The Compliance and Audit Program

Promoting effective information management

Privacy, Compliance and Training
Corporate Information and Records Management Office

BRITISH COLUMBIA
The Best Place on Earth

Ministry of Finance

February 2017

Trusted financial and economic leadership for a prosperous province

Presentation Team

Privacy Compliance and Training Branch, Ministry of Finance:

Brent Grover, Senior Auditor

Teresa Woods, Senior Auditor

Deloitte:

Rob Witcher, Senior Manager, Cyber Security

Today's agenda

- What is the Information Management Compliance and Audit Program?
- Why is it important?
- How did we develop the criteria?
- How will we test?
- How did we decide on the maturity levels?
- Interactive case studies ☺

What *is* Information?

“Information is an asset that must be managed, shared and used in a way that demonstrates its value and importance”.

So what *IS* information management?

There are many aspects of Information Management but our current focus is “the series of processes and systems we use to manage the collection, use, flow, storage and disposal of information”

Some of us are really good at this, others less so, but almost ***every*** organization does some things well ☺

Thank you for the good work you’re already doing

The idea is continuous improvement

Why does it matter?

Managing information is critical for good government.

- foundation of effective analysis and policy making
- evidence to support decision making
- critical enabler of efficiency
- supports accountability through publications, audit, parliamentary scrutiny, freedom of information and open public records.

Information is one of the core assets of government. Like other assets, it needs to be managed well if we are to get best value from it.

Excerpted from 'Better Information for Better Government', UK Cabinet Office, Jan 18, 2017

However…

Organizations still struggle with managing information.

Moving to the Future

- Auditing privacy compliance has been under development since 2014
- In September 2015 Government announced that there would be a cross-government review of privacy protection policies and procedures to ensure that they are as robust as possible.

- Recommendations made by the Office of the Information and Privacy Commissioner regarding record retention and disposal practices. (F15-03, Loukadelis Report)

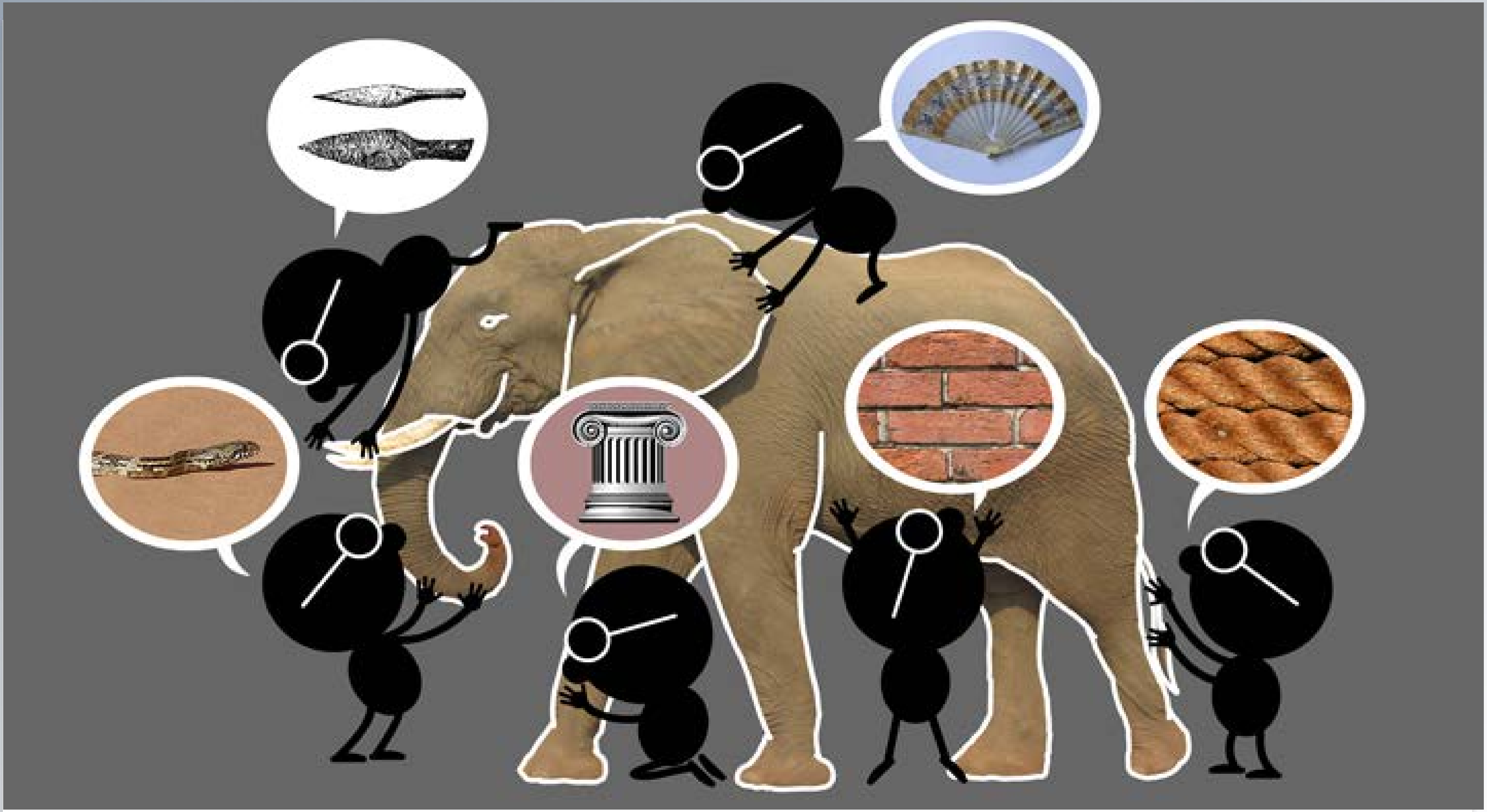
Introduction of the *Information Management Act* (May 2016) and the mandate of the Chief Records Officer

Information Management Life Cycle

Information Management concerns a cycle of organisational activity:

- authorized **creation/acquisition** and **retention** of information from one or more sources,
- **Custodianship** and the **disclosure** of that information to those who need it, and are authorized to access it; and
- **disposition** through **archiving** or **destruction**.

But are we managing information effectively?



Chief Records Officer

The mandate of the Chief Records Officer is:

(a) to promote the preservation of valuable government information for current and future use,
(b) to approve information schedules governing the holding, transferring, archiving and disposal of government information,
(c) to manage the digital archives and promote its availability to the public, and
(d) to promote effective **information management** by government bodies.

s. 3, *Information Management Act*

Compliance and Audit Program

- Our mandate is to assess Information Management practices in four areas/domains:
  - Privacy;
  - Records Management;
  - Information Access; and,
  - Information Protection.

Privacy

Privacy relates to Personal Information (PI):

- Limiting collection, use and disclosure of Personal Information
- Ability to correct your own Personal Information
- Responsibility for accuracy of PI retained
- Reasonable protection and storage of PI

Records Management

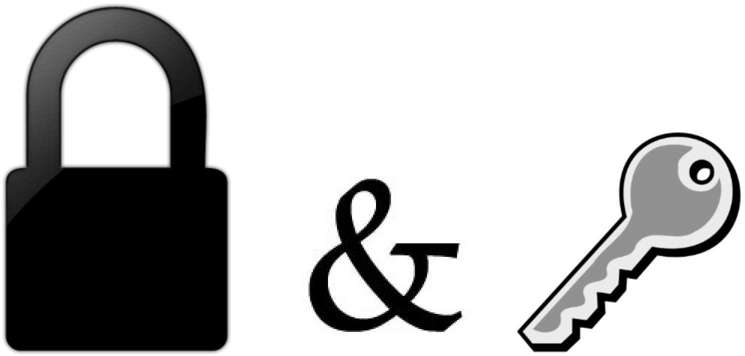
- The systems and processes used to systematically control the creation, distribution, use, maintenance, and disposition of recorded information
- Our collective responsibility to save all necessary information in a recordkeeping system
- Please work hard to avoid saving transitory records. It’s unnecessary and expensive ☺

Information Access

- Fulfilling our obligations under FOIPPA
- Responding to FOI requests
- 10,000 requests a year!
- We must respond ASAP

Information Protection

- Information assets and systems
- Protection against malicious code
- Access control and monitoring
- Business continuity



Continuous Improvement

- Our part is to help create a culture of continuous improvement in the Information Management practices of Ministries
- Collaborate, communicate, assist, and assess

Because *this* is unsustainable

Organizations

CONTINUING

to struggle with managing information.

Do your part

Like Smokey the Bear always said,

“Do your part”

Now we’ll do OUR part

- We’ve created and will utilize a Framework by which we can assess processes

The goal

- Our goal is to assess how well Ministries are doing with their Information Management processes
- This led to the development of testable criteria across 4 domains - Privacy, Records Management, Information Access and Information Protection

Our Approach

- Initial or baseline audits will examine the current state of compliance to create a ‘benchmark’
- The benchmark assessment is intended to be constructive, not punitive
- Self assessments – where Ministries regularly review their progress to enable continuous improvement
- Focused – a review of a specific area or specific risk

The dream outcome?

COMPLIANCE that adds VALUE!!

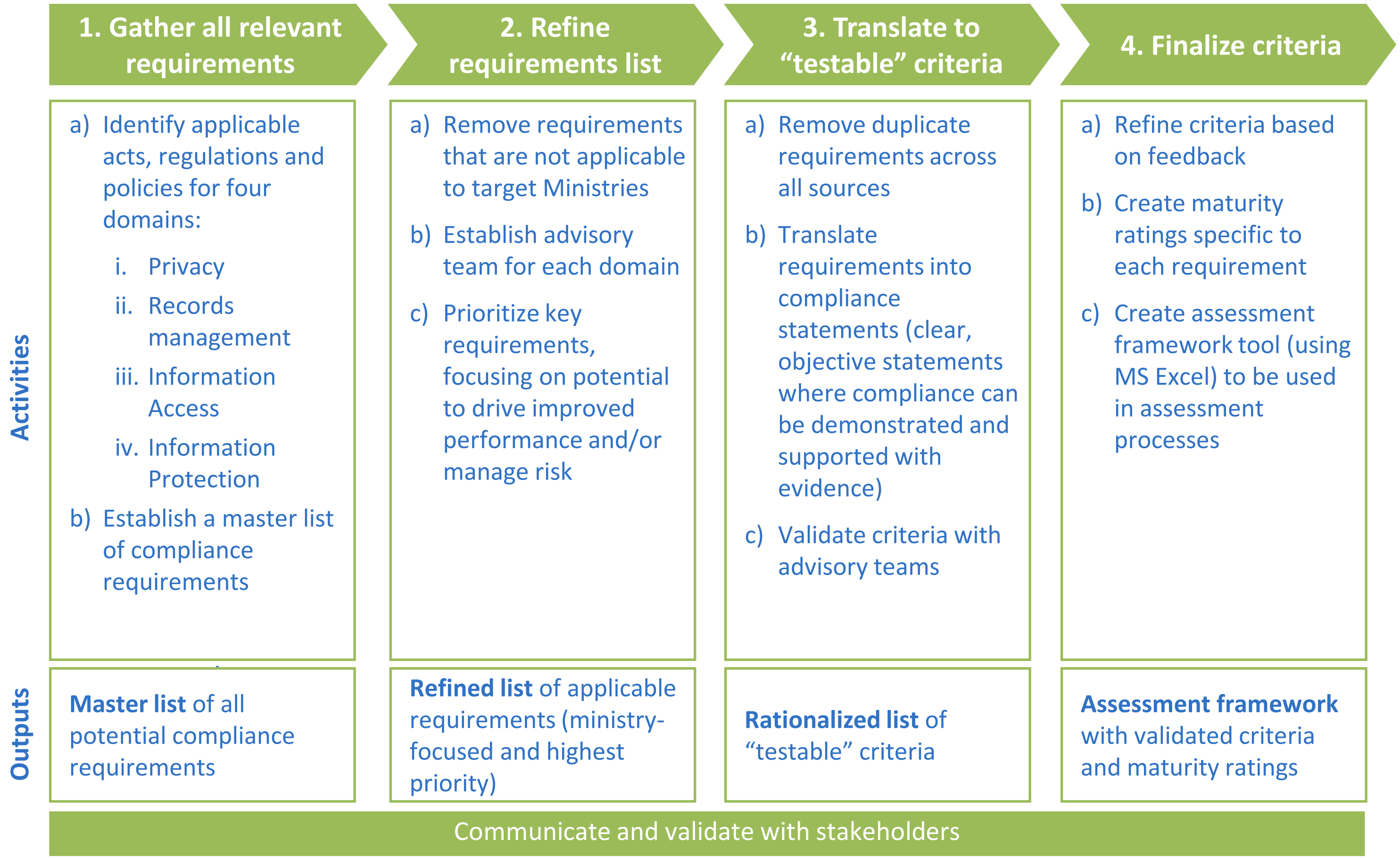
- Better decisions
- Service delivery optimized
- Records of value preserved
- Information is findable
- Information access within time limits
- Information secure
- Information accessed and shared as authorized

Development of the framework: Guiding Principles

- **Risk-based** – focus on priority compliance areas without creating an overly complex “check-box” exercise
- **Measurable** – Focus on establishing a baseline of current performance and supporting continual improvement over time
- **Objective** – utilize a clearly-defined maturity scale to enable objective assessment, consistency and comparability (over time and across organizations)
- **Efficient/Practical** – Create a framework that supports efficient assessments and enables Ministries to focus on high-priority requirements
- **Integrated** – recognizing linkage between Records Management, Privacy, Information Access and Information Protection, seek to integrate requirements and encourage interrelationships where possible

Development of Assessment Criteria

- **Objective:** Translate **400+** compliance requirements into a comprehensive but practical compliance program (targeting 50-70 criteria)



	1. Gather all relevant requirements	2. Refine requirements list	3. Translate to “testable” criteria	4. Finalize criteria
Activities	a) Identify applicable acts, regulations and policies for four domains: i. Privacy ii. Records management iii. Information Access iv. Information Protection b) Establish a master list of compliance requirements	a) Remove requirements that are not applicable to target Ministries b) Establish advisory team for each domain c) Prioritize key requirements, focusing on potential to drive improved performance and/or manage risk	a) Remove duplicate requirements across all sources b) Translate requirements into compliance statements (clear, objective statements where compliance can be demonstrated and supported with evidence) c) Validate criteria with advisory teams	a) Refine criteria based on feedback b) Create maturity ratings specific to each requirement c) Create assessment framework tool (using MS Excel) to be used in assessment processes
Outputs	**Master list** of all potential compliance requirements	**Refined list** of applicable requirements (ministry-focused and highest priority)	**Rationalized list** of “testable” criteria	**Assessment framework** with validated criteria and maturity ratings

Communicate and validate with stakeholders

Overview by domain

Domain	# of criteria	Sources (examples)	Additional notes
Privacy	23	• FOIPPA • PMAP • Core Policy	• Focuses on processes and capabilities that enable strong privacy performance
Records Management	15	• IMA • RIM • Core Policy	• Focuses on processes and capabilities that enable strong records management practices • Recognizes central role of effective records management
Information Access	7	• FOIPPA	• Focus on processes and capabilities that enable effective FOI processes • Does not duplicate OIPC audits of FOI performance/compliance
Information Protection	15	• ISP • Core Policy	• Developed in consultation with MTICS • Leverages outputs of AISR to highlight areas for additional follow up where appropriate

Maturity scale

- Supports measurable, objective and consistent assessment
- Specific maturity ratings developed for each criterion
- In general, the target is to have a defined, documented, repeatable process that is being used (i.e., Level “3” vs. Level “5”)
- Higher ratings are used to highlight exceptional practices that can be shared with other Ministries
- Looking to see improvement over time

Overview of maturity levels

Initial	• No recognizable process in place. • Activities are ad-hoc where they exist.
Repeatable	• No formal policy, process or related documentation • Informal process in place that is inconsistently delivered
Defined	• Formal documentation in place and processes are standardized • No formal monitoring of performance • No regular updates
Managed	• Compliance is monitored and measured and actions are taken where issues are identified • Practices are regularly reviewed and improved
Optimized	• Maturity Level 4 has been met and additional leading practices are demonstrated • Designed to highlight and recognize good practice and support sharing of good practice where appropriate

How does it work?

- So now we’ve covered the “WHY?” of effective Information Management, we of course will discuss ‘How?”
- We will assess or *audit* existing processes for compliance to our framework

Pre-Audit Planning

- Scope
- Create and agree the terms of the engagement (Terms of Reference)
- Collect and review all relevant documentation
- Establish contact persons for interviews

Audit Processes

Typically, auditors:

- Identify RISKS and consider IMPACT
- Determine representative CRITERIA against which to test
- Determine CONTROLS that mitigate the risk
- TEST the controls
- EVALUATE the controls
- DEVELOP recommendations to reduce risk/improve controls

Scenario 1

- RISK: Theft from a home.
- SITUATION: Owner has a rare book collection valued 5 years ago at $45,000.
- Factors that affect the degree of risk
- Factors affecting the degree of impact

Criteria/Controls

- Deadbolts on doors and windows
- Books are kept in a walk in safe
- 24/7 alarm system with 3 minute response time
- Security guards
- Replacement insurance with current appraisals
- Big dog ☺

Test the Controls

- Check doors and windows. Test locks
- Ask to be shown the safe
- Test security system, follow up
- If there are security guards, examine service contract
- Ask to review insurance policy
- Check for doghouse/dog dish ☺

Testing Results

- Deadbolts doors, and ground floor windows
- No safe: Actually a large locked crate in the attic
- Security system – only activated if owner is out of town
- No security guards
- Has insurance, no replacement value
- No dog - Small cat ☺

Controls Assessment

- On a scale of 1 – 5, how effective are these controls?
- 1 - ineffective
- 2 - somewhat effective
- 3 – satisfactory
- 4 – good
- 5 - robust

Is this good enough?

Control	Effectiveness
Deadbolts doors, and ground floor windows	4
No safe: Actually a large locked crate in the attic	3
Security system – only activated if owner is out of town	2
No security guards	1
Has insurance, no replacement value	2
No dog - Small cat ☺	1

We don’t think so

- With the exception of the deadbolts on doors and ground floor windows, we do not feel the controls are adequate
- Overall average: 2.2/5
- Recommendations are strongly suggested

What we thought

T= Test R=Recommendation

T: Deadbolts? R: None – this is fine

T: Crate? R: better lock, place in closed cupboard

Sec System? R: upgrade to 24/7 with 3 min response

Guards? R: hired during the owner's absence

Insurance? R: new appraisals, add replacement

Dog? R: keep the cat ☺

Two high priority items

Upgrade the security system

- Implementing this one recommendation will almost completely mitigate the risk of theft. (but there will always be some residual or leftover risk)

Update insurance policy

- Replacement insurance at current values will effectively *transfer* the remaining risk

New maturity level

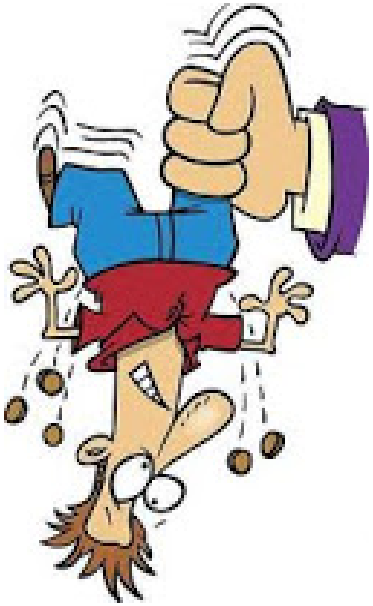
- By implementing the 2 high priority recommendations, we would now consider this risk to be well mitigated and would likely move the overall ranking to 4 – which is very good
- The possible addition of hiring guards during the owner's absences would push the ranking to a 5

Spend your time and money wisely

It’s important to note that although we made several recommendations………

- Implementing 2 of them will get the job done.
- **‘highest risk’**
- **‘Low hanging fruit’**
- **‘Biggest bang for the buck′**

TOO BUSY



Same process – different subject

- Risk
- Criteria
- Testing
- Evaluation
- Assignment of rankings
- Recommendations

The only difference is now we will use the example of COMPLIANCE

How much work will this be for Ministries?

Less than you think☺

One of the more difficult processes in an audit is CORRECT RISK IDENTIFICATION

And here is the really good news for Ministries:

You don’t have to identify the risks –

WE’VE DONE IT FOR YOU

And the risks led to the development of the criteria☺

Scenario 2 - Training

- We will assess performance at a fictitious Ministry for one of the criteria related to Training

- The following slides:
  - Outline the steps the PCT team will take prior to meeting with the Ministry
  - Provide a description of the current state at the Ministry
  - Walk through the evaluation process to arrive at a maturity rating

Example Criteria

Employee Training

Records Management training requirements are identified for all employees based on their roles.

Employees have completed training related to records management (e.g. "Managing our information assets" and/or "Managing government records").

Individuals have received additional, role-specific records management training where appropriate.

How will we test?

Prior to assessment

- PCT Team to review training statistics for Ministry to assess mandatory training completion rates and any additional training statistics
- Request and review Ministry documentation related to training and awareness activities (procedures, training materials, links, etc.)

During assessment

- Walk through training-related processes with Ministry representative. Examples include:
  - Onboarding
  - role changes
  - monitoring of training completion
  - identification of role-specific training requirements
  - awareness-related processes
- Request examples of any additional training related materials
- Ask for feedback regarding overall training program effectiveness, including strengths and gaps/challenges

Observations during the audit

- Prior to visiting the Ministry: mandatory training completion rate is 90%
- At the Ministry:
  - There is a process in place to monitor and follow up on mandatory training
  - Requirements for role-specific training have been identified and role-specific training has been provided
  - Evidence of “awareness”-related activities is observed (posters, monthly emails, meeting minutes, etc.)

Example Criteria Maturity Ranking

Employee Training - Maturity Rankings

1-Initial	2-Repeatable	3-Defined	4-Managed	5-Optimized
No formal records management training requirements have been identified or documented for Ministry employees. Training has not been completed by individuals as. required	Formal training requirements have not been defined, but some employees have received basic training. .	Training requirements are defined for employees. This includes mandatory government-wide training as well as role or ministry specific training. All Ministry employees receive mandatory training when they are hired, and all existing employees have received mandatory training.	"A ministry-wide records management awareness program exists (beyond basic training requirements) and there is a process for follow up where training or awareness gaps exist. Training is augmented by regular awareness activities (emails, posters, presentations, etc.).	Level 4 has been attained and the Ministry has demonstrated additional leading practices for this criterion.

Scenario 3 – Year Round Fun Camps

Provincially funded Association’s mandate is “Fun for Everyone”

Fun, open and sharing culture

- No secrets kept at camp ☺, trust is granted readily, staff is hired for their athletic and handicraft skills
- Passwords are all the same – it saves time
- Camp and office staff trade jobs during the summer

Privacy, please

- Information retained in journals might be personal, medical or financial including banking information
- The head office manager routinely sends personal and confidential information by email

Records management….or not

- Records have been kept in journals maintained by individual staff members, who exercise judgment about what is kept.
- Journals are not protected in any way
- They are sent by mail to head office
- Stored in a coat closet

Information Access

- When athletic staff is working in head office, no filing is done and FOI requests are ignored
- No one has been trained to respond to FOI requests

Information Protection

- Camp passwords are shared and doors are not locked
- Journals contain sensitive and confidential information.
- Every Friday, the journals are deposited in a basket on the front counter at each camp

PROTECTION
CONSEIL CANADIEN POUR LES RÉFUGIÉS
CANADIAN COUNCIL FOR REFUGEES

Trouble ahead

- A journal containing full banking information of a powerful BC politician was found on the deck of the Saltspring Ferry;
- A parent has requested verification of her child’s attendance at the camp in Tofino as she had paid in full for a 3 week camp and has heard that her daughter in fact never left her father’s home Vancouver and finally,
- A precocious 13 year old has entered the unlocked medical hut, taken photos of prescriptions used by other campers and posted them on Facebook.

What risks can you identify?

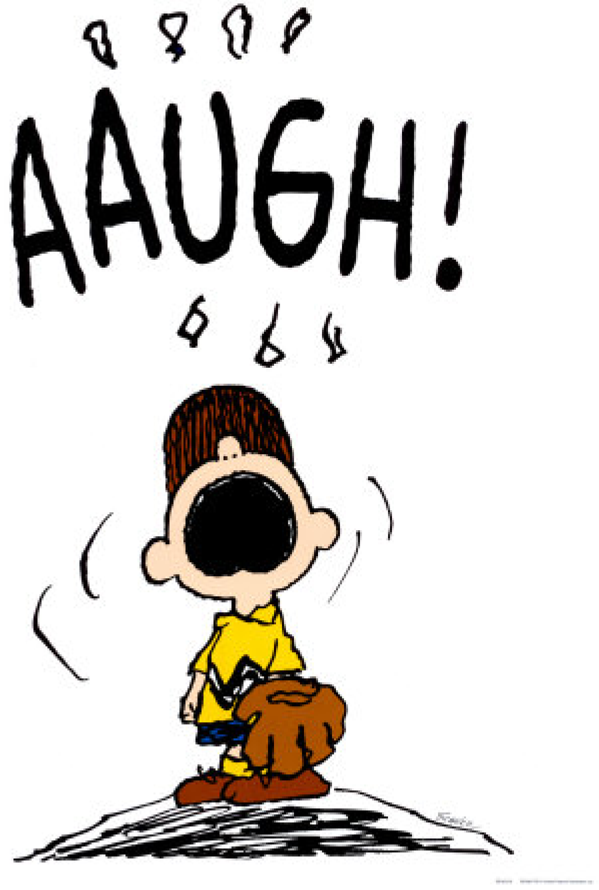
So many risks!

- Information breach
- Personal information in the public domain
- Violation of policies (FOIPPA, AUP, CPPM Ch12)
- Lawsuits
- Job loss

Yes, even more risks

- **Harms to reputation (clients and association)**
- **Inability to access records for business purposes**
- **Inability to respond promptly to FOI requests**
- **Risk of identity theft, fraud**
- **What else?**

It had to happen



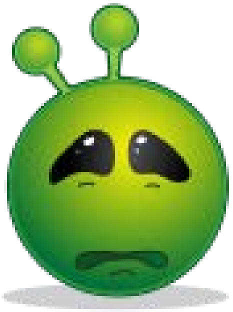
We’d better have a look

- Refer to the synopsis
- Review the criteria
- Review the observations made
- How would you rank compliance to the criteria?

Privacy

• There is a process in place to ensure that PIAs are completed :	1
• There is a process in place to monitor Service Provider compliance :	1
• Information incidents are reported immediately:	1
• Mandatory training	2 – 3

AVERAGE: 1.1



Records management

• Training:	2
• Classification:	1
• Retention schedule:	2
• Personal Info:	1
• Physical Records:	2
• Disposition:	1

AVERAGE: 1.6

Information Access

There is a specific training course on Access:	1
Designated information access officer:	1
Searches for responsive records are conducted thoroughly:	1
There is a process to respond to FOI requests:	1
Staff is aware of the responsibilities related to ‘Duty of Care’:	1

AVERAGE: 1

EPIC FAIL

Information Protection

- Mandatory training: 2
- Relevance of training content: 1
- Training content is current: 1
- Training is tracked: 1
- Employee awareness: 2

Info Protection cont’d

- Preventing individuals from accessing others’ personal or sensitive information 1
- Limiting access 2

AVERAGE: 1.5

Scorecard

Privacy:	1.1
Records Management :	1.7
Information Access:	1.0
Information Protection:	1.5

Recommendations

- Lots of material here for improvements!
- Are these issues localized or systemic?
- Recommendations can be general or specific; some risks should be addressed right away
- Where should we start?

Audit recommendations

- We can see that the controls – criteria, policies, procedures, training and practices – are not working

- Several risks exist in this organization, so we have to **determine which ones matter the most and recommend accordingly**

Remember:

- ***Highest risk***

- ***Biggest bang for the buck***

- ***Low hanging fruit***

For immediate action

What is the most urgent problem to be addressed? If not already done....

- Report and attempt to contain the breaches!

As soon as humanly possible

Appoint a manager for the camps who will enforce:

Use of unique passwords

Locked storage at end of day for all records

Review of all emails before deletion

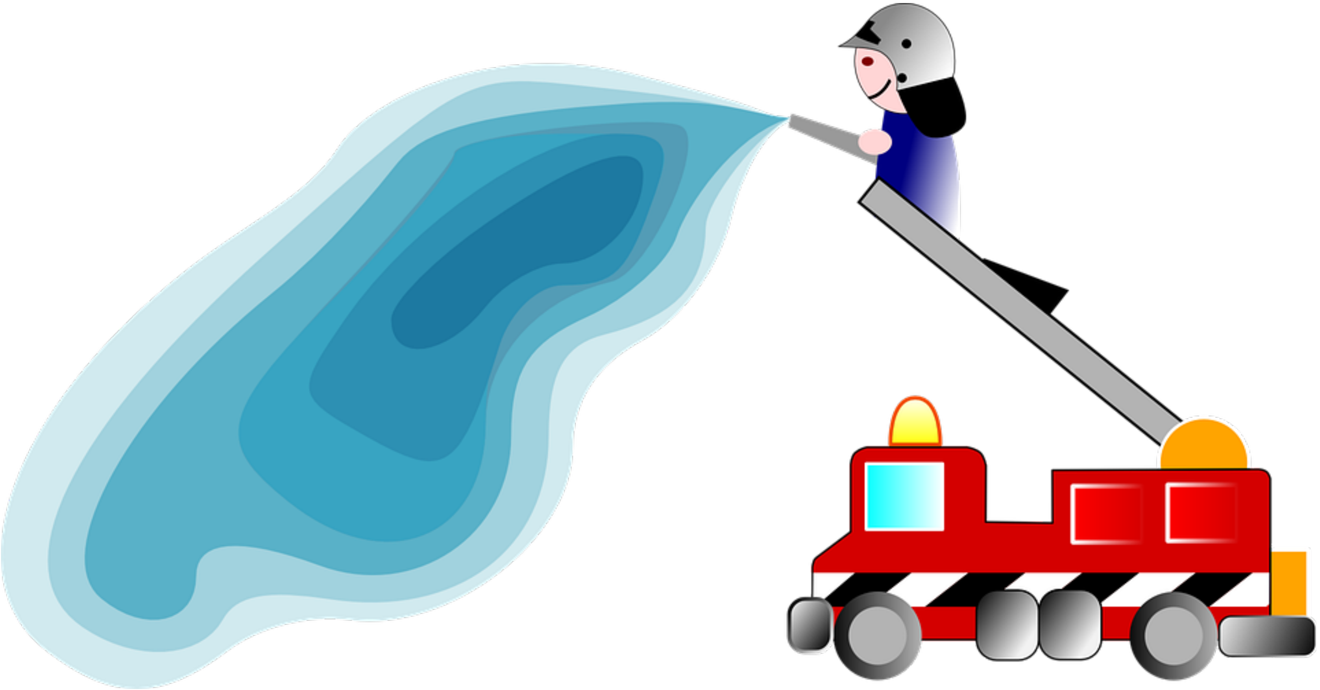
Using the computer systems for creation, protection and usage of information

The end of the handwritten journal era☺

Meanwhile, back at head office

- Stop emailing sensitive information to open computers at the camps
- Rename the paper files and store them in a locked area away from the door
- Implement the correct process for responding to FOI requests
- Stop letting swimming instructors work in head office – seriously.

Damage Control



- OK… the biggest fires are out. What’s next?

Medium term recommendations

- Manage training – all aspects
- Establish some firm processes that can be repeated
- Hire a shredding company

Medium- longer term

- Regularly review and follow relevant policies
- Monitor migration to new system
- Develop PIAs in accordance with requirements
- Review and amend off site security arrangements
- Establish proper records management processes, including scheduling and destruction

That wasn’t so bad, was it?

- Simple changes
- Low cost, practical actions
- Education, awareness, discipline and a desire to do better
- WELL WORTH IT ☺

To sum up……

- The Information Management Compliance and Audit Program and:
- Why it's important
- How we developed the criteria
- How we will test
- How we decided on the maturity levels
- How you applied the information presented ☺

Big takeaways

- Information is valuable, and it’s up to all of us to protect it, use it with care, store it properly and retrieve it efficiently
- Good records management underpins good practice in all the domains
- Think about what you are doing with information

What we hope to achieve

- From 400+ criteria down to only 60……

  You’re welcome ☺

- Robust approach designed to minimize disruptions to your routine and maximize our ability to assess your various levels of compliance
- PCT’s goal is to inform, guide, assist and assess
- Our collective goal is to improve our practices around Information Management

Outcomes

- By applying this framework to your own unique set of policies, procedures and processes, we hope to build a clear picture of your present successes and good practices

- We know and understand your big two constraints: TIME AND MONEY so our recommendations will be as practicable as possible

- Thank you for all your good work to date and for your attention here today ☺

Next steps

- Schedule of reviews
- How-to Guidelines for Ministries – how to prepare
- Regular communications
- Feedback

Questions?

Please contact us with your questions – we'll help.

Telephone: 250 356 1851

Email: privacy.helpline@gov.bc.ca

Thank you!