Office of the Chief Information and Privacy Officer

Privacy Impact Assessment Workshop Part Two

Tracy Ann Kosa, PIA Specialist

Wednesday, October 28, 2009

Ontario

Outline

- Module 1: Understanding Privacy Risk
- Module 2: Risk Methodology Using PIAs
- Module 3: Group Case Studies
- Module 4: Summary / Lessons Learned


PLAY AT
YOUR
OWN
RISK

Module 1

- Types of Risk
- Calculating Risk
- Risk Language

Types of Risk

- Defining Risk
  - Application and Situation
- Generally risks are seen as future issues which can be avoided or mitigated
- 3 variables to consider:
  - Probability that there is a threat
  - Probability that there are any vulnerabilities
  - Potential impact to the business

Calculating Risk

$$R(\theta, \delta(x)) = \int L(\theta, \delta(x)) f(x|\theta)\, dx$$

$$\text{Risk} = (\text{probability of an accident}) \times (\text{losses per accident}).$$

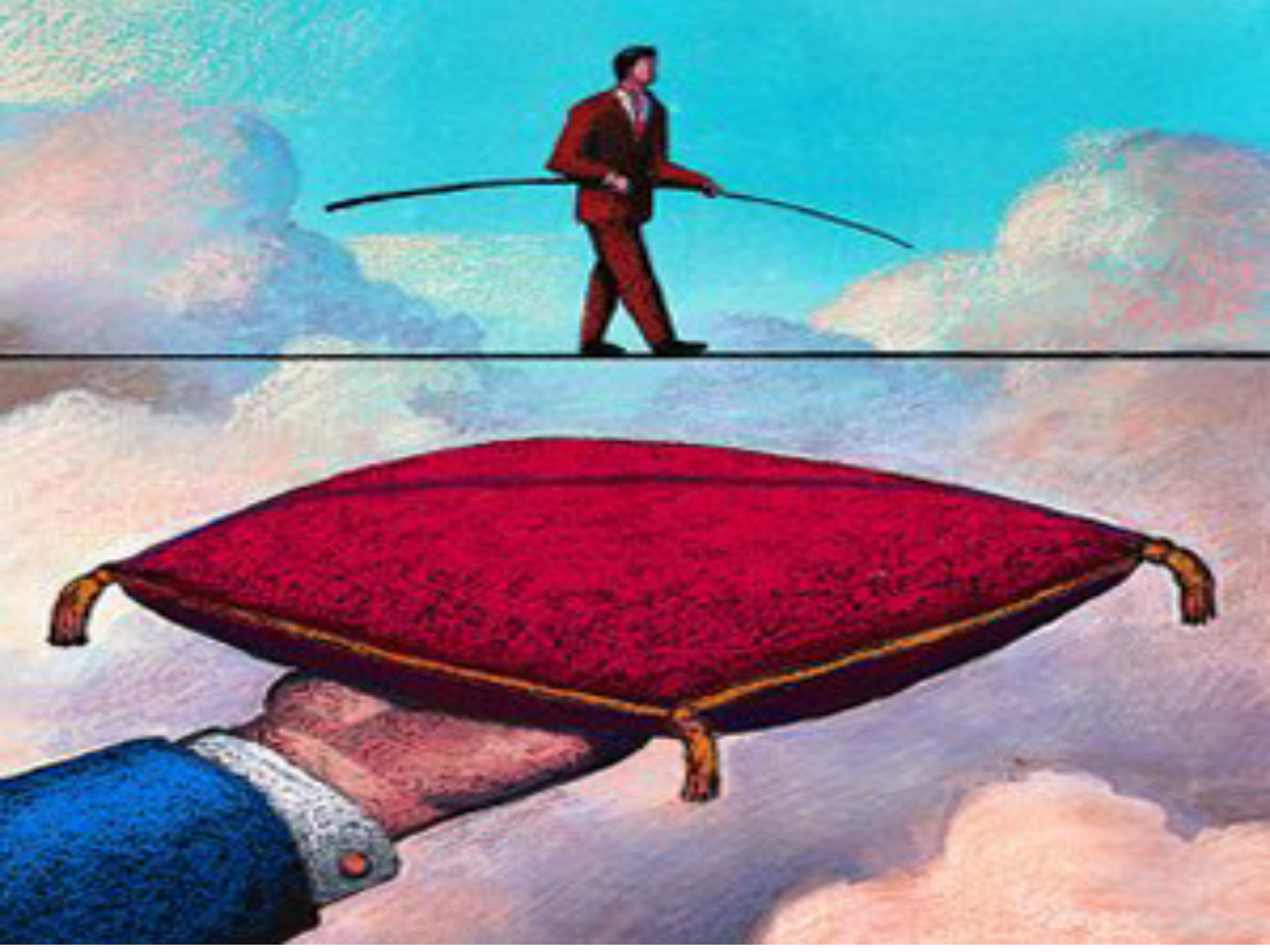
Or more generally,

$$\text{Risk} = (\text{probability of event occurring}) \times (\text{impact of event occurring}).$$

Risk Language

- Risk
  - A state of uncertainty where some of the possibilities involve a loss, catastrophe or other undesirable outcome
  - Measurement
    - A set of possibilities each with quantified probabilities and quantified losses

- Uncertainty
  - A lack of complete certainty and the existence of more than one possibility; the true outcome / state / result / value is unknown
  - Measurement
    - A set of probabilities assigned to a set a probabilities



- *We can be uncertain about the winner of a contest, but unless we have some personal stake in it, we have no risk.*

- *If we bet money on the outcome of the contest, then we have a risk. In both cases there are more than one outcome.*

- *The measure of uncertainty refers only to the probabilities assigned to outcomes, while the measure of risk requires both probabilities for outcomes and losses quantified for outcomes.*

Module 2

- Privacy Risk Methodology
  - Step 1: Create Risk Statements
  - Step 2: Apply the Action Items
  - Step 3: Assign Ratings
  - Step 4: Plot on Risk Map

Case Study: MEDT

Ontario

Ontario.ca | Français

MINISTRY OF ECONOMIC DEVELOPMENT AND TRADE

Search GO

HOME | ABOUT THE MINISTRY | PROGRAMS & SERVICES | NEWS | SUCCESS STORIES | OPEN FOR BUSINESS

› Minister of Economic Development and Trade, Sandra Pupatello

Link to International Trade and Investment

- International Trade and Investment

Spotlight

Ontario Helps Local Cabinet Manufacturer Go Green

Ontario is helping a manufacturer of commercial millwork and custom cabinetry create jobs and reduce its impact on the environment.

The company, Bamco Custom Woodworking, is investing in robotic finishing equipment that will reduce production times by 75 per cent. Bamco will become one of the first manufacturers in North America to offer an environmentally friendly finishing process by developing water-based stains and lacquers. The project will create 72 new jobs at the company.

Summer Company

SUMMER COMPANY

Success Stories

Summer Company is an Ontario government program that has been helping students aged 15-29 start up and run their own businesses since 2001. For more information, visit our **Summer Company** section.

Crafting a unique business and a new career

Jen Van Herten's Summer Company uses skills she's learning in the three-year Crafts and Design program at Sheridan College.

LONDON--Jen Van Herten has found her calling at age 29, and Summer Company is helping her achieve her new career goals. Like many students, Van Herten wasn't sure what she wanted to do after high school. She attended college and began a career working at a large insurance company, moving up from a call centre to head office over six years. She enjoyed her job, but an office retirement party prompted a change.

"I had just discovered my love for working with glass, when I was framing some photos and just couldn't seem to stop," she laughs. "The thought of spending my life in insurance wasn't appealing, so I quit my job, did some traveling, and started working with glass seriously in New Hampshire. I'm now in my second year in the Crafts and Design program at Sheridan, specializing in glass. I'm here because I want to be."

PIA

Office of the Chief Information and Privacy Officer

PIA Development Service

PIA Centre of Excellence

Privacy Impact Assessment

Summer Company Grant Management System

Entrepreneurship Branch

Ministry of Small Business & Entrepreneurship

Step 1: Create Risk Statements

- Gather all the findings in the PIA
- Classify the findings

Findings

6 Privacy Findings

This section contains findings and action items related to the Summer Company program, with a specific emphasis on the SCREEN application.

As stated earlier, MSBE is also subject to the *Freedom of Information and Protection of Privacy Act,* 1990 (FIPPA), in providing the Summer Company p
Association International's Model Code for the Protectior
used to benchmark the privacy posture of the program b
adaptive analysis. However, there are two notable point
separately: authority for collection and personal informat

	Finding
F1.	The Summer Company program includes a number of paper-based and electronic processes.[1] These intersections create additional risks for MSBE by requiring additional processes and controls to protect PI in multiple media (e.g. electronic and paper).
F2.	Program providers give paper copies of applicant data to mentors in advance of meetings. MSBE retains accountability of these (and all other) paper copies.
F3.	Contact information for each of these positions has not been made widely available within the SCREEN application.
F4.	MSBE does not have contracts in place with internal organizations (i.e., other government institutions) that have access to records in its custody and control, including ITS and OSS.
F5.	Contracts with program providers (non-profits and SBECs) do not extend the information management obligations for the protection of PI under FIPPA.
F6.	MSBE does not have a ministry-wide privacy policy.
F7.	Summer Company program staff are working with MSBE staff to schedule privacy training.
F8.	The notice of collection is extremely detailed, and also used as a statement of authority to support release of information documentation requirements.
F9.	The SCREEN application applicant database can be considered a personal information bank (PIB), and is subject to additional requirements under FIPPA.
F10.	Preliminary review of contracts indicates no specific statements relating to organizational custody and control of applicant PI.
F11.	The notice of collection does not reflect the totality of information management practices (including electronic and paper-based processes) associated with Summer Company program, from the point of collection to secure destruction.
F12.	Not applicable.
F13.	The ministry FOI Coordinator is working with the program area to schedule privacy training to supplement existing knowledge, and tailor it specifically to privacy compliance.
F14.	Consent documents are sent by unsecured fax to MSBE, and become part of the applicant's paper records retained at the ministry. These paper records are stored in an open shelving unit on a card-accessed floor.
F15.	The current consent document does not accurately and completely describe all information management practices associated with applicant PI. For example, the current consent document includes references to the now-outdated practice of performing a credit check on applicants.

ID	Risk Statement	Risk Description
SBE01	Summer Company and its internal OPS service providers have no agreements in place for the provision of services.	MSBE, as the collecting institution, retains accountability under FIPPA for all information management practices associated with Summer Company program applicant PI. These obligations extend to all actions taken by third parties such as ITS and OSS with applicant PI when disclosed by MSBE.
SBE02	Summer Company and its program providers have no privacy clauses in their agreements.	MSBE, as the collecting institution, retains accountability under FIPPA for all information management practices associated with applicant PI. Agreements with program providers, SBECs and non-profits, do not contain an adequate description of the information management practices these organizations must implement as agents of MSBE. In retaining this risk, Summer Company retains all obligations for assuring program provider compliance with FIPPA.
SBE03	Safeguards associated with the SCREEN application do	The SCREEN application was built to replace a number of existing Summer Company paper-based processes. Existing paper-based

Step 2: Apply the Action Items

- Apply the action items to the appropriate / corresponding risk statement

	Action Item
A1.	All paper-based processes associated with Summer Company (including but not limited to those documented in this PIA) should be documented, reviewed and eliminated where possible.
A2.	The login page of the SCREEN application should have a link to the contact information for the Summer Company program director, and the Ministry FOI Coordinator.
A3.	Privacy clauses extending the specific obligations for PI information management practices under FIPPA should be developed and appended to all program provider agreements.
A4.	MSBE should develop information management service level agreements (SLA) with other governmental organizations to whom it discloses applicant PI.
A5.	The program area should have a privacy policy to guide its privacy practices.
A6.	The planned delivery of privacy training should be finalized so that all staff that collect, use and / or disclose PI for Summer Company are trained in basic FIPPA and best practice-related privacy requirements.
A7.	The notice of collection should be amended to include a clear and specific statement of authority.
A8.	A release should be provided when applications are initially submitted for consideration.
A9.	The program area needs to develop and implement an Acceptable Use Policy for the SCREEN application.
A10.	MSBE should explore the additional reporting requirements for PIBs under FIPPA.
A11.	Privacy clauses specific to the custody and control of applicant PI should be developed and appended to all program provider agreements.
A12.	In developing information management SLAs with other governmental organizations, MSBE should include clauses that pertain to custody and control of all applicant PI, including logs.
A13.	MSBE, in conjunction with the ministry FOI Coordinator, should update the notice of collection to reflect an accurate and detailed statement of authority, and all information management practices as documented in the PIA.
A14.	The updated notice of collection should be made available to all past, current and new applicants via the SCREEN application at the point of login.
A15.	Not applicable
A16.	Not applicable
A17.	Applicant paper records should be eliminated where possible. Alternatively, additional physical security controls should be implemented to restrict access to paper copies of applicant data (including consent forms), such as locked filing cabinets.

Mitigation Strategy	Residual Risk[55]
1. Action Items A4, A12, A42, and A58	Minimal
2. Action Items A3, A11 and A53	Minimal
3. Action Items A1, A17, A36, A41,	Minimal

Step 3: Assign Ratings

- In consultations with the project / program area, choose the impact categories
  - Harm to Individual
  - Impact to Cost
  - Impact to Reputation
  - Impact to Service Delivery

- Apply the appropriate impact level
  - Scale from 1 to 5

- Apply the applicable probability rating
  - Scale from 1 to 5

Risk Owner	Risk Impact[53]	Risk Likelihood[54]	Risk Level
Ministry Program	Very High	High	5
Program	High	High	4
Program	High	High	4

Step 4: Plot on Risk Map

- This is where the math comes in …

Table 3: Risk Map

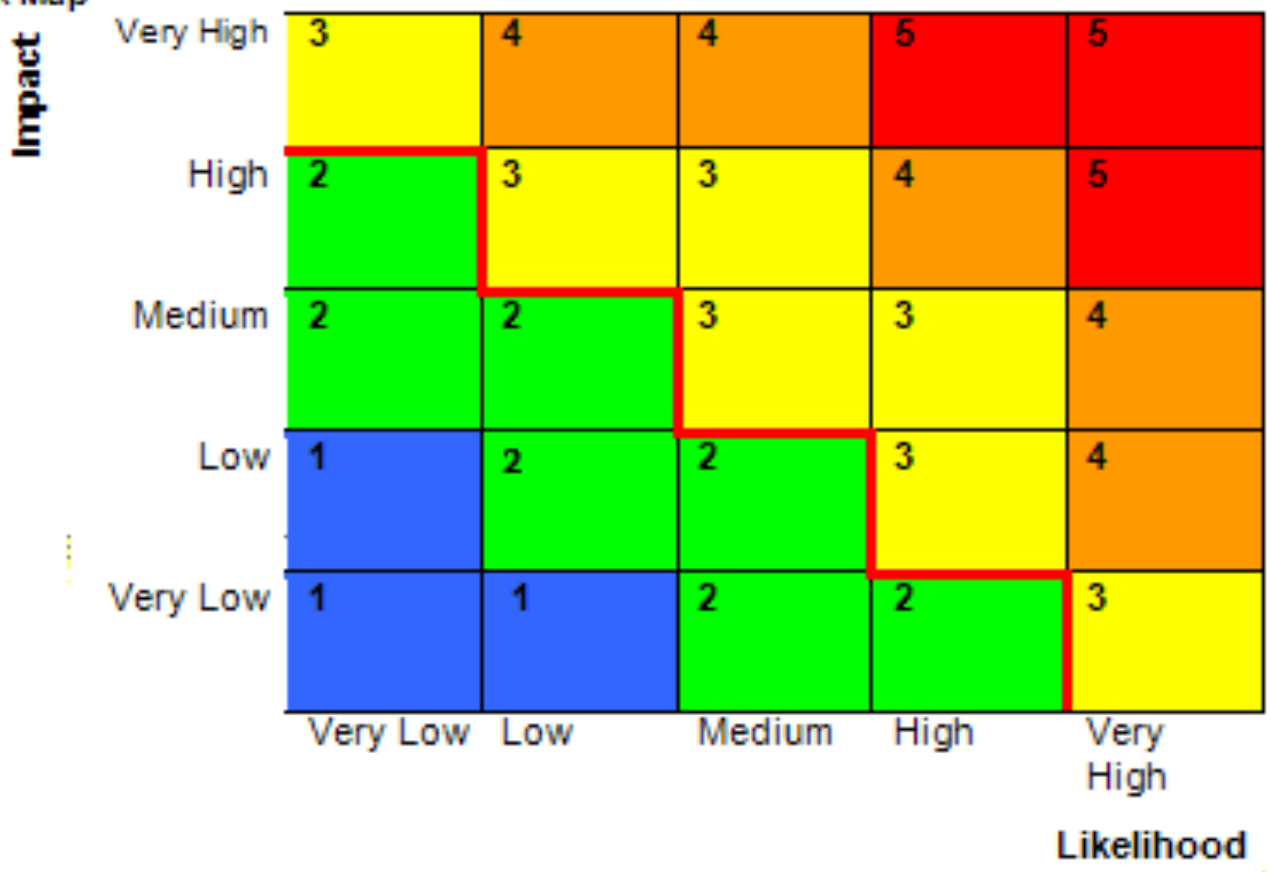
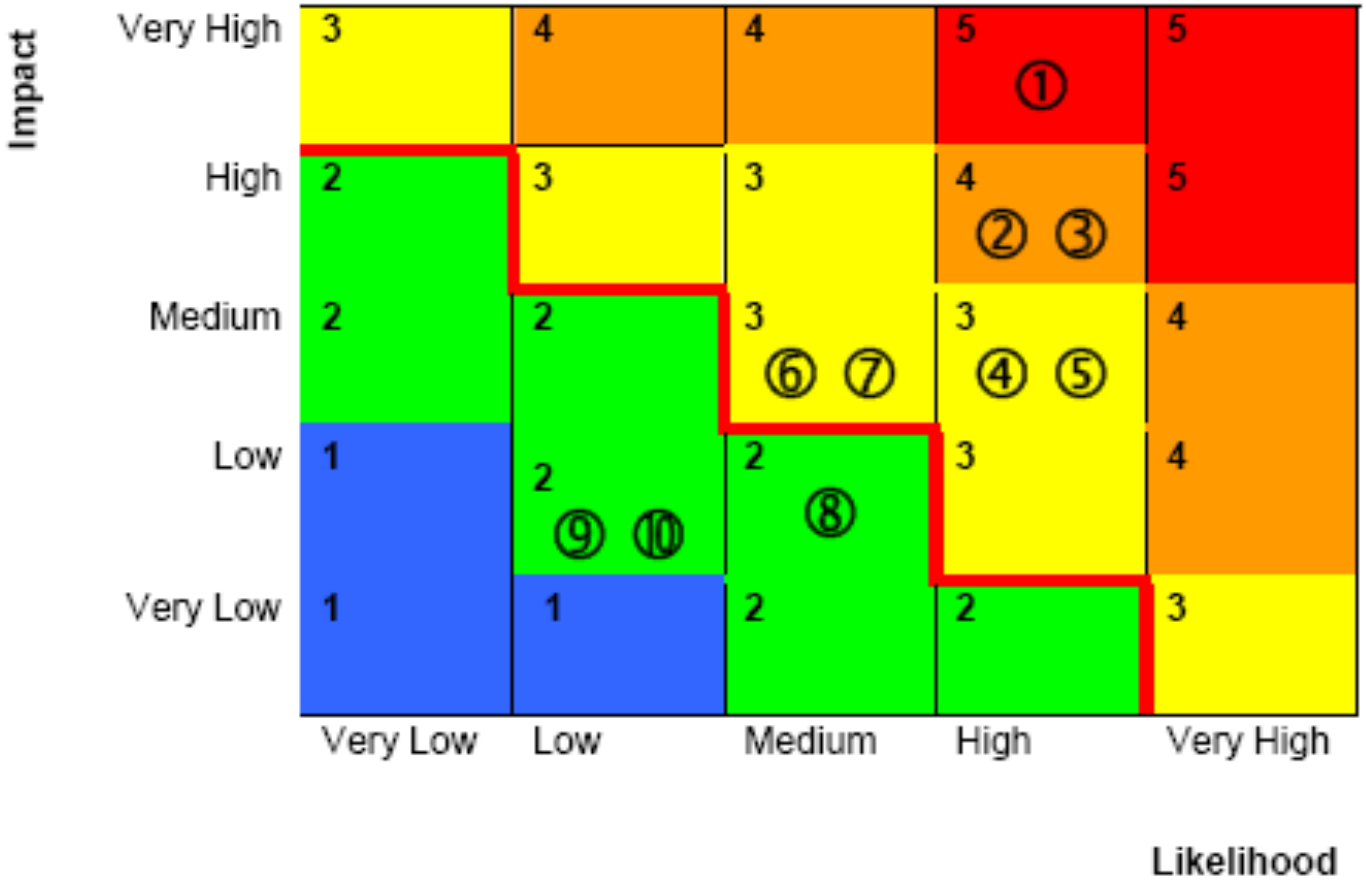


Table 3


Impact
Very High
High
Medium
Low
Very Low
3
4
4
5
5
2
3
3
4
5
2
2
3
3
4
1
2
2
3
4
1
1
2
2
3
①
②
③
④
⑤
⑥
⑦
⑧
⑨
⑩
Very Low
Low
Medium
High
Very High
Likelihood

Module 3

- Case Studies

The Deliverable

- A completed privacy risk map that includes:
  - A list of risk statements
  - An impact and likelihood ranking for each risk
  - A list of corresponding action items / mitigation strategy
  - Create a risk map

Risk Statements

- Pull out or create a list of at least 15 findings
- Classify the list of findings into groups
- Write the risk statements about each group

"No fingerprints, no picture ID, no Social Security number. I'm afraid your baby presents a serious security risk."

How do you classify findings?

- Handout - Table 5
- Handout - Table 6

CSA Code or Privacy Risks

CSA Code	Risks
Accountability	Breach
Identifying Purpose	Non-Compliance
Consent	Over-Compliance
Limiting Collection	Complaints
Limiting Use, Disclosure and Retention	Inadvertent Data Matching
Accuracy	Re-Identification
Safeguards	… Other Look Fors …
Openness	Records Management
Individual Access	Security
Challenging Compliance	Information Classification

Assign Impact & Likelihood Rankings

- Choose an impact category that applies best to the case study
- Assign an impact rating to each risk statement
- Assign a likelihood rating to each risk statement

How do you assign ratings?

- Handout - Table 1
- Handout - Table 2

Impact Categories

	Impact to Individual (Harm)	Impact to Cost	Impact to Reputation	Impact to Service Delivery
Very High	▪ Could reasonably be expected to cause loss of life	▪ Capital Cost of > $100 M	▪ Potential for reduction in program mandate	▪ Six months or more ▪ May not be able to deliver on most critical requirements
High	▪ Could reasonably be expected to cause loss to public safety, extremely serious personal injury, significant financial loss, social hardship	▪ Capital Cost of $10M to $100 M	▪ Serious adverse attention from media and / or public	▪ Between two and six months ▪ Major shortfalls in one or more critical requirements
Medium	▪ Could reasonably be expected to cause serious personal injury, damage to relationships and reputation	▪ Capital Cost of $1M to $10 M	▪ Minor adverse attention from media, medical establishment and / or public	▪ Between two weeks and two months ▪ Minor shortfalls in one or more key requirements
Low	▪ Could reasonably be expected to cause injury that would result in minor financial loss, embarrassment, inconvenience	▪ Capital Cost of $100,000 to $1M	▪ Loss of reputation among clients / partners	▪ Less than two weeks ▪ A few shortfalls in desired functionality
Very Low	▪ Will not result in any harm or injury	▪ Capital Cost of < $100,000	▪ Internal loss of reputation	▪ Less than two days ▪ System should still fully meet mandatory requirements

Likelihood / Probabilities

	Probability	Likelihood Description
Very High	> 80%	• This event will probably occur in the near future.
High	51% to 80%	• This event is likely to occur in the near future.
Medium	21% to 50%	• This event may occur in the near future.
Low	6% to 20%	• This event is possible but highly unlikely to occur in the near future.
Very Low	0% to 5%	• This event is not expected to occur in the near future.

Create a Mitigation Strategy

- Decide how best to address each risk statements
- If the findings in the PIA have associated action items, assign them to the risk statements
- If the findings in the PIA do not have any associated action items, create them in a mitigation strategy for the risk

Create a Risk Map

- Map the assigned impact and likelihood rankings for each risk and plot them on the graph

How do you plot on a map?

- Handout - Table 3

Results

- Review the results of the risk map
- Reality check

Module 4

- Summary
- Lessons Learned

Summary

- Get input from the experts
- Many heads are better than one
- Take your time

Lessons Learned

- Involve the project team in assigning risk impact and likelihood
- Provide mitigation strategies for all risks
- Do a reality check on the risk map

Resources

- Treasury Board, Risk Management – Policies and Publications, http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/siglist-eng.asp
- Treasury Board, Integrated Risk Management Framework, http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12254
- Treasury Board, Integrated Risk Management Implementation Guide, http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/riskmanagement/guide-eng.asp
-

"We've considered every potential risk except the risks of avoiding all risks."

Tracy Ann Kosa
PIA Specialist
Office of the Chief Information and Privacy Officer
Ministry of Government Services
(416) 212-1136
tracy.kosa@ontario.ca