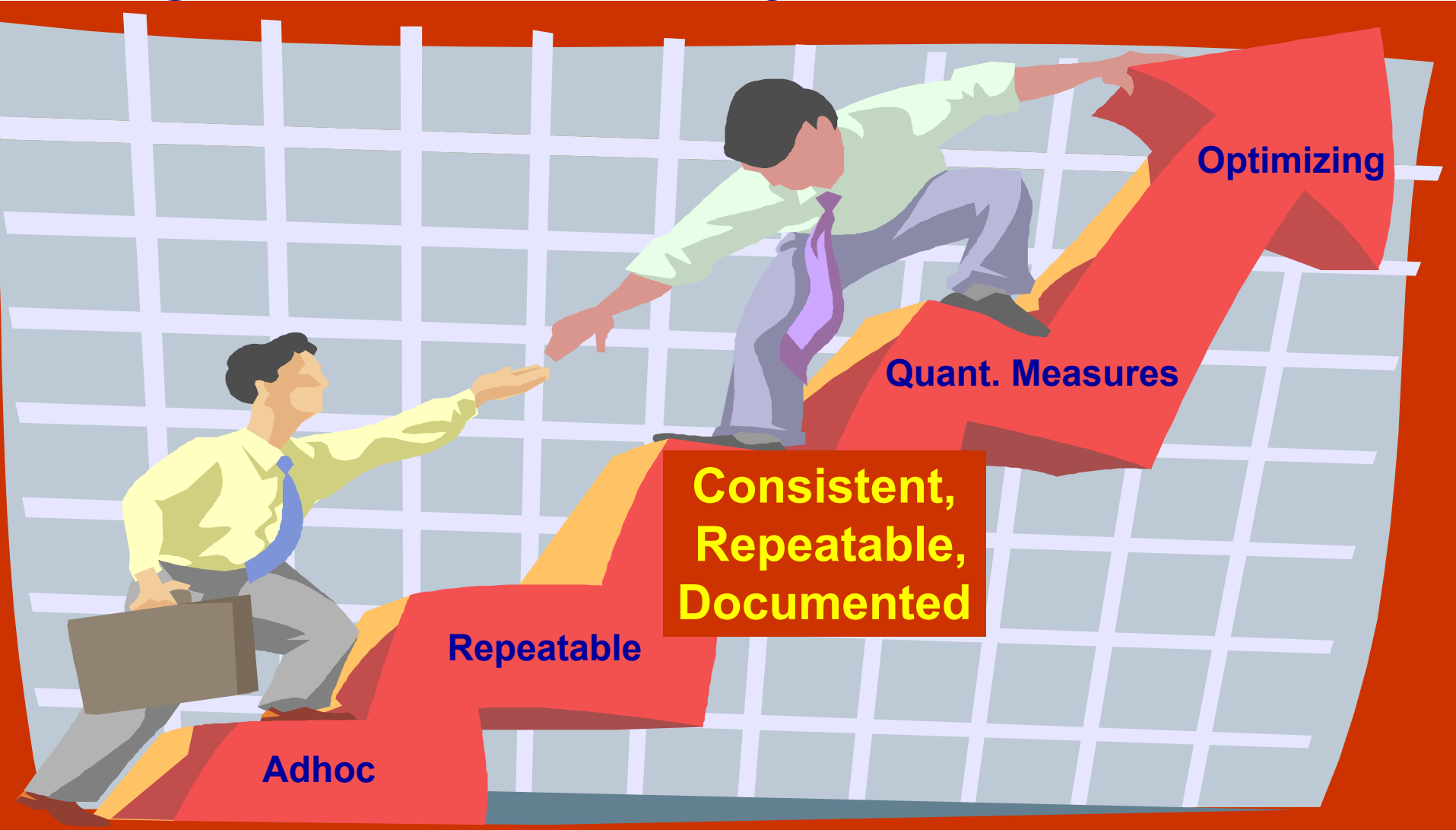


# Policy, Roles and Standards (PRS)

## Goals and Objectives

- **Base security policies, procedures and measures on internationally recognized best practices**
- **Standardize approach to policy development for the Office of the CIO (Information Policy and Privacy role)**
- **Create an Enterprise Security Policy that is consistent, repeatable, documented and will in the very near future be measurable and enforceable**

# Organizational Maturity





# **PRS Sub-Projects**

**CPPM Chapter 12**

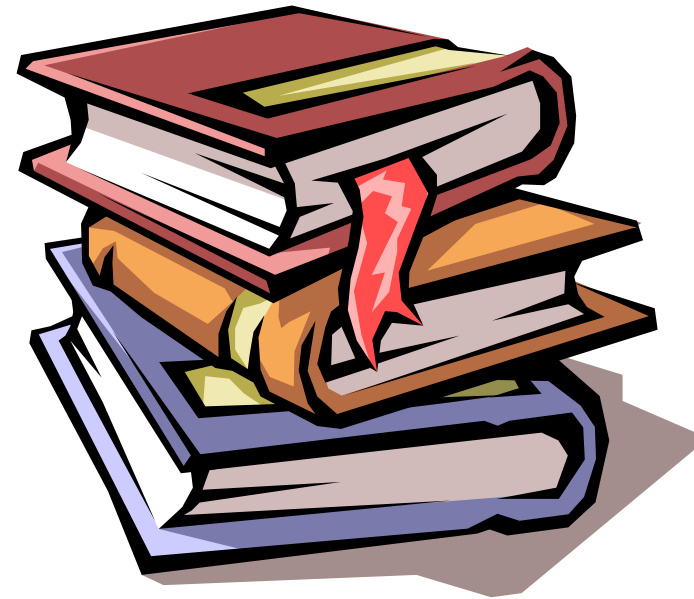
**IT Security Policy**

**Roles and Responsibilities**

**Standards**

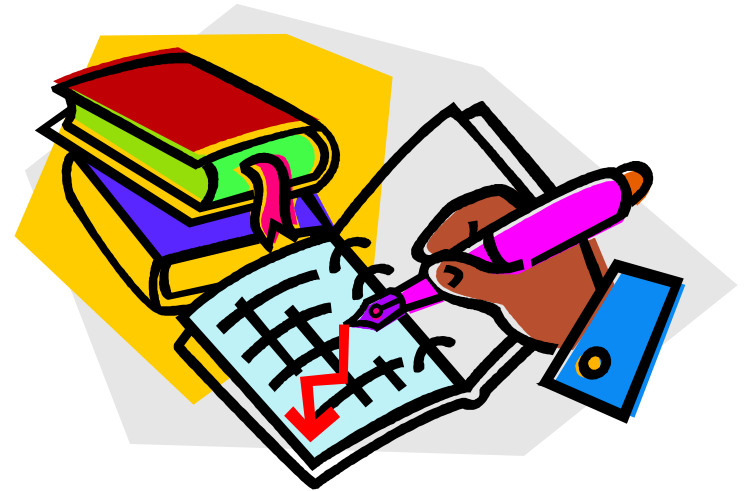
# CPPM Chapter 12

- Replaced the General Management Operating Policy
- Based on Financial Administration Act s. 4 and 9
- Government CIO responsible for IM/IT Management - Chapter 12
- Oblique IM/IT security references in Chapter 15



# CPPM Chapter 12

- **Identify and Document Content Owners**
  - Consistent, repeatable, documented process and policies
- **Distill text to Principle Statements**
  - Consistent, documented policies
  - 133 security policies
  - 18 principles (draft)
- **Augment supplementary manuals to describe the people, processes and procedures**



# CPPM Chapter 12



## For More Information Contact:

Phil Jennings  
Information Policy and Privacy Branch  
Strategic Planning and Policy  
Office of the Chief Information Officer  
(250) 387-0326

# IT Security Policy



## ISO 17799:2005

- 11 Domains, 39 Categories, 133 Policies
- Structured approach to Information Security
- Internationally recognized
- Covers the water front, reduces/eliminates blind spots



# IT Security Policy Format



## Common Look and Feel

- Looks like it was issued by the CIO

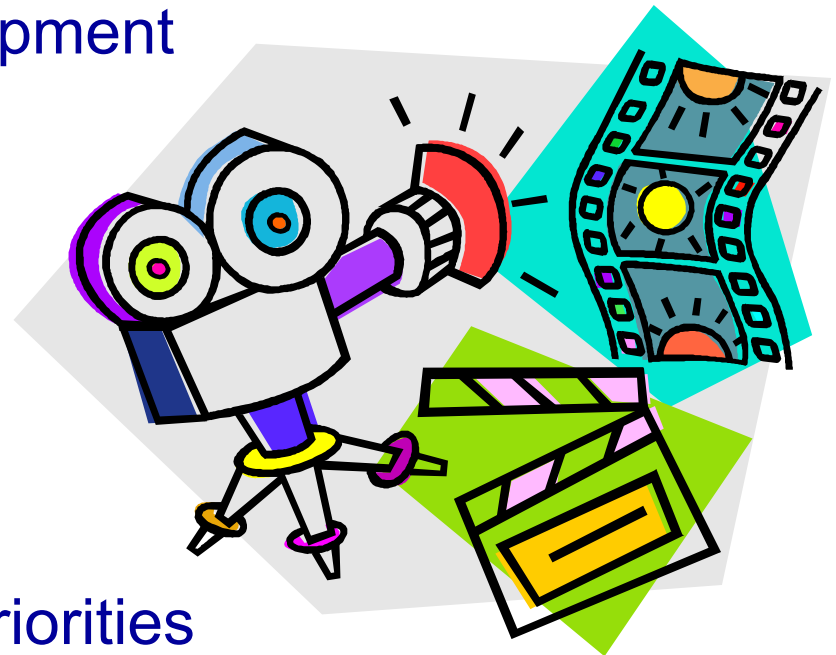
## Combines Policy, Procedures, Standards and Guidelines in one place

- Reduces the need for specialist knowledge
- Easy to ‘pull’ a policy and have everything you need to put it into context
- Consistent, repeatable, documented

# Shooting List

## Shooting List (like in the movies)

- Schedule for policy development
- Three phases
  - Balance workload
  - Identify Quick Wins
  - Identify Must Do's
- Schedule published
- Shift to meet new needs/priorities
- Non-sequential, development as resources, priorities dictate



# Consultation Process



## CIO Consultation Process (via Sharepoint)

- Draft prepared
- Circulate to SMEs - Review/Revise
- Circulate to business and IT contacts - Review/Revise
- Identify issues
- Recommend to SEP Steering Committee
- Approval by the CIO

# Research To Date

## International

- Australia
- New Zealand
- Malta
- Malaysia

## United States

- Georgia, Maine and New York

## Canada

- Ontario
- Alberta

**Plus Standards sites – NIST, ISO, ANSI, etc.**



# IT Security Policy



## For More Information Contact:

Lori Bulmer, CISSP

IT Security Branch

Office of the Chief Information Officer

(250) 356-1890

# Roles and Responsibilities



## Authorities

- Policy framework

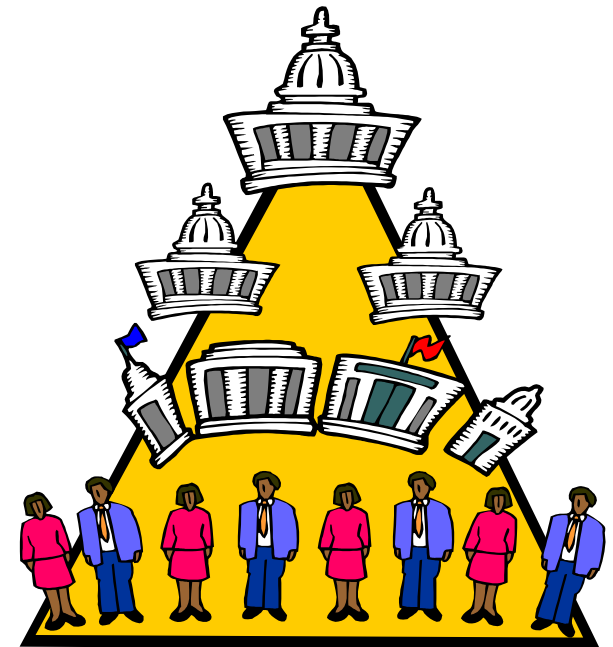
## Organizational changes

- Restructuring
- Centralizing functions e.g.,  
Shared Services

## Downsizing

- People, Budgets, Programs

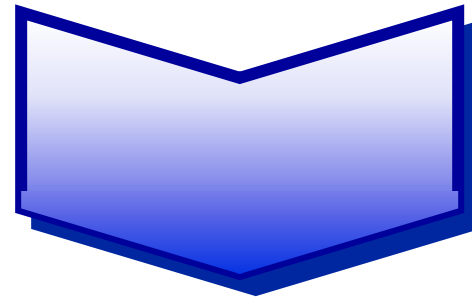
## Policy Synchronization



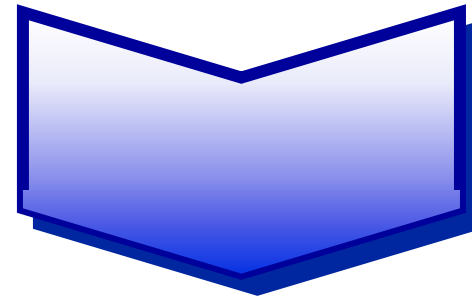
# Roles and Responsibilities



**CPPM, Chapter 12**



**IT Security Policy**



**Procedures**

# Roles and Responsibilities



## For More Information Contact:

Phil Jennings (Chapter 12)  
Information Policy and Privacy Branch  
Strategic Planning and Policy  
Office of the Chief Information Officer  
(250) 387-0326

Lori Bulmer (IT Security Policy)  
IT Security Branch  
Office of the Chief Information Officer  
(250) 356-1890

# Standards

- **Policy (paper) Standards**
  - Standard Forms or Templates
  - Phrasing for Contract Language
  - Inventory Requirements
- **Technical Standards**
  - Hardware and Software
  - Anti-virus, patch versions, etc



# Standards

- **Technical standards in partnership with Business Requirements, and Technical Project Streams of SEP**
- **Liaise with Architecture and Standards, Office of the CIO and other stakeholders**
- **Documented as part of the IT Security Policy**
- **Consistent, repeatable, documented**



# What We Covered

- **PRS Purpose**
- **PRS Goals and Objectives**
- **Organizational Maturity**
- **PRS Sub-Projects**
- **Contacts and References**



## For More Information Contact

### **Brent Grover**

Project Lead: Policy, Roles & Standards

(250) 356-0604

Brent.Grover@gems8.gov.bc.ca

### **Lori Bulmer, CISSP**

Senior Security Advisor: Policy, Roles & Standards

(250) 356-1890

Lori.Bulmer@gems3.gov.bc.ca

**S**

**Presentation available at:**

**<http://www.mser.gov.bc.ca/privacyaccess/Conferences/>**

# References

[Policy Development Process](http://gww.cio.gov.bc.ca) at [gww.cio.gov.bc.ca](http://gww.cio.gov.bc.ca)

Australia - [www.dsd.gov.au/library/infosec/acsi33.html](http://www.dsd.gov.au/library/infosec/acsi33.html)

New Zealand - <http://www.security.govt.nz/sigs/sigs.pdf>

Malta – links to other pages -

<http://www.cimu.gov.mt/htdocs/section.asp?s=76>

Malaysia - [www.sgcert.org/pdf/chapter1.pdf](http://www.sgcert.org/pdf/chapter1.pdf)

Georgia - [gta.georgia.gov/vgn/images/portal/cit\\_1210/62/58/1218035EnterpriseInforSecurityPoliciesGEITLF.pdf](http://gta.georgia.gov/vgn/images/portal/cit_1210/62/58/1218035EnterpriseInforSecurityPoliciesGEITLF.pdf)

Maine - <http://www.maine.gov/CIO/ispb/IT%20Security%20Policy.doc>

New York - [wings.buffalo.edu/computing/policies/NYS-CyberSecurity-3-7-03.pdf](http://wings.buffalo.edu/computing/policies/NYS-CyberSecurity-3-7-03.pdf)



**Thank you for your time**

**Questions?**