Integrating the Principles

Information Management – Access and Privacy

Monday, April 20, 2015 Nanaimo, BC

Julie Luckevich, MLIS, CIAPP-P
Eclaire Solutions Inc

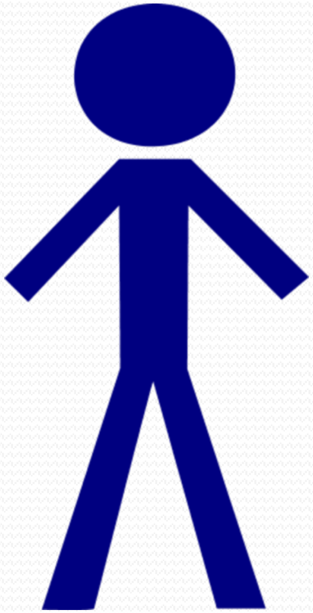
Introduction

- Today’s theme: Bridging Privacy, Information Governance and Records Management
- Part I: Comparing the concepts of Information Management (IM) and Privacy
- Part II: Using the Maturity Models (2 case studies)
- Recap / Questions

Part 1 IM and Privacy

Information Management

Access and Privacy



How did we get here?

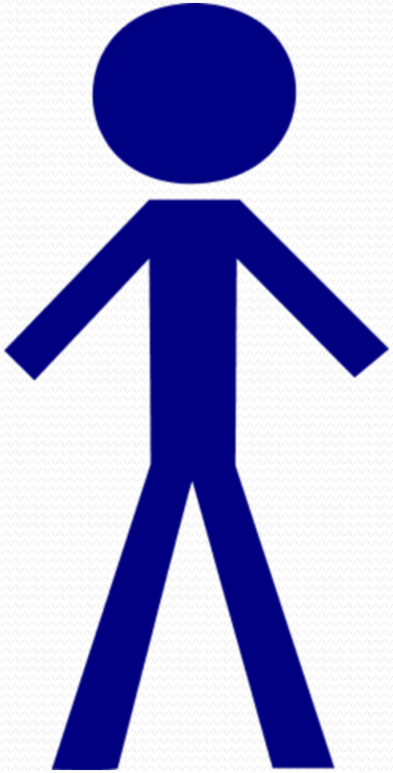
Information Management

- General Services Administration (USA) (1950s)
- ARMA's Generally Accepted Recordkeeping Principles®, the Principles (formerly GARP)
- 8 Principles
- Uses Information Governance Maturity Model (IGMM) (c2009)

Privacy

- OECD Guidelines (late 70s)
- CSA's Privacy Principles, the "Model Code" (early 90s)
- AICPA/CICA Generally Accepted Privacy Principles (GAPP)
- 10 Principles
- Uses the CICA Privacy Maturity Model (c2007)

Access and Privacy



Program Focus

- Internal and external
- Policies, procedures
- Privacy Culture
- FOI Process
- Auditing /Compliance
- Privacy Impact Assessments
- Preventing breaches

Information Management

Program Focus

- Internal only
- Policies, procedures
- Findability throughout life cycle
- User acceptance
- Class. and Retention
- Auditing /Compliance
- Archiving

IM vs. Privacy

In common

- Program management (policies and procedures)
- Accountability
- Availability / Access
- Compliance
- Retention and Disposition / Limiting retention
- Accuracy and Integrity
- Protection / Safeguards
- Transparency / Openness

Unique to Privacy

- Consent / Withdrawing consent
- Identifying the purposes for collection
- Limiting collection

Recordkeeping and Privacy: How they compare

Principle	the Principles (ARMA)	CSA Model Privacy Code
1. Accountability	☑	☑ Focus on Personal Information
8. Transparency / Openness	☑ Documentation available	☑ More proactive - available to public

Recordkeeping and Privacy: How they compare

Principle	the Principles (ARMA)	CSA Model Privacy Code
2. Identifying purposes for collection		☑ Core Privacy Concept
3. Consent / Withdrawal of consent		☑ Core Privacy Concept
4. Limiting collection		☑ Core Privacy Concept

Recordkeeping and Privacy: How they compare

Principle	the Principles (ARMA)	CSA Model Privacy Code
5. **Use** / Limiting use, disclosure and retention of personal information	☑ Valid business use	☑ Use limited to purpose; limited disclosure
5. **Retention** / Limiting use, disclosure and retention of personal information	☑ Retention Based on 4 values	☑ Limiting retention Varies - only as long as needed, or +/- 1 year
5. **Disposition** / Limiting use, disclosure of personal information	☑ Disposition Secure destruction	☑ Limiting retention, or anonymizing

Recordkeeping and Privacy: How they compare

Principle	the Principles (ARMA)	CSA Model Privacy Code
6. Integrity / Accuracy	☑ Integrity	☑ Accuracy
7. Protection / Safeguards	☑ Protection, incl. confidentiality Secure destruction	☑ Safeguards (logical, physical, procedural) Secure destruction

Recordkeeping and Privacy: How they compare

Principle	the Principles (ARMA)	CSA Model Privacy Code
9. Availability / Individual Access	☑ Availability to the organization	☑ Availability to the individual
10. Compliance / Challenging Compliance	☑ Internal compliance	☑ External (based on rights of the individual)

A linear view of the life cycle

Privacy

- Purpose
- Consents
- Limit collection

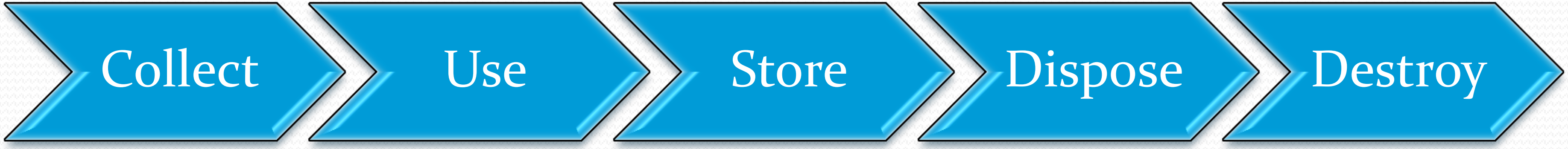
- New purpose
- New consent

- Disclosure (FOI)
- Audit access by staff

- De-identify
- Anonymize for research purposes
- Keep some PI past retention date

- Secure destruction

- Apply safeguards, including encryption
- Privacy Impact Assessments



Collect

Use

Store

Dispose

Destroy

Recordkeeping

- Classify
- Assign retention

- Move location
- Migrate media
- Capture legacy data
- Purge transitory

- New records created

- Secure destruction

- Transitory records destroyed (training)

Part I Recap

- Core concepts of privacy
- Similarities and differences of Information Management (IM) and Privacy program priorities
- Activities at various point of the life cycle

Part 2 Case Studies

- Privacy Practices Report
  - IM program elements incorporated into the Privacy gap analysis
- Information Management Priorities Report
  - Privacy program elements incorporated into the IM gap analysis

Case Study 1:
Privacy Practices Report

Scenario

Large upper tier municipality. Recently merged public health and social services departments represent all Health Information Custodians as defined in legislation (Ontario's PHIPA – Ontario), 2000+ employees

Gap Analysis

CICA's GAPP privacy maturity model

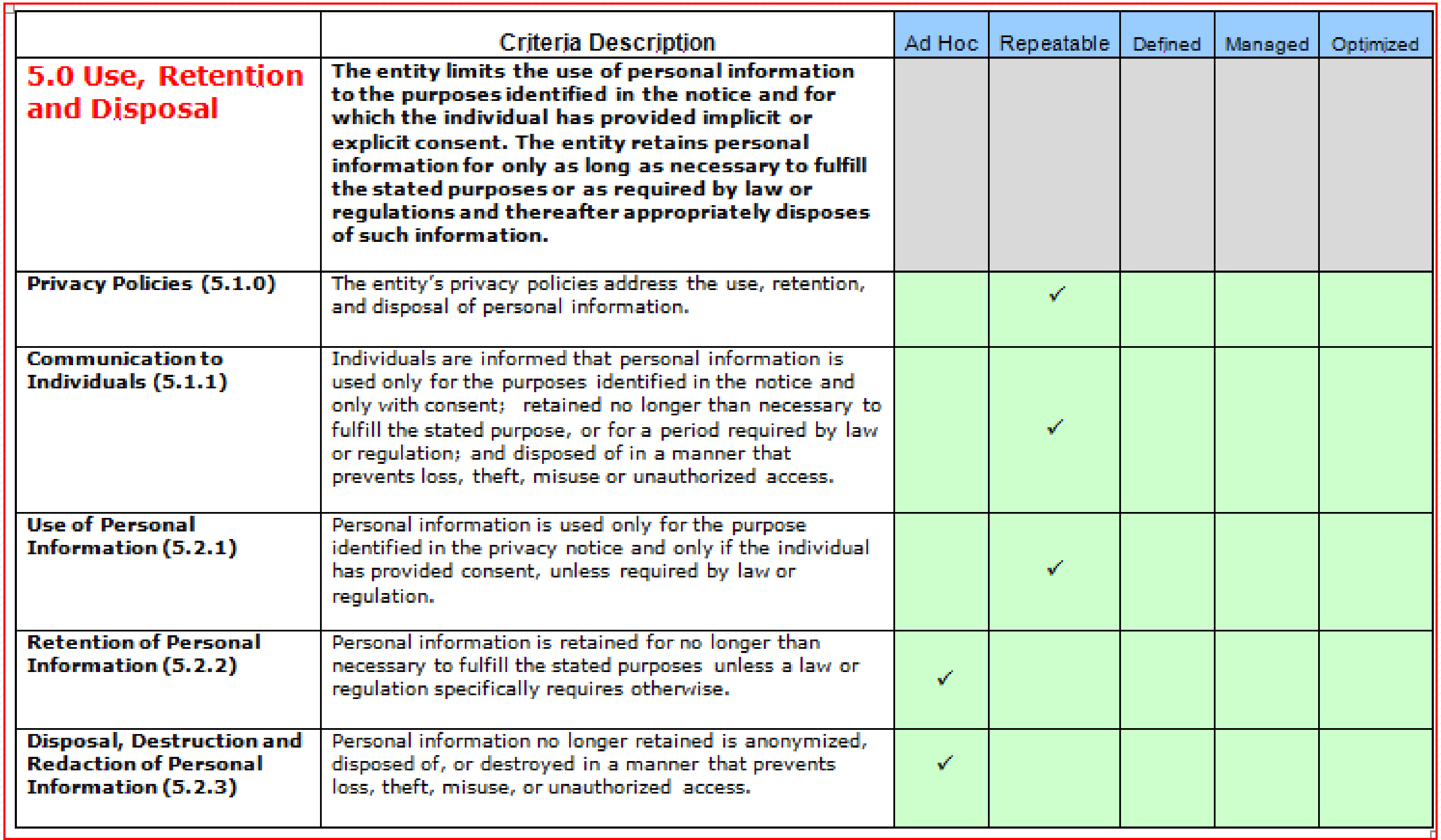
Case study 1:
Privacy Practices Report

- Methodology
  - Many disparate sources of information
  - Challenge was to bring it all together into a coherent narrative
  - Personal Information Bank (PIB) unknown repository search
  - Assessment of current practices using the Generally Accepted Privacy Principles (GAPP) framework
  - Report compiled from all sources, integrating departmental records management and privacy concerns/risks (note: well-established RM program)

Case study 1: Privacy Practices Report, cont'd

- Methodology, cont'd
  - Rated the Department against each of the 73 criteria in the CICA Privacy Maturity Model
  - For each criteria, one of five values was assigned (*ad hoc*, repeatable, defined, managed, or optimized)
  - Level 3 of "defined" was used as the benchmark
  - **All values of "*ad hoc*" and "repeatable", and some values of "defined" were identified as gaps**
  - **Assessments reviewed with program manager**

Case study 1: GAPP Criteria & Maturity Levels

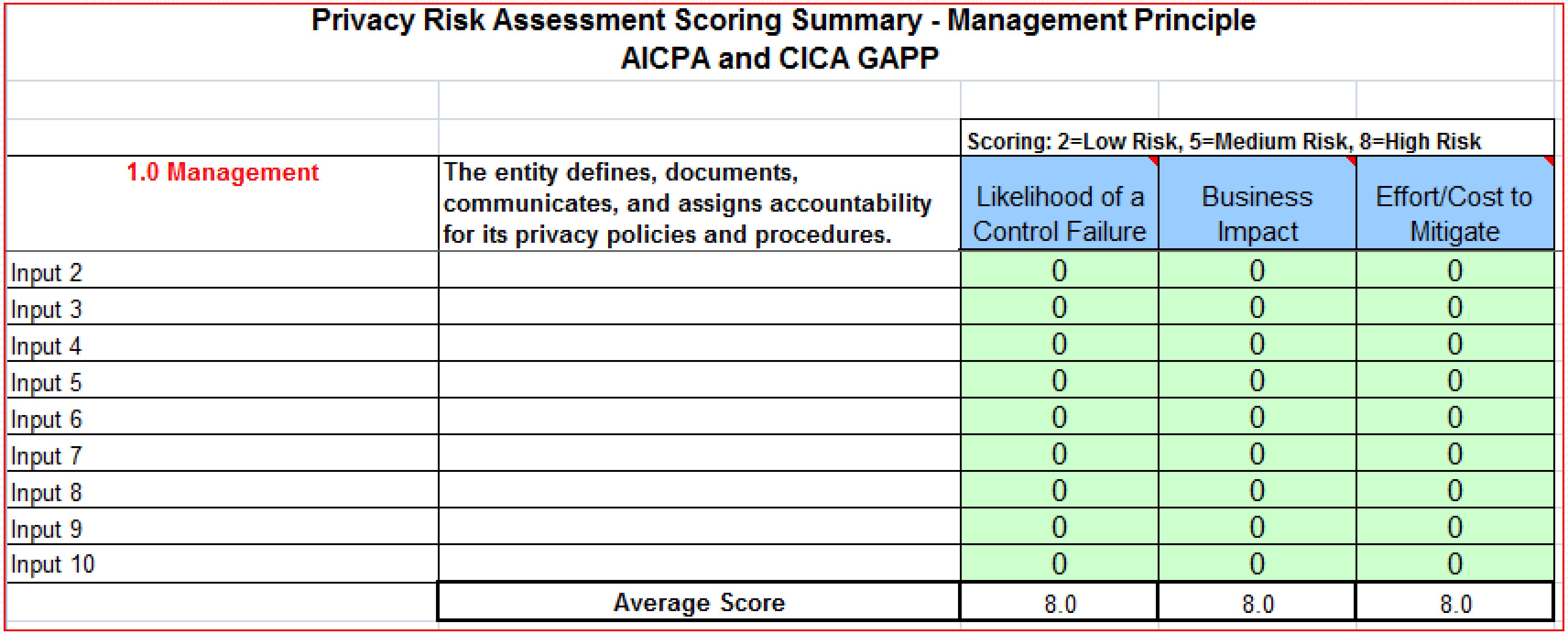


	Criteria Description	Ad Hoc	Repeatable	Defined	Managed	Optimized
5.0 Use, Retention and Disposal	**The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.**					
Privacy Policies (5.1.0)	The entity's privacy policies address the use, retention, and disposal of personal information.		✓			
Communication to Individuals (5.1.1)	Individuals are informed that personal information is used only for the purposes identified in the notice and only with consent; retained no longer than necessary to fulfill the stated purpose, or for a period required by law or regulation; and disposed of in a manner that prevents loss, theft, misuse or unauthorized access.		✓			
Use of Personal Information (5.2.1)	Personal information is used only for the purpose identified in the privacy notice and only if the individual has provided consent, unless required by law or regulation.		✓			
Retention of Personal Information (5.2.2)	Personal information is retained for no longer than necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise.	✓				
Disposal, Destruction and Redaction of Personal Information (5.2.3)	Personal information no longer retained is anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access.	✓				

Case study 1: Another way to do it

- AICPA/CICA Privacy Risk Assessment Tool
- Excel-based
- Consists of
  - a scoring input template (10 separate, individual files for up to 10 different evaluators)
  - a scoring summary that automatically updates using the scores from the 10 templates
- Reports the 5 levels of the privacy maturity model into low risk, medium risk and high risk
- Generates numeric values, more quantitative approach
- Resources lacking for this approach

Case study 1:
Another way to do it



Privacy Risk Assessment Scoring Summary - Management Principle
AICPA and CICA GAPP

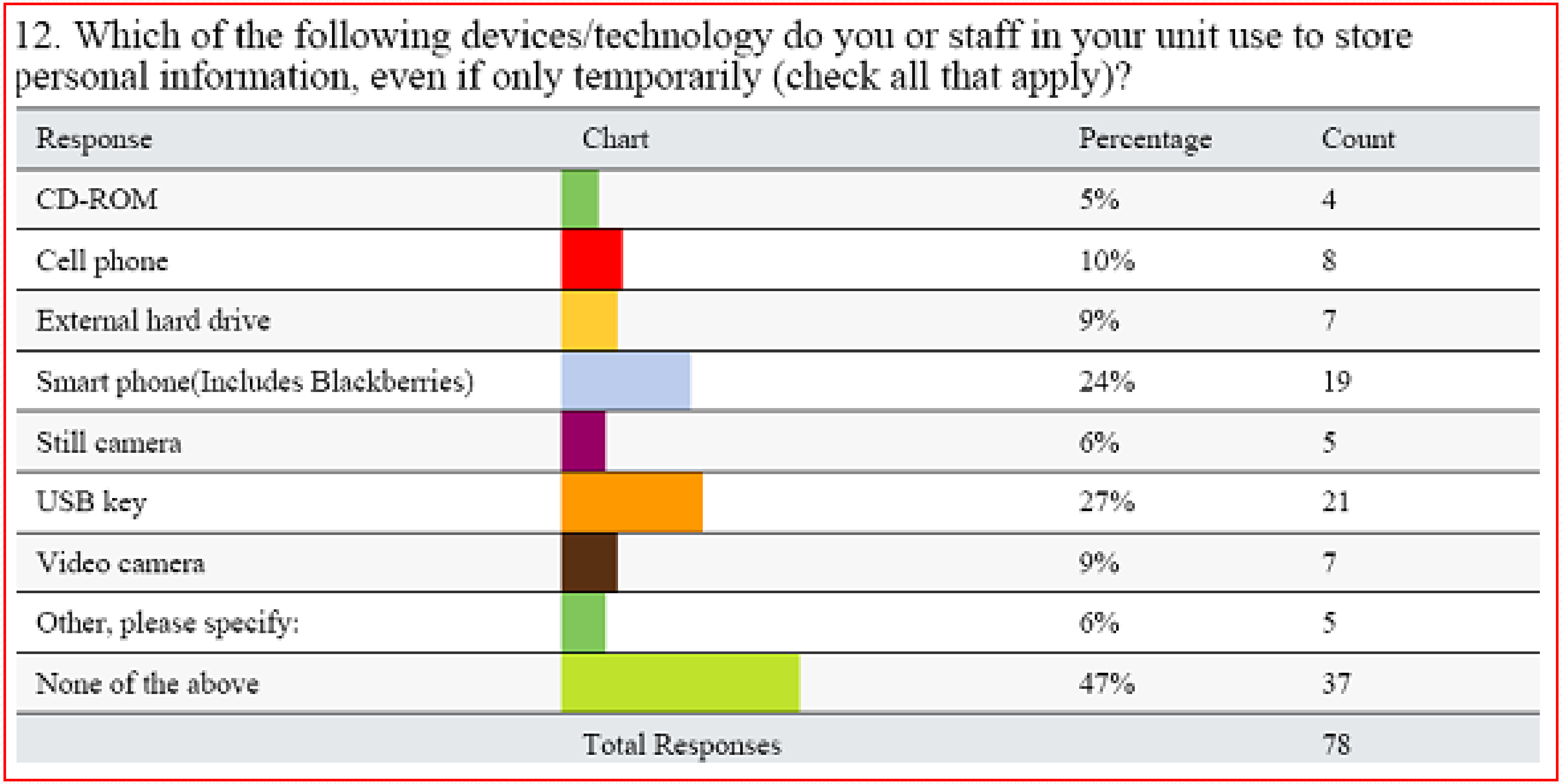
		Scoring: 2=Low Risk, 5=Medium Risk, 8=High Risk		
1.0 Management	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.	Likelihood of a Control Failure	Business Impact	Effort/Cost to Mitigate
Input 2		0	0	0
Input 3		0	0	0
Input 4		0	0	0
Input 5		0	0	0
Input 6		0	0	0
Input 7		0	0	0
Input 8		0	0	0
Input 9		0	0	0
Input 10		0	0	0
	Average Score	8.0	8.0	8.0

2 = ad hoc + repeatable

8 = managed + optimized

5 = defined

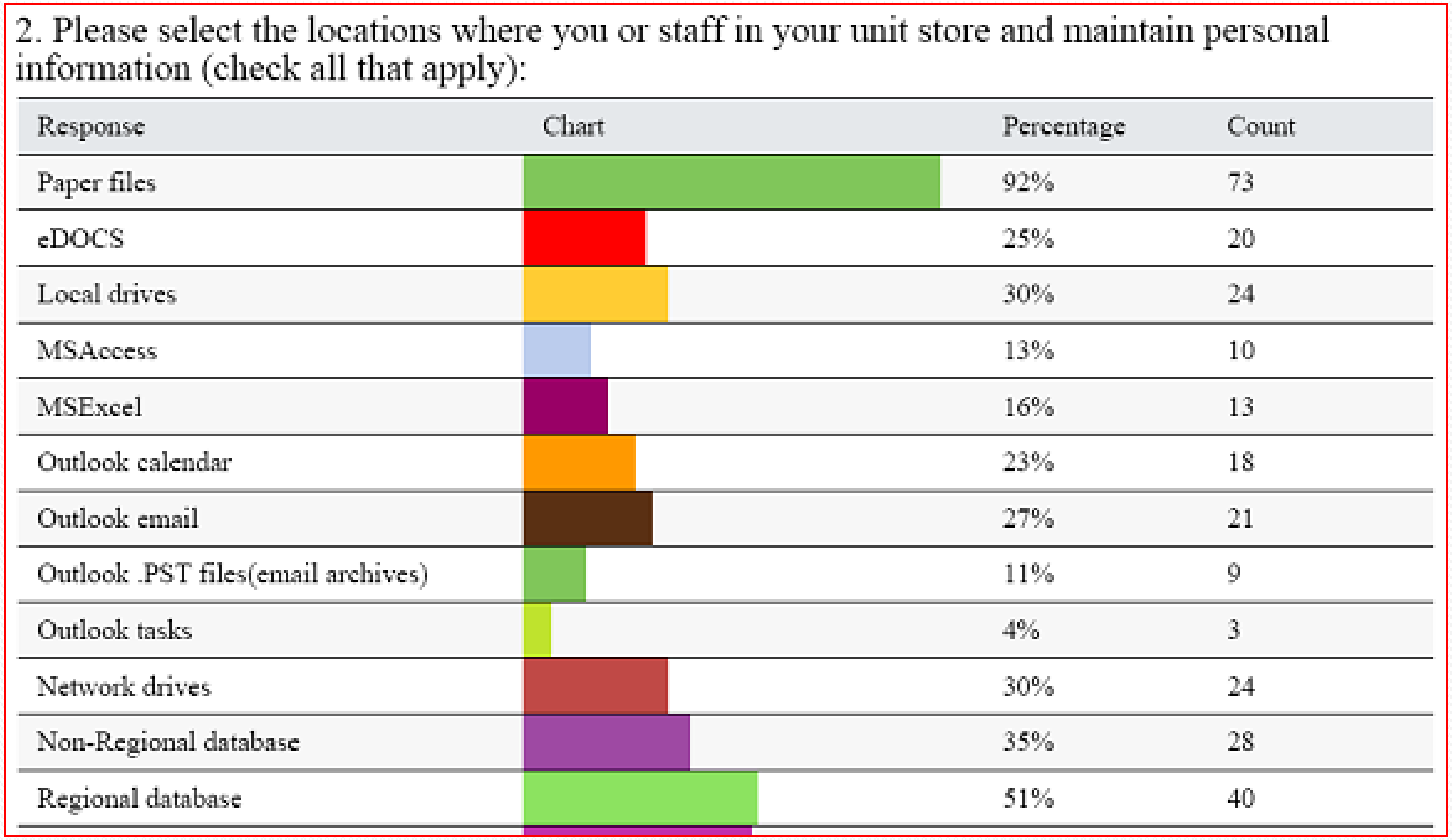
Case study 1:
Sample survey results



12. Which of the following devices/technology do you or staff in your unit use to store personal information, even if only temporarily (check all that apply)?

Response	Chart	Percentage	Count
CD-ROM		5%	4
Cell phone		10%	8
External hard drive		9%	7
Smart phone(Includes Blackberries)		24%	19
Still camera		6%	5
USB key		27%	21
Video camera		9%	7
Other, please specify:		6%	5
None of the above		47%	37
	Total Responses		78

Case study 1:
Sample survey results



2. Please select the locations where you or staff in your unit store and maintain personal information (check all that apply):

Response	Chart	Percentage	Count
Paper files		92%	73
eDOCS		25%	20
Local drives		30%	24
MSAccess		13%	10
MSExcel		16%	13
Outlook calendar		23%	18
Outlook email		27%	21
Outlook .PST files(email archives)		11%	9
Outlook tasks		4%	3
Network drives		30%	24
Non-Regional database		35%	28
Regional database		51%	40

Case study 1: Putting it all together

- GAPP Principle re: "**Use**" 5.2.3 Disposal, Destruction and Redaction of Personal Information**:** "Personal information no longer retained is anonymized, disposed of, or destroyed in a manner that prevents loss, theft, misuse, or unauthorized access."

- *The Records Management and Privacy Practices Policies cover the secure disposal of confidential and personal information respectively. Procedures for the secure destruction of paper records are well established*. *Procedures for the secure disposal of personal health information are lacking for electronic records.* **Level: Ad Hoc**

Case study 1:
Privacy Practices Report

- Final report and recommendations
- Gap Analysis
- Online Survey
- Several other appendices
    - Review of relevant IPC orders
    - Encryption of mobile devices (IPC order)
    - Verified Personal Information Banks
- Some risks and concerns were communicated verbally

Case study 2: IM Priorities Report

Scenario Small lower tier municipality, with well-developed privacy processes but lacking corporate IM program

Gap Analysis ARMA’s Information Governance Maturity Model, supplemented by Model Code Privacy Principles and the CICA Privacy Maturity Model

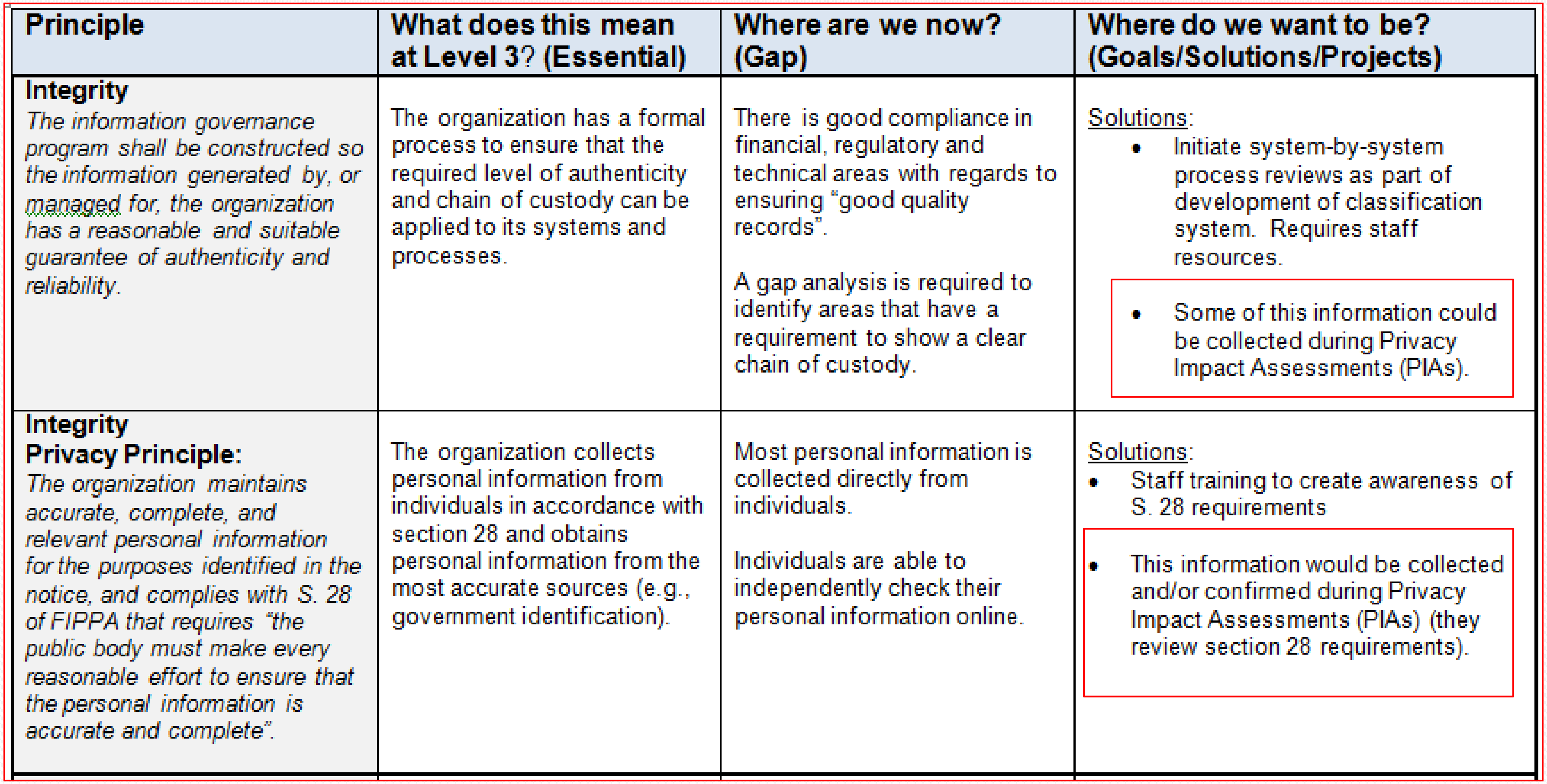
Case study 2:
IM Priorities Report

- Methodology
  - Previous consultant's report reviewed
  - 13 recommendations needed to be updated/validated and did not include access and privacy
  - Decision to overlay privacy program components into ARMA's Information Governance Maturity Model, using CICA's Privacy Maturity Model
  - 65 criteria
  - Level 3 of "essential" chosen as the benchmark

Case study 2:
IM Priorities Report

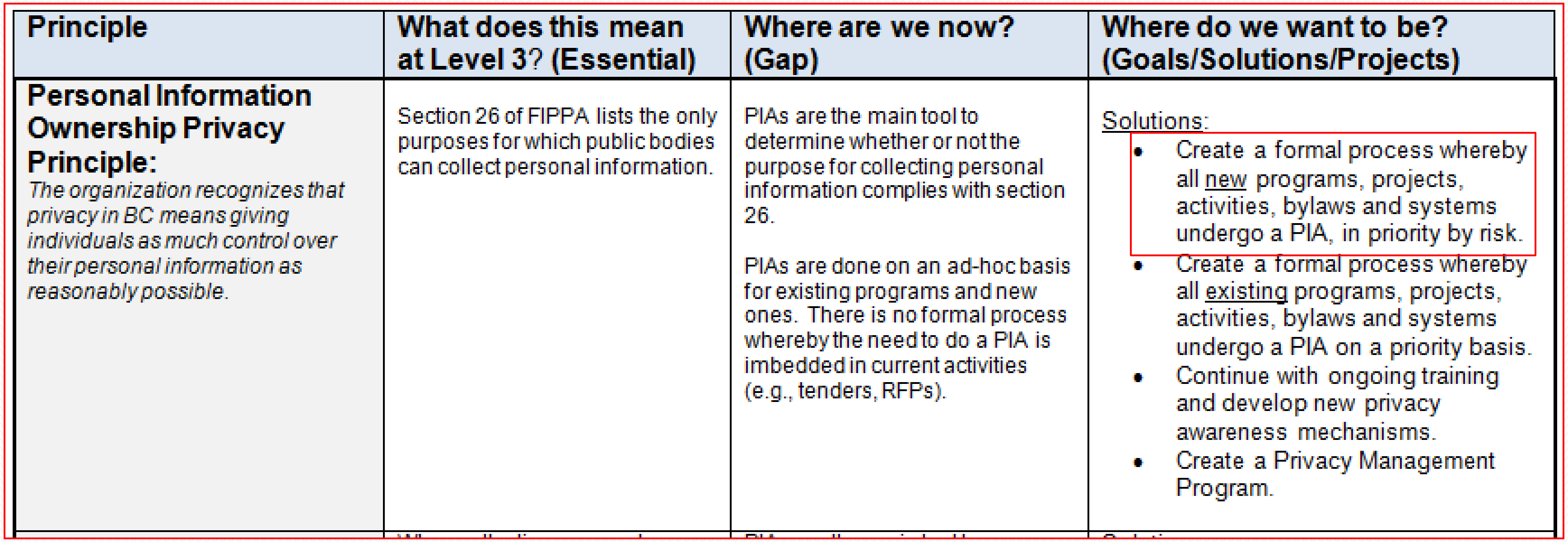
- Methodology, cont’d
  - Created Gap Analysis collection tool based on ARMA
  - Added in privacy-related criteria
  - Added three privacy principles:
    - Personal Information Ownership Privacy Principle
    - Protection of Privacy Principle
    - Access to Information Principle
  - Detailed recommendations, with dependencies
  - 1 page strategic plan
  - 1 page short term work plan

Case study 2:
ARMA Criteria & Maturity Levels



Principle	What does this mean at Level 3? (Essential)	Where are we now? (Gap)	Where do we want to be? (Goals/Solutions/Projects)
Integrity *The information governance program shall be constructed so the information generated by, or managed for, the organization has a reasonable and suitable guarantee of authenticity and reliability.*	The organization has a formal process to ensure that the required level of authenticity and chain of custody can be applied to its systems and processes.	There is good compliance in financial, regulatory and technical areas with regards to ensuring "good quality records". A gap analysis is required to identify areas that have a requirement to show a clear chain of custody.	Solutions: • Initiate system-by-system process reviews as part of development of classification system. Requires staff resources. • Some of this information could be collected during Privacy Impact Assessments (PIAs).
Integrity **Privacy Principle:** *The organization maintains accurate, complete, and relevant personal information for the purposes identified in the notice, and complies with S. 28 of FIPPA that requires "the public body must make every reasonable effort to ensure that the personal information is accurate and complete".*	The organization collects personal information from individuals in accordance with section 28 and obtains personal information from the most accurate sources (e.g., government identification).	Most personal information is collected directly from individuals. Individuals are able to independently check their personal information online.	Solutions: • Staff training to create awareness of S. 28 requirements • This information would be collected and/or confirmed during Privacy Impact Assessments (PIAs) (they review section 28 requirements).

Case study 2:
ARMA Criteria & Maturity Levels



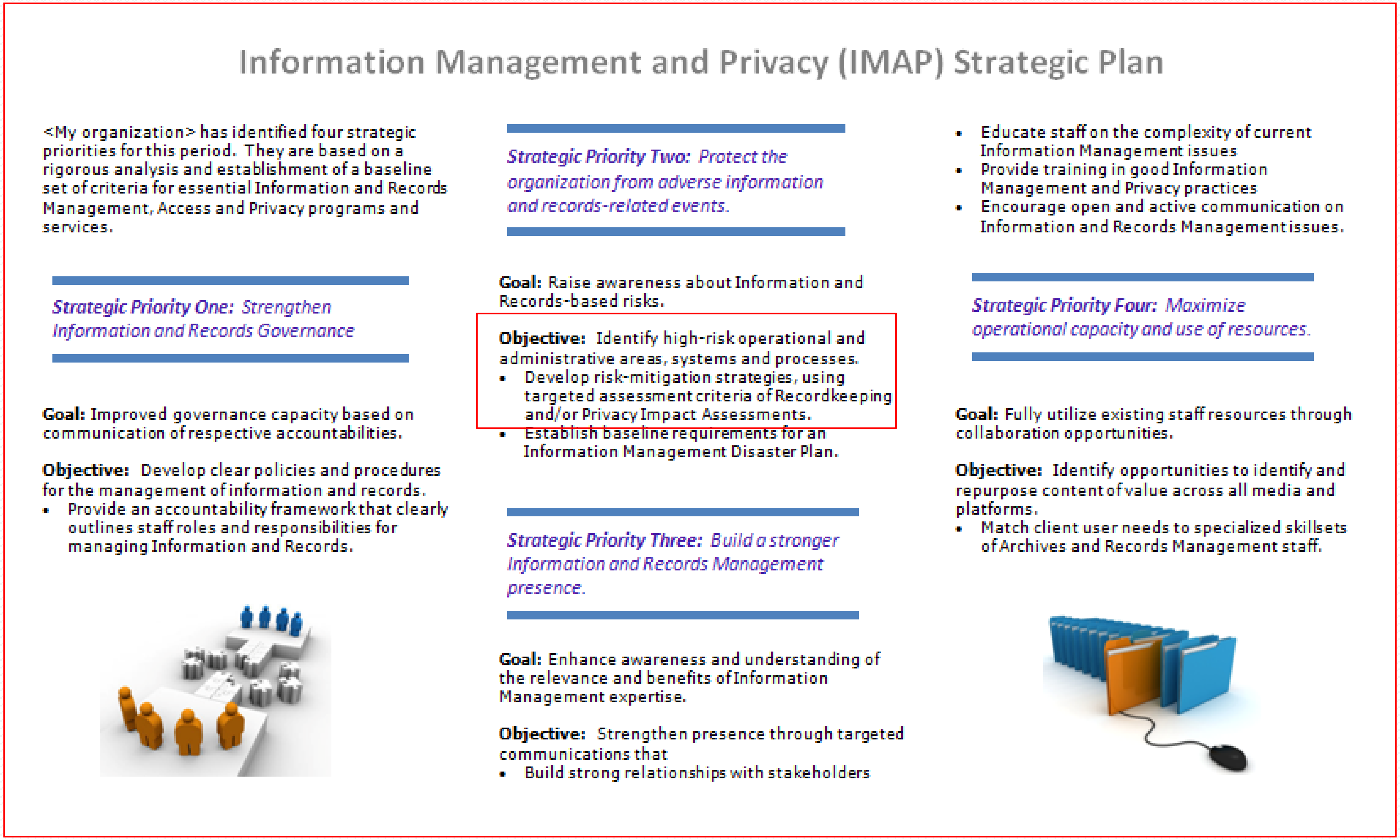
Principle	What does this mean at Level 3? (Essential)	Where are we now? (Gap)	Where do we want to be? (Goals/Solutions/Projects)
Personal Information Ownership Privacy Principle: *The organization recognizes that privacy in BC means giving individuals as much control over their personal information as reasonably possible.*	Section 26 of FIPPA lists the only purposes for which public bodies can collect personal information.	PIAs are the main tool to determine whether or not the purpose for collecting personal information complies with section 26. PIAs are done on an ad-hoc basis for existing programs and new ones. There is no formal process whereby the need to do a PIA is imbedded in current activities (e.g., tenders, RFPs).	Solutions: • Create a formal process whereby all new programs, projects, activities, bylaws and systems undergo a PIA, in priority by risk. • Create a formal process whereby all existing programs, projects, activities, bylaws and systems undergo a PIA on a priority basis. • Continue with ongoing training and develop new privacy awareness mechanisms. • Create a Privacy Management Program.

Case study 2: ARMA Criteria & Maturity Levels

Sample IM recommendations incorporating privacy

- **Create an Information Management and Privacy (IMAP) Working Group**
  - This group tasked with developing a priority ranking of outstanding PIAs based on risk
- **Develop a corporate-wide privacy policy (if not in corporate-wide IM policy)**
  - Continue to complete Privacy Impact Assessments on high priority processes/programs

Case study 2:
High Level Strategic Plan



Information Management and Privacy (IMAP) Strategic Plan

<My organization> has identified four strategic priorities for this period. They are based on a rigorous analysis and establishment of a baseline set of criteria for essential Information and Records Management, Access and Privacy programs and services.

***Strategic Priority One:** Strengthen Information and Records Governance*

Goal: Improved governance capacity based on communication of respective accountabilities.

Objective: Develop clear policies and procedures for the management of information and records.

- Provide an accountability framework that clearly outlines staff roles and responsibilities for managing Information and Records.

***Strategic Priority Two:** Protect the organization from adverse information and records-related events.*

Goal: Raise awareness about Information and Records-based risks.

Objective: Identify high-risk operational and administrative areas, systems and processes.

- Develop risk-mitigation strategies, using targeted assessment criteria of Recordkeeping and/or Privacy Impact Assessments.
- Establish baseline requirements for an Information Management Disaster Plan.

***Strategic Priority Three:** Build a stronger Information and Records Management presence.*

Goal: Enhance awareness and understanding of the relevance and benefits of Information Management expertise.

Objective: Strengthen presence through targeted communications that

- Build strong relationships with stakeholders
- Educate staff on the complexity of current Information Management issues
- Provide training in good Information Management and Privacy practices
- Encourage open and active communication on Information and Records Management issues.

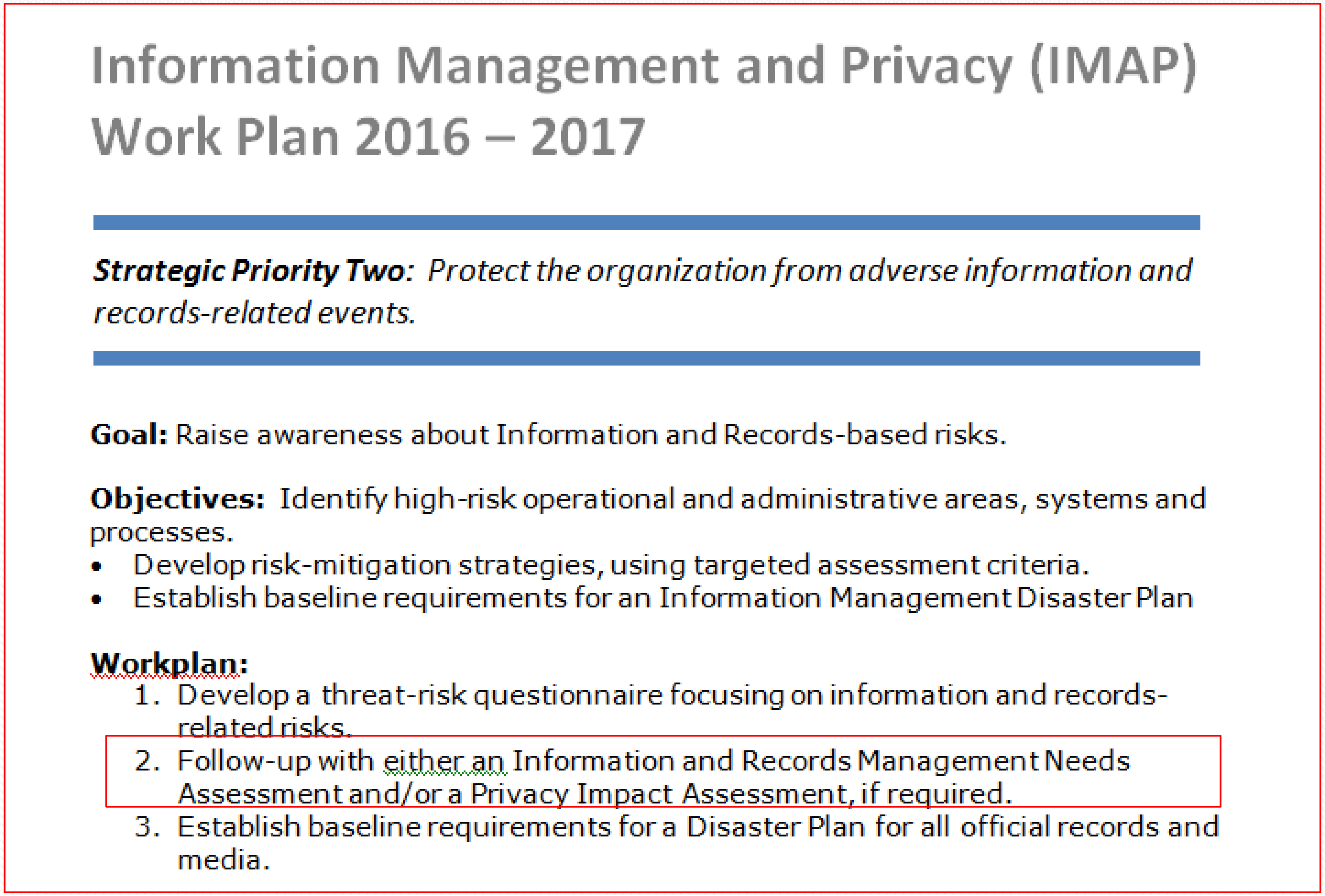
***Strategic Priority Four:** Maximize operational capacity and use of resources.*

Goal: Fully utilize existing staff resources through collaboration opportunities.

Objective: Identify opportunities to identify and repurpose content of value across all media and platforms.

- Match client user needs to specialized skillsets of Archives and Records Management staff.

Case study 2:
High Level Work Plan



Information Management and Privacy (IMAP) Work Plan 2016 – 2017

Strategic Priority Two: *Protect the organization from adverse information and records-related events.*

Goal: Raise awareness about Information and Records-based risks.

Objectives: Identify high-risk operational and administrative areas, systems and processes.

- Develop risk-mitigation strategies, using targeted assessment criteria.
- Establish baseline requirements for an Information Management Disaster Plan

Workplan:

1. Develop a threat-risk questionnaire focusing on information and records-related risks.
2. Follow-up with either an Information and Records Management Needs Assessment and/or a Privacy Impact Assessment, if required.
3. Establish baseline requirements for a Disaster Plan for all official records and media.

Recap / Questions

- Core concepts of privacy

- Similarities and differences of Information Management (IM) and Privacy programs priorities

- 2 Case Studies

- Lessons learned from using a Maturity Model

Thank you for sharing your time with me.

Julie Luckevich, MLIS, CIAPP-P
Eclaire Solutions Inc
eclaires@telus.net