



**Bank Financial Group**

**ATB Financial**

*Where there's a way*

## **Building a Culture of Privacy**



**Robin Gould-Soil and Sandra Smith-Frampton**

**PIPA conference 2008**

**November 18, 2008**



## ***Today's Presentation***

1. Be Strategic About Positioning Privacy
2. Develop a Privacy Governance Structure
3. Policy, Standards and Communication
4. Metrics to Measure Privacy Compliance
5. Monitoring
6. Educate and Train By Role

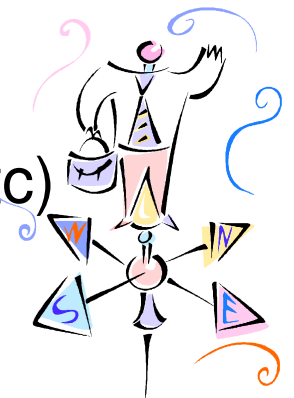




## 1. Be Strategic About Positioning Privacy

### Privacy is NOT just a compliance issue

- It's a customer service issue
- It's a business issue
  - Linked to brand/reputation – and the bottom line
- It's a security issue
  - Protection against threats (ID theft, phishing, etc)





## 1. *Be strategic about positioning privacy(cont'd)*

**Don't see the chief privacy officer's role as limited to mediation and enforcement.**

**A good privacy officer must be:**

✓ A salesperson



✓ A partner



✓ A champion



✓ A preacher





***1. Be strategic about positioning privacy(cont'd)***

**Do's and Don'ts**

- **Avoid “police officer” label**
- **Build a business case**
- **Be flexible and co-operative**
- **Need access to executives, not necessarily direct reporting**
- **Use outside examples to illustrate the good, the bad and the ugly**



## 1. *Be strategic about positioning privacy(cont'd)*

### Some lessons learned...

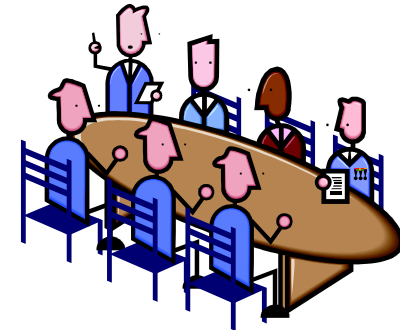
- Engage people - make them feel accountable and involved
- Be, and be seen as, a partner
  - Demonstrate how privacy can help them perform their day to day business function
- Recognize that you're in business to make money
- Network and communicate often
- Develop and offer tools to make compliance easy (see next slide)





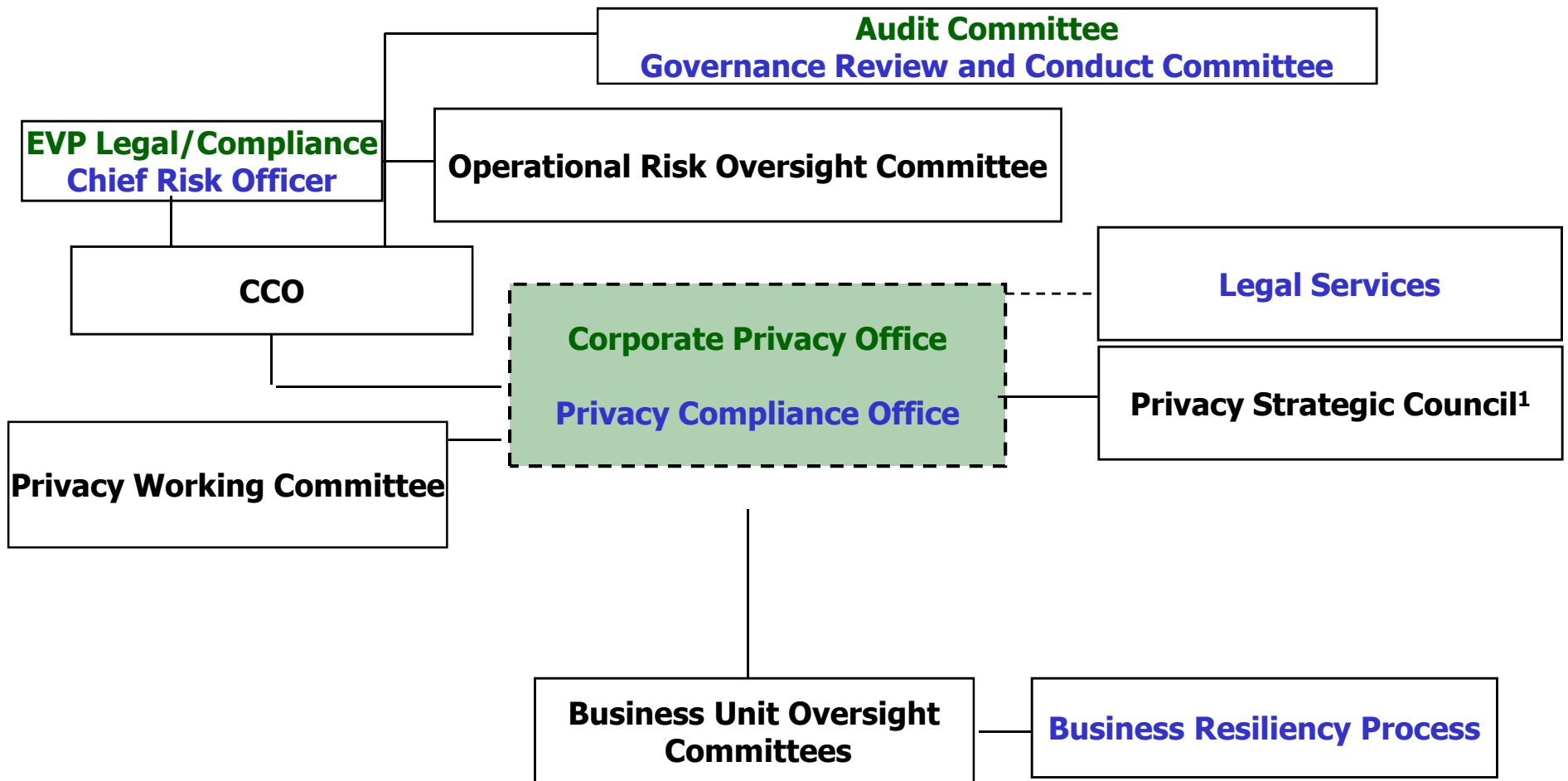
## 2. Global Privacy Governance Framework

- Establish governance team(s)
  - Schedule regular meetings
  - Report issues to senior executive
- Create committees/working groups
  - Ensure proper business representation
  - These can evolve according to need
- Establish organization-wide linkages (designates/ambassadors)
- Develop privacy value proposition and measure program effectiveness





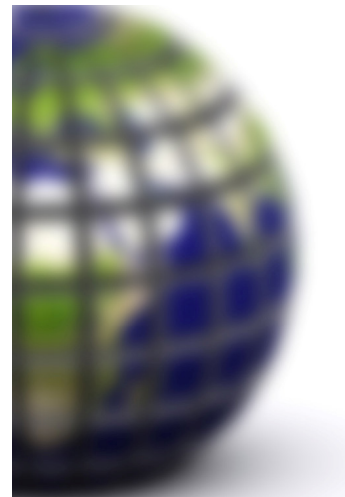
## 2. Global Privacy Governance Framework





### ***3. Policy, Standards and Communication***

- **Board Policy**
- **Corporate / Executive Policy**
- **Business rules, Guidelines & Standards**
- **Role based hands-on procedures**
- **Organizational Uniqueness**





## 4. Metrics to Measure Privacy Compliance

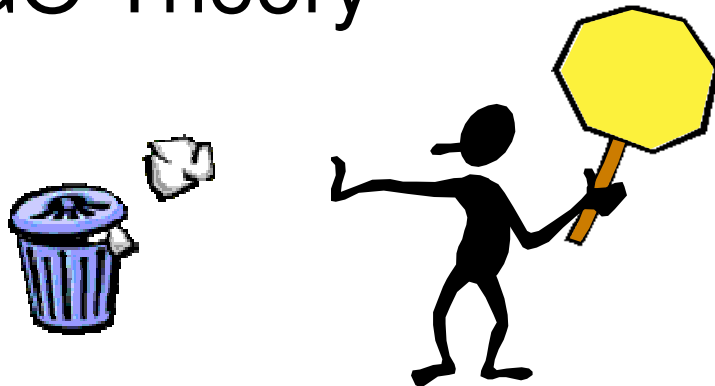
- Measuring Success Builds Awareness
- Generates Accountability
- Identifies and Defines Tolerance
- Balancing Act
  - quantitative vs. qualitative
  - delivering tangible results
  - accuracy is key
- Compliance and Risk Management





## 4. Metrics to Measure Privacy Compliance

- Solution and Strategy
- What Metrics Should Deliver
  - Completeness and reliability
- Define the Metrics to Measure
- Auditing to Compliance
- GIGO Theory

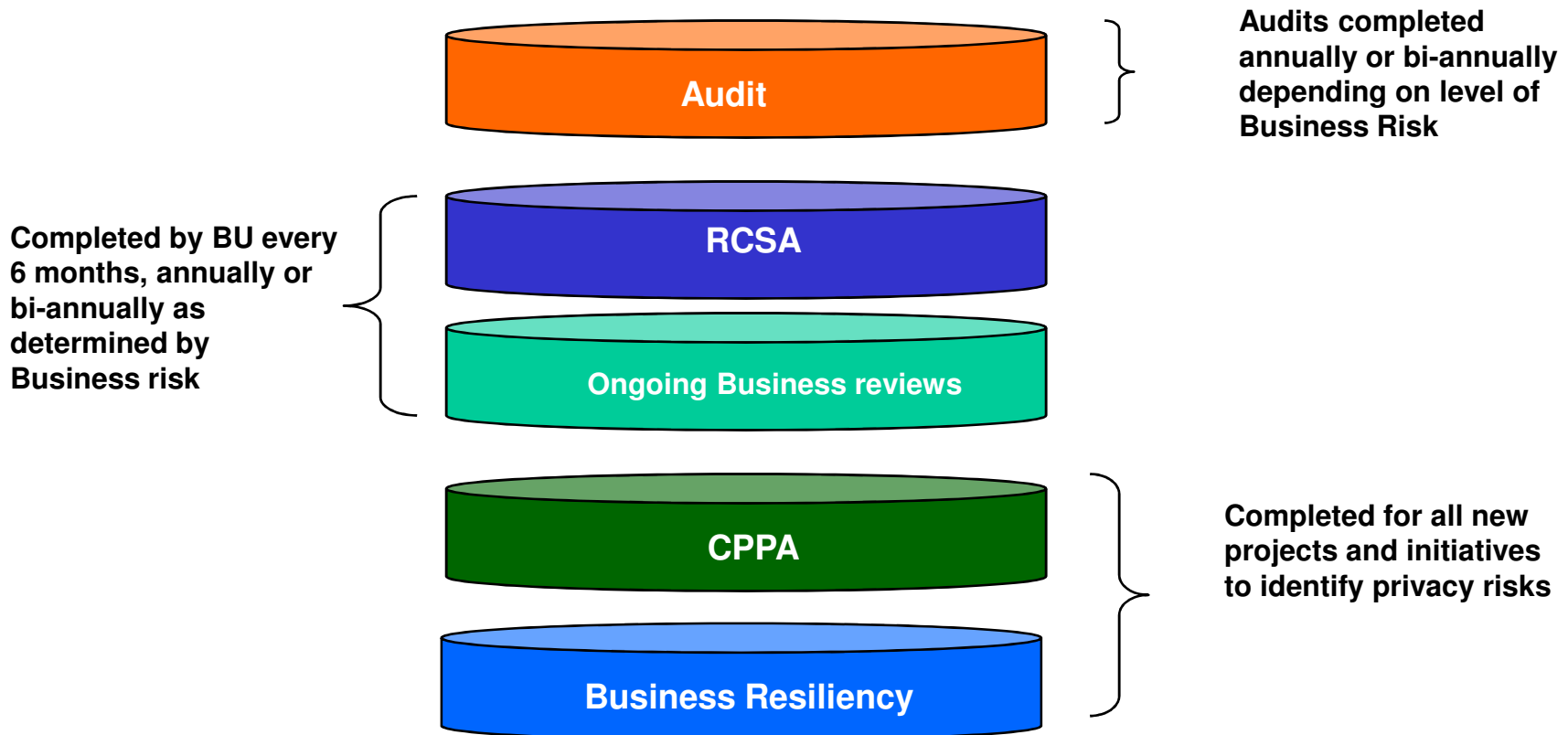




Privacy Incident Trends 08/09 Q2	Manual	System User Update Error	Automated Technical Data Error	3rd Party (contracted)	Ethics and Conduct	No ATB Involvement	Formal Access Request	Formal Correction Request	Not Well Founded	Un-Determined
MisDirected, Lost or Disclosed (breach)										
Misdirected, Lost (no breach)										
Consent Challenge										
Deliberate Breach, Destruction or Theft										
Formal Access Request Nothing Severed										
Formal Access Request Severed or Refused										
Request to Correct Applied										
Request to Correct Refused										
Request Pending										
Request Withdrawn /Abandoned										
Total Incidents	0	0	0	0	0	0	3	0	0	



*5. Monitoring : Privacy Risk Assessment: a layered approach*



- The Privacy component of the RCSA is a compliance measure to help BUs identify risks or exposures within their businesses and ensure compliance with PIPEDA and the Privacy Code



**5. Monitoring : Privacy Risk Assessment: a layered approach**

*Identifying Privacy Risks*

<b>Risks</b>	<b>Things to Consider</b>	<b>Processes and Controls</b>
<b>Breach of customer information</b>	<ul style="list-style-type: none"> <li>•Are your processes built around faxing? Emailing? Transmission of data?</li> <li>•Is customer information out in the open?</li> <li>•Do you know what to do if a breach occurs?</li> </ul>	<ul style="list-style-type: none"> <li>•Implement electronic and physical communication policies and controls</li> <li>•Securely store all customer information held on BU premises</li> <li>•Established escalation protocols and ensure they are followed</li> </ul>
<b>3rd Party Vendor, agent and supplier relationships</b>	<ul style="list-style-type: none"> <li>•Have you performed due diligence to ensure vendors can meet the privacy and security standards</li> <li>•Do you ensure your contracts have privacy clauses?</li> </ul>	<ul style="list-style-type: none"> <li>•Security Assessments and onsite visits are conducted</li> <li>•Legal reviews all contract language</li> </ul>
<b>Unauthorized employee access or theft of information</b>	<ul style="list-style-type: none"> <li>•Is access to information limited and reviewed regularly?</li> <li>•Is customer information securely stored?</li> </ul>	<ul style="list-style-type: none"> <li>•Management deletes access when employees leave the department</li> <li>•Access to key information and records is controlled and authorized</li> </ul>



## ***6. Educate and Train By Role***

**Each and every employee is a potential privacy risk!**

- Competing priorities
  - Privacy compliance is a customer service opportunity
  - An absent customer is absent revenue
- Information overload
  - Understanding and apply legislative requirements and company policies
- Human nature
  - Ignorance is not bliss



## 6. Educate and Train By Role

- Train the people (users, doers, viewers)
  - Use on-line tool
  - customize the training by role
  - repetition and hands on sessions (RRS)
  - be flexible - work with the masses
- Incorporate train mandates (ie) employee orientation handbook
- Stay on top of trends and rules

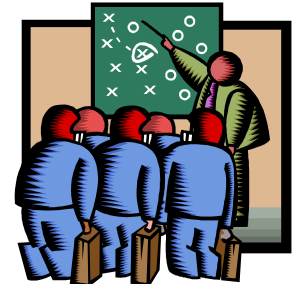




## 6. Educate and Train By Role

### Training – what is the goal?

To instill a **privacy mindset** in the workforce -  
changing the way employees perform job-related tasks  
that involve personal information  
and helping them understand how to apply  
regulatory requirements to their day-to-day work



Privacy should not be an afterthought, it should be embedded in staff behaviour and organizational culture



## ***6. Educate and Train By Role***

The “privacy mindset”

Privacy Smarts

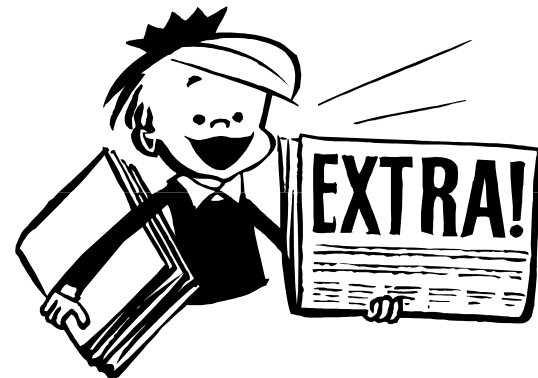
Privacy Skills

Privacy Sensitivity



***“It only takes one employee,  
breaking one privacy requirement,  
to get your company negatively plastered  
across major news outlets as an organization that  
can’t uphold privacy and security best practices.”***

*Source: Privacy Council Inc.*





***“Compliance and the right to privacy are not obstacles or necessary evils... they are an opportunity”***

***“An opportunity to leverage success measures to build a business culture with core values”***



## The Tool Box

Creating a tool box for business units and employees is key



Governance Framework

Policies and Standards

Metrics

Monitoring

- Leverage compliance and internal audits
- Ongoing business reviews
- Adjust training address trends and causes
- RCSA
- Privacy Impact Assessment / Business Resiliency



Training

- Online course designed by role
- Complaint handling guide and situational FAQs
- Easy to find privacy intranet resources



**Bank Financial Group**

**ATB Financial**

*Where there's a way*

***Questions...***

