



Evolving Privacy

The Need for Change in Privacy Administration

Alec Campbell



Trends (Actual and Hoped-For)

- Regulatory compliance
- Privacy and security
- The role of the privacy officer
- Privacy impact assessments
- The role of audit
- Privacy commissioners
- Training and Awareness
- The challenge of new technology
- The way ahead

Privacy and Regulatory Compliance

- Disclosure Forces
 - Public security legislation
 - Breach notification
- Retention Forces
 - E-Discovery
 - Civil litigation
 - SOX and C-SOX

New Technology

- Technology risks to privacy
 - Web 2.0
 - Social networking (Facebook, LinkedIn, etc.)
 - Viral marketing
 - ‘Cloud’ computing
 - RFID and other chip technologies
 - Passports, ‘enhanced’ driver’s licenses, etc.
 - Surveillance – physical and network
 - Audio, photo, video
 - Network activity – eg. Deep packet inspection
 - Workstation activity – keyloggers, parental controls, etc.

Privacy and Security

- For years we have said “Privacy and security are different”
 - True, but can be misleading
- Need for better integration of privacy & security
 - Balance may have to shift for some applications, e.g.,
 - National security – privacy diminished (but don’t overdo it)
 - Customer convenience – security diminished (but don’t overdo it)
 - Health care – both privacy & security may be diminished in emergencies
- Must achieve the right balance

Privacy and Security

- Privacy legislation should be more specific about security requirements
 - Embed security standards references (e.g. ISO/IEC 27002) into privacy legislation, allowing for future standards revisions.
 - Better specify circumstances in which security considerations may be allowed to diminish privacy obligations.
 - “Adequate security safeguards” is not enough.
- Privacy and security officers need to be joined at the hip, or even be the same person.

Privacy Standards

- Legislation tells you what to do; standards tell you how to do it
- Privacy has legislation but no standards; security has standards but no legislation
- Both privacy and security need both legislation and standards
 - Privacy legislation should specify security requirements
 - Development of privacy standards should be a priority for commissioners in concert

Commissioners

- Order Making Commissioners:
 - Prompt investigations and orders
 - Justice delayed is justice denied
 - Publish all orders and investigation reports online
 - Update practice notes and guidelines to reflect recent orders and trends
- Ombudsmen Commissioners:
 - Seek order making power!
 - Identify parties to investigations whenever possible
 - Publish all investigation results online

The (Chief) Privacy Officer

- Must *lead* privacy but not *do* privacy
 - CPOs should *not* be doing PIAs
 - And role of PIA should diminish – see later slides
 - Develop & maintain privacy policy...
 - ... but the whole organization must implement privacy policy
 - CPO monitors compliance and risk (review and audit)
 - Support from internal audit
- Must collaborate closely with security & risk management
 - CPO and CSO need to be in lockstep
 - If risk management unit exists, collaborate with them, too

Privacy Impact Assessment

- Traditional PIAs are not very effective
 - Time-consuming, expensive
 - Seen as impediment to business outside CPO office
 - Require scarce privacy expertise to do and to interpret
 - Often poorly done, or not done at all
- PIAs must change
 - Multi-stage processes
 - PIA "tools" – checklists, spreadsheets, etc.
 - Focus on areas of identifiable privacy risk

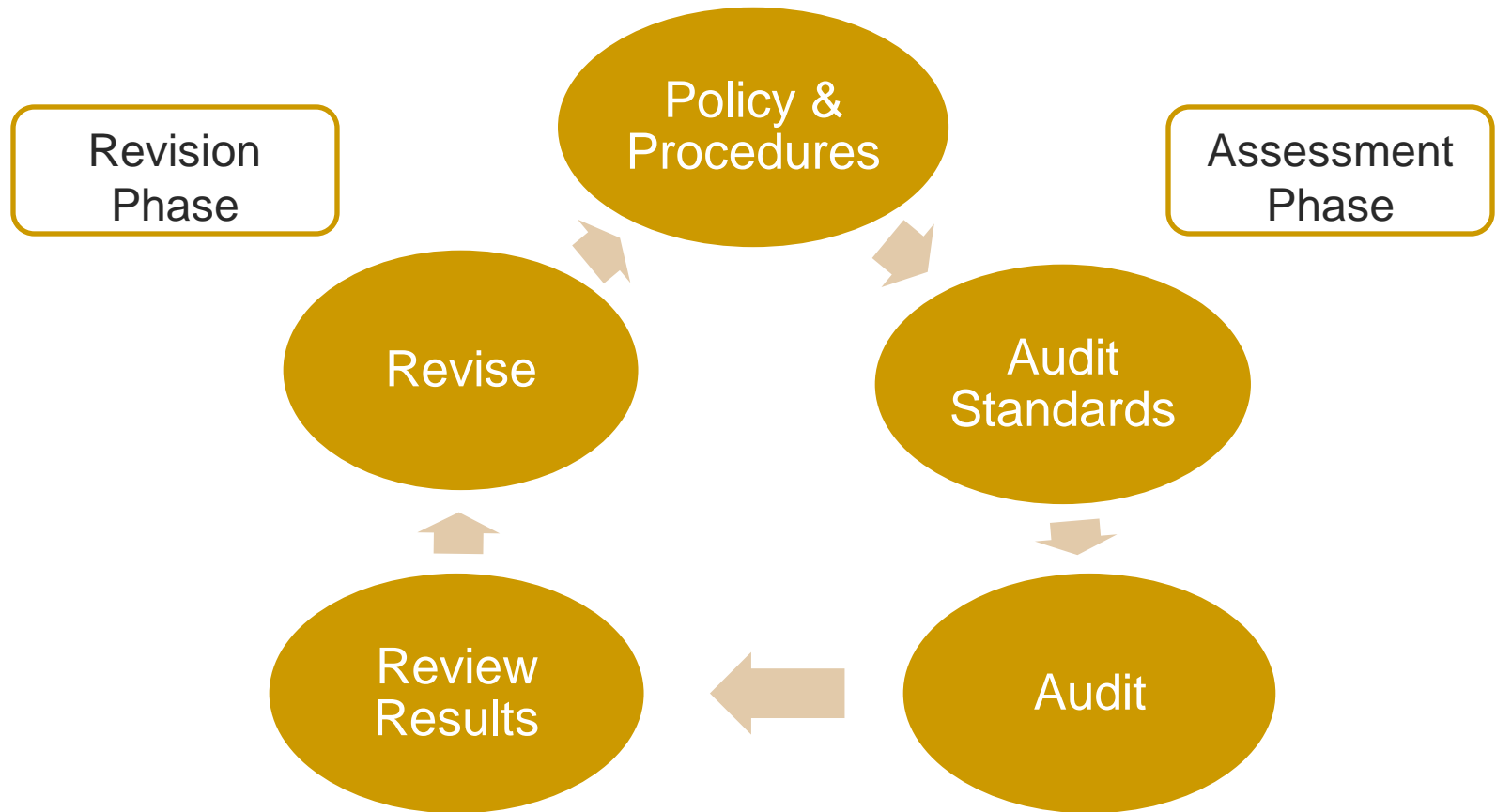
Audit Functions

- Privacy assessment should be replaced by privacy audit in a privacy-mature organization
 - Develop strong privacy policies and procedures
 - Use audits to monitor compliance and effectiveness
 - Integrate privacy and security audit functions
- CPO develops policy, procedures
- Auditors conduct audits
 - Use internal audit unit if it exists
- In some cases, less formal policy compliance reviews may be sufficient

Privacy Audit Frequency

- Privacy audits should be on a regular annual cycle
 - Every business unit audited at least every three years
 - So one-third of business units each year
- Any business unit that has a breach should be included in the next audit
- Audit detail should reflect the amount and sensitivity of personal information involved – varied audit levels
 - GAPP is a sound basis, but not the only one
- Include security at an appropriate level of detail

Privacy Audit Cycle



Training and Awareness

- Classroom training is not very effective
 - Point in time
 - Infrequent delivery
 - Dependent on trainer skill
 - Long lag times between sessions
 - Limited metrics available to assess effectiveness
 - Usually hesitant to use exams
 - Satisfaction surveys are a poor proxy for effectiveness

Training and Awareness

- Online training is better if done right
 - Need feedback mechanism for questions and discussion
 - VoIP, email, online chat, etc.
 - Needs to be well designed and engaging
 - Should be professionally designed if possible
 - Use combination of delivery formats – text, graphics, video, audio
 - Can be supplemented by a live trainer in an online meeting format
 - Requires more investment and preparation
 - Multiple organizations can collaborate

New Technology

- Technology for privacy administration
 - Automated assessment and audit tools
 - E-discovery tools
 - Electronic document management
 - Email management
 - Privacy architecture
 - Improved and easier encryption

The Way Ahead

- Improved privacy policy and procedures
- Better integration of privacy and security
- Privacy audit gradually replaces PIAs
- Improved employee training and awareness
- Technology becomes a tool for privacy administration, not just a risk factor

Questions?

Alec Campbell
President, Excelsa Associates Inc.

alec@excelsa.info

780-945-0123

www.excelsa.ca