

# ***How do we get to 100% FOI & Privacy compliance?***

## **Managing, Monitoring and Improving Access and Privacy Compliance in Your Organization**

Eric Lawton

October 27, 2009

Ontario Access and Privacy Workshop  
Toronto, Ontario

***How can we improve our compliance?***

***What do we do this year? Next year?***

***Is there an end in sight?***

***When will the resources I've given you finally be 'enough'?***

# Three reasons to map

To evaluate

1. What we do (**practices**)
2. Where we want to go (**goals**)
3. How to make the change (**process improvements**)

# Capability Maturity Models

- The **concept** of maturity models is **well developed** and accepted.
- CMMs are valuable tools for business planning and **risk mitigation**.
- Capability Maturity Models assist organizations in achieving strategic objectives through maturing **decision-support** processes
- CMMs are used to **benchmark** risk management strategies to identify program maturity levels, **strengths and weaknesses**, and next steps in the evolution of business processes.
- When organizations start using CMM, the level of implementation is usually **low or uncertain**.
- At present, the City of Toronto has not formally adopted CMMs for decision-making.

# Generic CMM Levels

## 1. Initial (Worship the Hero)

- **Ad hoc** decision-making processes, occasionally even **chaotic**.
- Few defined processes.
- Success depends on individuals abilities and experience.
- **Remove** an individual and the processes may change dramatically commiserate with the next individual's level of ability and experience.

## 2. Repeatable (Write it Down)

- **Basic** management processes are established.
- Management activities are documented.
- Necessary process **discipline** is in place to repeat earlier successes.
- **Examples** exist of the desired behaviour and these are publicised.

## 3. Defined (Plan the Work, Work the Plan)

- Defined management requirements are **integrated** into the decision-making process.
- All decisions use the **approved standards** for decision-making.
- Management requirements and standards are **promoted** by leaders and governance bodies.

## 4. Managed (Informed Decision-Making)

- **Detailed** measures of management decisions are established.
- **Formal** processes exist to manage risk and quality of management decision-making
- All the **processes** and outputs are quantitatively **understood** and **controlled**.

## 5. Optimising (To Infinity And Beyond)

- **Continuous** process improvement enabled by quantitative **feedback**
- Piloting **innovative** ideas and technologies to improve processes and **services**.

# Example – US DoC Maturity Model

- The Dept of Commerce IT **Architecture Capability Maturity Model** (ACMM) provides a framework that represents the key components of a productive IT architecture process.
- The goal is to **enhance the overall odds for success** of IT architecture by identifying weak areas and **providing a defined evolutionary path** to improving the overall architecture process
- Proposes five levels of maturity
  - 0 – None
  - 1 – Initial
  - 2 – Under development
  - 3 – Defined
  - 4 – Managed
  - 5 – Measured
- **Nine characteristics**

Process	Operating Unit Participation
Architecture Development	Architecture Communication
Business Linkage	IT Security
Senior Management Involvement	Architecture Governance
IT investment and acquisition strategy	

# Creation of the AP-CMM

- To develop a model that Access and Privacy Professionals can use to address the whole “evaluate, change, review” assessment cycle, I need to complete all 12 steps in the cycle identified below.

- 1. Agree on maturity model structure (levels and attributes)**

2. Describe each maturity level in a summary “vision statement”

- 3. Identify a set of characteristics which comprise each attribute**

- 4. Define each characteristic for each maturity level**



- 5. Determine how to measure each characteristic**

6. Create diagnostic tools to measure characteristics

7. Create analysis tool to assist in interpretation of data

8. Identify barriers to progressing between maturity levels

9. Identify enablers to overcome barriers

10. Create generic template “development plans” for moving between maturity levels

11. Perform pilot applications of the model, reviewing and modifying if necessary following pilot

12. Publish

# Creation of the AP-CMM

- To develop a model that Access and Privacy Professionals can use to address the whole “evaluate, change, review” assessment cycle, I need to complete all 12 steps in the cycle identified below.

- 1. Agree on maturity model structure (levels and attributes)**

2. Describe each maturity level in a summary “vision statement”

- 3. Identify a set of characteristics which comprise each attribute**

- 4. Define each characteristic for each maturity level**

- 5. Determine how to measure each characteristic**

6. Create diagnostic tools to measure characteristics

7. Create analysis tool to assist in interpretation of data



- 8. Identify barriers to progressing between maturity levels**

9. Identify enablers to overcome barriers

10. Create generic template “development plans” for moving between maturity levels

11. Perform pilot applications of the model, reviewing and modifying if necessary following pilot

12. Publish

# Creation of the AP-CMM

- To develop a model that Access and Privacy Professionals can use to address the whole “evaluate, change, review” assessment cycle, I need to complete all 12 steps in the cycle identified below.

- 1. Agree on maturity model structure (levels and attributes)**

2. Describe each maturity level in a summary “vision statement”

- 3. Identify a set of characteristics which comprise each attribute**

- 4. Define each characteristic for each maturity level**

- 5. Determine how to measure each characteristic**

6. Create diagnostic tools to measure characteristics

7. Create analysis tool to assist in interpretation of data

- 8. Identify barriers to progressing between maturity levels**



- 9. Identify enablers to overcome barriers**

10. Create generic template “development plans” for moving between maturity levels


11. Perform pilot applications of the model, reviewing and modifying if necessary following pilot

12. Publish

# Applying the *Access and Privacy Capability Maturity Model* to Your Organization

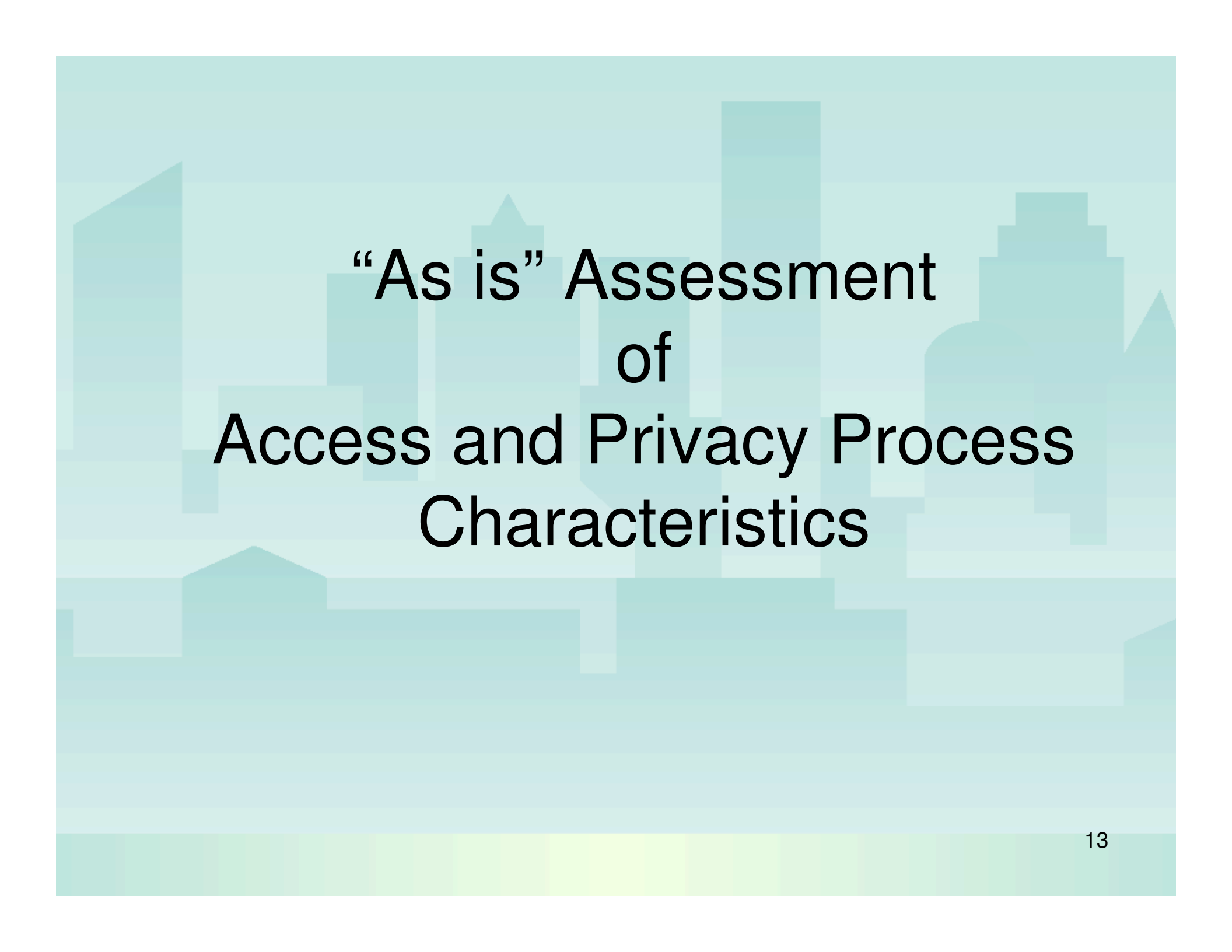
- Discuss the **attributes** for each level's process areas, revise if necessary.
- This will enable the organization to assess itself against an **agreed scale**.
- *Proposed AP-CMM reflects **Information Management** principles of:*
  - ▶ *Accessibility*
  - ▶ *Stewardship & Accountability*
  - ▶ *Risk Management*
  - ▶ *Usability & Quality Control*
  - ▶ *Integration*
- Having discovered its level, the organization can then **set clear targets** for improvement, aiming towards the next levels of capability and maturity.
- AP-CMM will provide a **roadmap** to the successful adoption of best practices in risk management for better decision-making.
- *You could have a multiplicity of Capability Maturity Models. CMM approach may be applied to other key decision-support processes such as Enterprise Architecture, Project Management, Financial Planning, Strategic Planning, etc.*

# Three reasons to map

- To evaluate
  - What we do (practices) 
  - Where we want to go (goals)
  - How to make the change (process improvement)

# Access & Privacy Capability Maturity Model

	Level 1 – Initial/ Ad hoc	Level 2 – Repeatable Processes	Level 3 – Defined Processes	Level 4 – Managed 100% Compliance	Level 5 - Optimising
<b>CAPABILITY BASICS</b> (Without which we cannot develop)	Senior Management Commitment	<b>Partial</b>	<b>Significant</b>	<b>Substantial</b>	<b>Full</b>
	Full COE Resources in place	Minimal	<b>Partial</b>	<b>Significant</b>	<b>Substantial</b>
	Policies and Procedures	No	Minimal	<b>Partial</b>	<b>Significant</b>
<b>CAPABILITY DEVELOPMENT</b> (Leveraging the basics)	All Staff Trained	No	Minimal	<b>Partial</b>	<b>Significant</b>
	Fully Embedded Divisional Resources	No	No	Minimal	<b>Significant</b>
	Functionally Joined Up Across the City	No	No	Minimal	<b>Significant</b>

The background of the slide features a stylized, light blue and green city skyline with various building shapes and heights. The text is centered over this background.

# **“As is” Assessment of Access and Privacy Process Characteristics**

# Process Area 1: SENIOR MANAGEMENT COMMITMENT

(Stewardship and Accountability)

Capability Cornerstone – Without which we cannot develop

- Level 1 (Initial)** – Limited management team awareness or involvement. Little communication about privacy compliance and process requirements. Creation of Chief Privacy Officer/Access Coordinator position and delegate.
- Level 2 (Repeatable)** – Basic management processes are established. Occasional/selective management team promotion. Due diligence activities are documented. Recognition that accountability must extend past CIPO.
- Level 3 (Defined)** – Pro-active response to risks and issues, no waiting for impact to appear. Defined management requirements are integrated into the decision-making process. All decisions use the approved standards for decision-making. Management actively supports Access and Privacy principles and understands these are corporate objectives.
- Level 4 (Managed)** – Senior management team directly involved in the privacy risk management process. Formal processes to manage risk and quality of management decision-making. All the processes and outputs are quantitatively understood and controlled. Only qualified/trained resources used in projects. Managers reinforce training on a day to day basis
- Level 5 (Optimising)** – Continuous process improvement enabled by quantitative stakeholder feedback. Senior management team directly involved in the optimization of IM processes.

## Process Area 2: Centre of Excellence / Expert Resources (Accessibility)

Capability Cornerstone – Without which we cannot develop

**Level 1 (Initial)** – COE can provide strategic support and advice only, no capacity for project involvement. Identify need to build expert capacity.

**Level 2 (Repeatable)** – limited capacity to take on new projects, needs assessments are possible, COE performs research on trends and new orders, legislation and trains own staff. COE coordinates roster(s) of consultants. COE develops performance measures.

**Level 3 (Defined)** – moderate capacity to perform corporate projects, corporate training, effective tracking and reporting processes established

**Level 4 (Managed)** – COE is routinely contacted for advice and support and risk assessments, COE can meet all requests within reasonable timeframe, COE supports corporate governance processes, centralised monitoring and reporting occurs. Transition from use of consultants/temp staff to internal resources.

**Level 5 (Optimising)** – COE performs research and professional development activities to support corporation.

# Process Area 3: Policies and Procedures

(Risk Management and Usability and Quality Control)

Capability Cornerstone – Without which we cannot develop

**Level 1 (Initial)** – few policies and procedures, generic roles and responsibilities, unsatisfactory mandatory reporting to IPC

**Level 2 (Repeatable)** – incomplete/outdated set of policies and procedures have been identified; tools borrowed from other jurisdictions; job descriptions created; basic access and privacy procedures established; taxonomy created for education purposes.

**Level 3 (Defined)** – Enterprise has full set of policies and procedures, risk management tools; Routine Disclosure policies in place; PIA policy; specialised roles and responsibilities are defined; Privacy Architecture artifacts created for EA framework; dependencies with other domains like information security are described; divisional best practices are publicized.

**Level 4 (Managed)** – Enterprise policies and procedures are known to all staff, communicated, and referenced in risk management processes; work targeted to proper position; divisional best practices are shared and used.

**Level 5 (Optimising)** – COE/Enterprise has a reputation for innovative policy development tools and procedures, gives presentations on lessons learned.

## Process Area 4: Staff Training

(no equivalent in IM framework)

### Capability Development – Leveraging the Basics

**Level 1 (Initial)** – No awareness of requirements among staff

**Level 2 (Repeatable)** – Minimal awareness, limited training resources, training provided on request, roster of trainers developed

**Level 3 (Defined)** – Mandatory manager and staff training in basics, training included in performance contracts, corporate orientation for new staff

**Level 4 (Managed)** – training statistics collected and monitored by Senior Management Team, certificates issued to signify levels of expertise

**Level 5 (Optimising)** – innovative training tools are developed by COE. Enterprise tools are requested by other jurisdictions for adaptation, Enterprise receives awards for training innovations.

## Process Area 5: Fully Embedded Divisional Resources / Governance

(No corresponding category in IM Framework)

### Capability Development – Leveraging the Basics

**Level 1 (Initial)** – no resources in divisions having knowledge/awareness of divisional responsibilities

**Level 2 (Repeatable)** – Divisional experiences in privacy compliance/FOI/IM are documented and accessible; compliance with governance requirements is spotty at best.

**Level 3 (Defined)** – divisions have defined policies and practices for their program, divisional coordinators are established, full charge-back is in place for COE Access and Privacy processes, eg PIAs. Most units comply with governance requirements, but not all.

**Level 4 (Managed)** – divisional resources pro-actively collaborate with COE and other corporate areas, eg. on risk management. Divisions monitor and track for reporting to corporate governance committees, capacity for delegated/independent decision-making.

**Level 5 (Optimising)** – divisional innovations are recognized and promoted across the Enterprise, horizontal collaboration, staff are mobile

# Process Area 6: Functionally Joined Up Across the City

## Capability Development – Leveraging the Basics

**Level 1 (Initial)** – silos, no enterprise wide coordination

**Level 2 (Repeatable)** – minimal or implicit linkage to business strategies or business drivers, Enterprise in constant crisis mode, forced collaboration, identification of barriers

**Level 3 (Defined)** – Explicit linkage to business strategies or drivers, planned responses to issues, Access and Privacy Coordinating Committee established, barriers removed, recognition of roles and responsibilities and willingness to collaborate.

**Level 4 (Managed)** – Capital planning and investment based on performance and feedback received and lessons learned (eg. on privacy breaches, ability to produce records), Senior Management Team understands numbers don't tell the whole story.

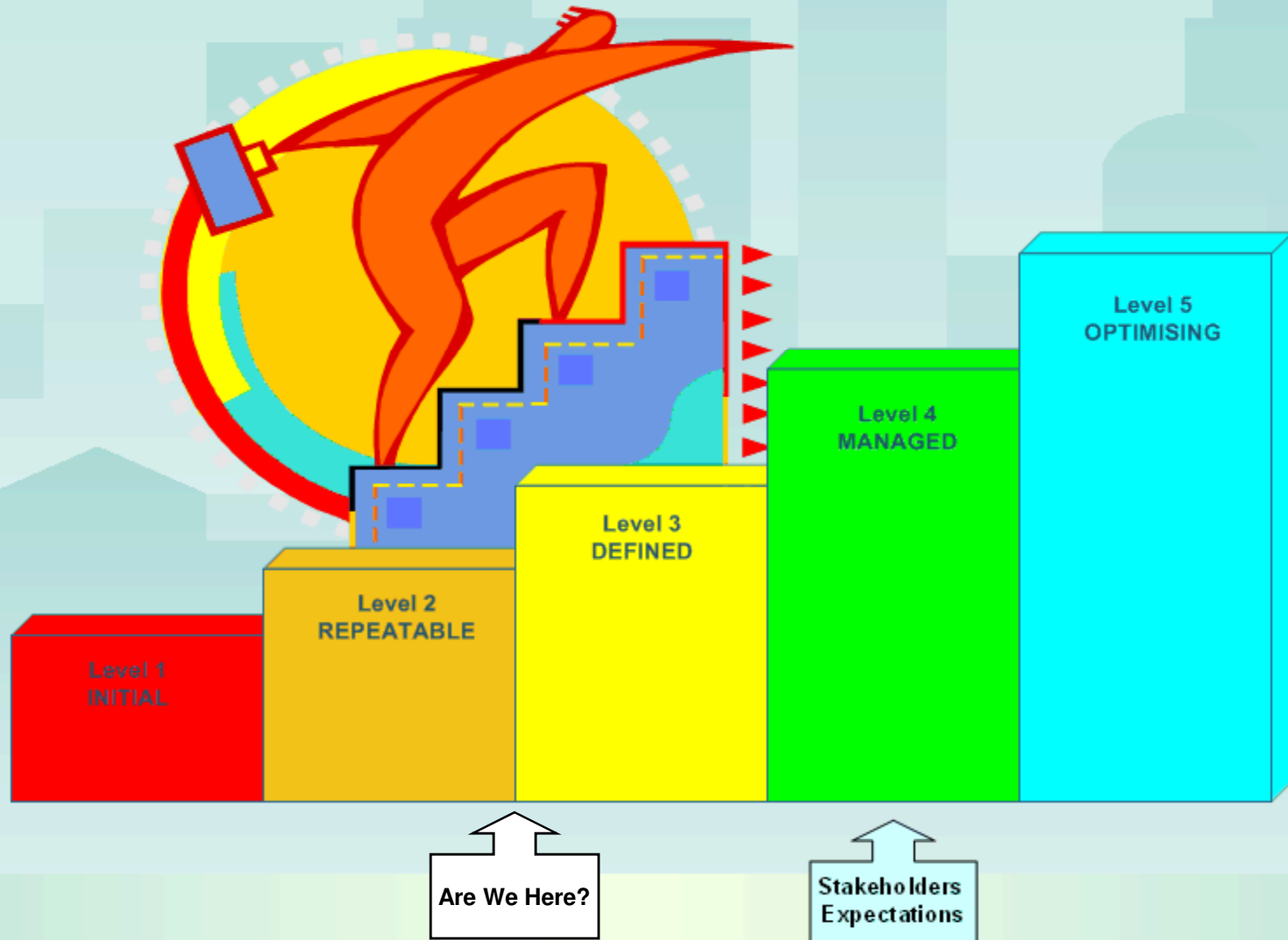
**Level 5 (Optimising)** – Leveraging for corporate benefit. Metrics are used to optimize and drive business linkages. Business involved in the continuous improvement of corporate policies and procedures. Divisional coordinators present their successes to colleagues.

# Determining Organizational Maturity Level

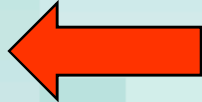
- The extent to which an organization displays the attributes noted in the AP-CMM determines the process maturity level rating of the organization.
- The extent of implementation of a specific attribute is evaluated by assessing:
  - **Commitment** to perform (leadership and policies)
  - **Ability** to perform (resources and training)
  - **Activities** performed (plans and procedures)
  - **Measurement** and analysis (measures and status)
  - **Verification** of implementation (oversight and quality assurance)

# Privacy Maturity Model – Where Are We Today?























Tuesday, October 23, 2007




# Three reasons to map

- To evaluate
  - What we do (practices)
  - Where we want to go (goals) 
  - How to make the change (process improvement)

# Example – Performance Measures on Access and Privacy Compliance

	Level 1 – Initial/ Ad hoc	Level 2 – Repeatable Processes	Level 3 – Defined Processes	Level 4 – Managed 100% Compliance	Level 5 - Optimising
Senior Management Commitment	Partial 	Significant 	Substantial 	Full 	Full 
Full CAP Resources in place	No	Partial 	Yes 	Yes 	Yes 
Policies and Procedures	No	Minimal 	Partial 	Yes 	Yes 
All Staff Trained	No	Minimal 	Partial 	Substantial 	Yes 
Fully Embedded Divisional Resources	No	No	Minimal 	Partial 	Yes 
Functionally Joined Up Across the City	No	No	Minimal	Partial 	Yes 

 Represents discrete activities building on previous levels

# Example – Performance Measures (Management Dashboard)

- **Level 1** – Management directs establishment of performance measures
- **Level 2** (repeatable processes)
  - A) Management chooses what will be measured.
  - B) CAP develops basic reporting processes and measurement capacity. CAP delivers services that drive performance.
  - C) CAP gathers information to set performance levels (standards)
  - D) Divisional staff receive training, participate in FOI and Privacy compliance activities
- **Level 3** (defined processes)
  - A) City Manager, Division Heads agree on Performance Measures and follow-up responses
  - B) CAP has established capacity to support Performance Measurement
  - C) CAP targets services to areas that are most in need.
  - D) CAP and divisions establish self-reporting mechanisms, monitored by CAP.
  - E) Most divisions are responsive to performance measurement standards
- **Level 4**
  - A) Governance committees routinely review performance measures in setting targets, approving projects, assigning resources and directing follow-up.
  - B) CAP refines performance measures based on knowledge gained from level 2 and 3
  - C) CAP services are reviewed for effectiveness and opportunities for enhancement
  - D) Only new staff in Divisions require training and development
  - E) Divisional staff are aware of other divisions performance; peer pressure.
- **Level 5**
  - A) Senior management can't imagine working without performance measures
  - B) CAP standards and services are exportable
  - C) Policies and procedures are comprehensive and mature
  - D) Training requirements are easily identified and specific
  - E) Divisions perform their access and privacy responsibilities largely without assistance

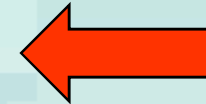
# Thoughts on process improvements

Should we:

- Focus on implementing process improvements **project by project** (rather than across the organization by Maturity Level)?
- Focus on delivering **value to...whom?** (the best value is at the higher maturities)
- Use our proven methods in areas with a **large “footprint”?** Or target **small projects** first (pilots)?
- Check progress how **often?**
- How **quickly** should we (can we) move up a level?

# Three reasons to map

- To evaluate
  - What we do (practices)
  - Where we want to go (goals)
  - How to make the change (process improvement)



# Process Improvements - Barriers to Overcome

- None to Initial (0 to 1)
- Initial to Repeatable (1 to 2)
- Repeatable to Defined (2 to 3)
- Defined to Managed (3 to 4)
- Managed to Optimizing (4 to 5)

# Level 0 to 1 – None to Ad Hoc

- Develop and implement a **legislative or policy impetus** for providing a right of access to information to external parties and the protection of personal information in the custody and control of the organization
- Define **who** will be held accountable for compliance
- Determine a **timeframe** for implementation of the legislation/policy

# Level 1 to 2 – Initial to Repeatable

- Clearly define the **objectives**
- **Get advice** and guidance from recognized experts
- Identify specific **personnel**
- Ensure adequate **training** and support
- Undertake **awareness** briefings
- Nominate senior management **sponsor**
- Publicize and celebrate **successes**.
- Plan for the long-term, including costs
- Produce draft **risk procedures** with templates for key inputs and outputs
- Identify and use appropriate risk management **tools**

# Level 2 to 3 – Repeatable to Defined

- Reinforce and **strengthen** corporate backing
- Provide **formal training** to develop in-house expertise
- Allocate adequate **resources**
- Select **key projects**
- Publicize **successes**, encouraging wider application of best practices
- **Formalize** the chosen principles and methodologies
- **Insist** that project managers use the appropriate tools and procedures as part of their routine management of projects and business processes.
- Start to assemble **metrics**.

# Level 3 to 4 – Defined to Managed

- Learn from experience. Undertake regular reviews.
- **Amend and strengthen** processes.
- Investigate novel applications
- Use every possible means to embed “**Open Data**” and “**Privacy by Design**” principles in the organization’s culture.
- **Ensure that risk is included as a routine criterion in all decision-making.**
- Identify and **counter** incidences of “risk fatigue”
- Undertake regular risk **management training**
- Consider use of external expertise to re-invigorate staff.

# Level 4 to 5 – Managed to Optimising

- Change the **sponsor** from time to time
- Use **audit** and review techniques
- Take full advantage of the competitive **edge**
- **Extend** beyond the usual applications
- Continually **invest** in improvements
- Continue to involve stakeholders and **partners** in the process improvements

# Thoughts on moving up levels

- **Senior management needs to understand moving up means adding more permanent resources**
  - **Need to maintain core process resources while moving up levels.**
  - **Only when capability basics are super-strong can project implementation resources be re-assigned. Cutting core process resources means instant slippage.**
- **Document, document, document.**
- **Cutting corners is counter-productive in the long-run.**
- **Benefits of training fade, need to continually re-train.**
- **Internal information-sharing, coordination is essential.**

# Additional reading (see speaking notes for comments)

1. **Treasury Board of Canada Secretariat Integrated Risk Management Framework:** <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12254>
2. **Organizational Maturity in Business Risk Management, The IACCM Business Risk Maturity Model** <http://www.risk-doctor.com/pdf-files/brm1202.pdf>
3. **Risk Management Maturity Level Development** (April 2002)  
<https://acc.dau.mil/CommunityBrowser.aspx?id=17748>
4. **Do's and Don'ts of Enterprise Risk Management** (March 13, 2006)  
[http://www.logicmanager.com/contents/knowledge\\_center/dos\\_and\\_donts/index.php](http://www.logicmanager.com/contents/knowledge_center/dos_and_donts/index.php)
5. **Article: Capability Maturity Model (RM-CMM) for Risk Management**  
[http://ieeexplore.ieee.org/xpl/freeabs\\_all.jsp?arnumber=1407492](http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1407492)
6. **SEI-CMMI Maturity Profiles:**  
<http://www.sei.cmu.edu/appraisal-program/profile/>
7. **Building a Culture of Privacy**, Robin Gould-Soil and Sandra Smith-Frampton, PIPA conference 2008  
<http://www.verney.ca/pipa2008/presentations/734.pdf>