Working Group on Information Risk Management Practice

Meeting #5
Tuesday, July 14, 2015
Simcoe Hall President's Boardroom
2:00pm to 4:00pm

Regrets: S. Senese, H. Bohaker, K. Hannah-Moffat, D. Hutt

Co-Chair: M. Loeffler

This is a working meeting to discuss a framework of Standards, Procedures and Guidelines.

Agenda

1. Discussion of criteria to inform the adoption of a possible framework. Suggested criteria may include but is not limited to the following:

   a) **Auditable** – *Recognized by industry and third party auditors*
   b) **Maintained/Updateable** - *regularly updated to reflect changing technologies, conditions, and best practices.*
   c) **Non-biased** – *not promoted, established, or maintained by a single body that does not represent a cross section of industry.*
   d) Academically Recognized – *used / usable in academic settings*
   e) Recognized by the University Audit Committee
   f) **External Alignment** – *in use by organizations that the University of Toronto must interface with either in a business, academic, or regulatory context (e.g. Government of Ontario)*
   g) **Adaptable** - Capable of being adopted in part, initially, and leaving room to define unit-specific controls.
   h) **Broad Scope** – Covers as much information security and information risk management under an umbrella of common structure, wording, and internally consistent references.

2. **Consideration of a Specific Framework**
   Please refer to the "crosswalk" document and Educause report, ISO/IEC 27002 2013 Information Security (attached)

   Further supplementary information to clarify the scope of ISO standards guidance *(pdf docs attached)*:
   ISO 31000 Risk Management
   ISO27001-21008
   ISO 27035 Incident Managment

   Documents also available online at: http://guides.library.utoronto.ca/c.php?g=250983&p=1672574 - 9791552

3. **Consideration of Specific Standards and Procedures as a Means to Implement a Framework**
   a) Faculty of Medicine Baseline *(document attached)*