Why Re-Invent the Wheel: How to Use ISO Auditing Techniques for Privacy Compliance
Q & A

• Show of hands – how many of you have attempted to audit organizational privacy compliance via a review of their privacy management program?
• What tools did you use?
• How many felt the credibility of their privacy audit was linked to the individual auditor and therefore somewhat subjective?
• How many believe – if they undertook the same audit – they would get the same result – if conducted by a different individual/company?
ISO 19011:2011 – GUIDELINES FOR MANAGEMENT SYSTEMS AUDITING

• Revised version was published in November of 2011. This version cancels and replaces the first edition (ISO 19011:2002)

• ISO 19011 – Guidelines for management systems auditing is an international consensus standard applicable to ALL management system audits...

• The revised ISO 19011 is an international consensus standard now applicable to ALL management audits:
  – Including a Privacy Accountability Management Program

• It is a voluntary standard made up of guidelines
SO WHAT IS THE “BIG DEAL”? 

• “Credibility” & “Standardization”
• Through an evidence-based approach we want to prove “accountability” demonstrating an organization’s Privacy Management Program’s capacity to comply with regulatory requirements / industry best practices
• “Adequacy” = Agreed Privacy Standard
A **management system** is the framework of **policies, processes and procedures** used to ensure that an **organization** can fulfill all tasks required to achieve its objectives.

The question as it relates to Privacy will be addressed by my colleague...
“Systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.”

- (ISO 19011:2011 3.1)
## TYPES OF AUDITS

<table>
<thead>
<tr>
<th>Internal auditing</th>
<th>External auditing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Supplier auditing</td>
</tr>
<tr>
<td>Sometimes called first party audit</td>
<td>Sometimes called second party audit</td>
</tr>
<tr>
<td></td>
<td>Third party auditing</td>
</tr>
<tr>
<td></td>
<td>For legal, regulatory and similar</td>
</tr>
<tr>
<td></td>
<td>purposes</td>
</tr>
<tr>
<td></td>
<td>For certification (see also the</td>
</tr>
<tr>
<td></td>
<td>requirements in ISO/IEC 17021:2011)</td>
</tr>
</tbody>
</table>
ISO 19011 AUDIT PROCESS

Management System Audit

Criteria → Evidence → Finding → Conclusion & Report

eCompliance
New Accountability Guidance: Regulatory Expectations for Privacy Management Program

“Evidence of an effective privacy management program assists Regulators in determining whether or not the organization has reasonable safeguards in place, and has complied with accountability requirements under applicable law”\(^2\)
EVIDENCE-BASED APPROACH

Clause 4: Principles of Auditing
6 PRINCIPLES OF AUDITING

- **Integrity:** the foundation of professionalism
- **Fair presentation:** the obligation to report truthfully and accurately
- **Due professional care:** the application of diligence and judgement in auditing
- **Confidentiality:** security of information
- **Independence:** the basis for the impartiality of the audit and objectivity of the audit conclusions
- **Evidence-based approach:** the rational method for reaching reliable and reproducible audit conclusions in a systematic audit process
ISO 19011 AUDIT PROCESS

Management System Audit

Reliable and Reproducible audit conclusions can only be achieved through EVIDENCE

Criteria → Evidence → Finding → Conclusion & Report
Evidence-based approach: the rational method for reaching reliable and reproducible audit conclusions in a systematic audit process

Audit evidence should be verifiable. It will in general be based on samples of the information available, since an audit is conducted during a finite period of time and with finite resources. An appropriate use of sampling should be applied, since this is closely related to the confidence that can be placed in the audit conclusions.
EVIDENCE-BASED APPROACH BROKEN DOWN:

• Rational (Logical) method:

Methods of collecting information include the following:

– Review of documents, including records;

– Interviews; and

– Observations.
EVIDENCE-BASED APPROACH BROKEN DOWN:

• Reliable:
  – Relevant: *to the audit objective and criteria*
  – Sufficient: *sample size appropriate to evaluate conformance to criteria*
  – Verifiable: *documented evidence gathered - audit evidence leading to audit findings should be recorded.*
EVIDENCE-BASED APPROACH BROKEN DOWN:

• Reproducible:
  – Audit findings need to be clear credible and based on a method that if applied by others would result in the same finding/conclusion
RELIABLE & REPRODUCIBLE
RELIABLE & REPRODUCIBLE
SYSTEMATIC AUDIT PROCESS

• Evidence-based approach: the rational method for reaching reliable and reproducible audit conclusions in a **systematic audit process**

• Audit principles, procedures and methods: knowledge and skills in this area enable the auditor to apply the appropriate principles, procedures and methods to different audits, and to ensure that audits are conducted in a **consistent and systematic** manner - Clause 7.2.3.2 (a)
EVIDENCE-BASED APPROACH BROKEN DOWN:

- Practical “Conundrum” of Reproducibility:
  - Audit findings need to be clear credible and based on a method that if applied by others would result in the same finding/conclusion
  - “Reproducible”? (in a Standard Format)
  - This is probably the biggest complaint from companies that employ ISO Auditors; i.e. inconsistency in findings and conclusions
RELIABLE & REPRODUCIBLE

Auditor

Method

Organization

Result

Harry

Sally
RELIABLE, REPRODUCIBLE AUDIT CONCLUSIONS

• Can only be achieved through a standardized evidence-based approach
RELIABLE & REPRODUCIBLE

Auditor

Standard Audit Protocol and Method

Organization

Result
EVIDENCE VERSUS EXPERIENCE

- Evidence
- Experience
Integrity: the foundation of professionalism - not basing findings on evidence will be irresponsible.

Fair presentation: not basing findings on evidence, takes away from the objectivity of the audit findings and brings the subjectivity of the auditor into play.

Due professional care: Confidence is placed in auditors by the auditee and other interested parties to exercise due care – not substantiating findings with verifiable evidence is not acting with due care.

Evidence-based approach – the lack of evidence will clearly and obviously be against this principle.
Privacy
Compliance
Accountability

ISO 19011:2011
THE ACCOUNTABILITY BUZZ

• Accountability – OECD and APEC
• Article 29 – EU Accountability
• CSA Model Code
• Ongoing Program Assessment and Revision
• Getting Accountability Right
  – Regulatory Expectations for Privacy Management Programs
REGULATORS’ RIGHT TO AUDIT

• “Audit” as defined by various privacy legislation
  “audit” means a financial, clinical or other formal or systematic examination or review of a program, activity or other matter under this Act;

• Regulators’ power, authority, responsibility

• Canadian Privacy Legislation
  – Personal Information Privacy Acts, Health Information Acts, Freedom of Information Protection Acts (see reference page), Personal Information Protection and Electronic Documents Act
### RELIABLE & REPRODUCIBLE

<table>
<thead>
<tr>
<th>Auditor</th>
<th>Standard</th>
<th>Organization</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Audit Protocol and Method</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Reliable, Reproducible, Verifiable
- Credible, Measurable and Evidence Based
- Evaluation of Privacy Program Compliance
- Quantifying the same set of rules against the same standards
- Due diligence
HITTING THE TARGET

In house ad hoc reviews

Privacy Impact Assessments

Standardizing Auditing

Out house undertakings
NEED TO STANDARDIZE

• Q & A

• Evidence based approach
  – demonstrates conformance AND compliance

• Engaging the right people, the right lines of business, knowing how to ask the right questions
  – producing qualitative and quantitative results = reliability, integrity, due diligence
ACCOUNTABLE ORGANIZATIONS

• Are able to:
  – Demonstrate a comprehensive up-to-date privacy management program
  – Demonstrate compliance with applicable privacy legislation
  – Demonstrate program controls
  – Conduct assessments and report privacy program controls (metrics)
WE SAID THIS SESSION WILL

• Help you discover how ISO 19011:2011 delivers evidence-based auditing
• Show why it is important to engage the right people in the right lines of business, how standardizing the right questions can deliver qualitative and quantitative audit results.
• Help you understand that compliance accountability can be properly audited.

What we said you would take away?

• Insight on how industry standard auditing will produce qualitative and quantitative results, and that if standardized auditing is applied, regulators’ privacy program accountability requirements can be demonstrated...measurable...and reliable.

In Summary...
ISO 19011 DEMONSTRATES ACCOUNTABILITY REQUIREMENTS

• ISO 19011:2011 techniques are evidence based
  – “Evidence of an effective privacy management program…” is what the Regulator’s want to see

• They are sufficient to evaluate and audit any program – even Privacy Management Programs to demonstrate compliance and accountability
APPLICABLE AND POSSIBLE
WHY REINVENT THE WHEEL?

- It is time to compare apples to apples
- Move away from individualized auditing methods
- Leverage existing standardized auditing techniques (ISO 19011:2011) that can produce evidence-based results to demonstrate privacy program accountability and compliance

Thank You…
Please complete your evaluations and
Please see us at the front if you have any more questions
YOUR TURN TO ASK QUESTIONS

If we haven’t answered all your questions, please visit us at booth #9
References:

1. www.privacyaccountability.com and www.ecompliance.com

2. GETTING ACCOUNTABILITY RIGHT WITH A PRIVACY MANAGEMENT PROGRAM:  
   http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.pdf

3. A FRAMEWORK FOR INITIATING AUDITS

4. UNDER SECTION 18(1) OF PIPEDA: http://www.priv.gc.ca/leg_c/frame/EnforcementTools/sec18_e.pdf AND  
   http://www.priv.gc.ca/leg_c/framework_e.asp

5. ARTICLE 29 DATA PROTECTION WORKING PARTY:  

6. 4. ISO 19011:2011:  
   ISO 19011:2011 - Guidelines for auditing management systems  
   www.iso.org/iso/catalogue_detail?csnumber=50675
subsection 18(1) of PIPEDA.

When events have occurred that indicate a risk of non-compliance with the Act, the Commissioner will review the information available to determine whether there are reasonable grounds to initiate an audit (i.e. whether there is credible evidence that supports a serious possibility that an audit would disclose a contravention or intended contravention of the Act.

- The Commissioner must exercise this discretionary enforcement authority in good faith;
- The Commissioner’s discretion must be exercised on the basis of a clear record of facts and analysis which exists at the time the audit is ordered;
- The information must be capable of being believed and the Commissioner must not be aware of any cogent reason for rejecting the information as lacking credibility; and,
- The Commissioner must be able to assert that, at a minimum, the information available is such that it could realistically lead auditors on a focused train of enquiry which would reveal systemic non-compliance with statutory requirements.
PRINCIPLE 1: Do factors exist, or have events occurred, which indicate a risk of non-compliance with The Act and/or the absence of sound privacy management practices?

This process involves the identification, analysis and validation of potential privacy issues associated with an industry, entity or program, and where possible, a preliminary review of the area’s major privacy management control functions. Issue analysis is generally conducted internally using information collected by the OPC through investigations and/or research, but may involve several interventions, including enquiries with management. Factors indicating the absence of sound privacy management practices may include, but are not limited to: credible media reports, the recommendations of parliamentary committees, contraventions revealed through whistle-blowing, incident investigations, the results of complaint investigations, entity or industry requests for review, the results of empirical studies or industry polls, other.

PRINCIPLE 2: Does sufficient and credible evidence exist to support a serious possibility that an audit would disclose an ongoing contravention of The Act?

Reasonable grounds testing involves the examination of information gathered during issue analysis activities, and the assessment of whether there are sufficient grounds to support the Commissioner’s use of discretionary authority under section 18(1) of the Act. Internally, the OPC establishes a clear basis for audit and ensures that a sound evidentiary threshold is used in arriving at such a determination.

PRINCIPLE 3: Given the results of issue analysis and reasonable grounds determination, what measures would best promote and encourage compliance and the use of sound privacy management practices? Is the area under consideration best addressed through an audit and is it amenable to audit?

Our Office recognizes that no single tool or instrument will best ensure compliance in all situations. For that reason, the Commissioner considers all means available, including audit, to encourage compliance and promote sound privacy management practices. The final decision to audit would be subject to numerous considerations not limited to: the nature of the case, the significance of systemic risks, the frequency with which the issue has been identified, the extent to which remedial action has been taken, the results and findings of completed or on-going privacy investigations, previous Office positions, other.

A record setting out the basis upon which the Commissioner’s decision to initiate an audit is made.