DRAFT AGENDA

Working Group on the Implementation of Information Risk Management Practice

First Meeting – 24 March 2015

1. Membership and Introductions

2. Terms of Reference

    a. Goal

        "To produce, in collaboration between the University's divisions and ITS, a set of information risk management Guidelines, Standards, and Procedures that can be used across the University in support of delivering on the mandate of an institutional information security policy, or better manage information risk in anticipation of a policy."

    b. Proposed Process

    c. Deliverables

3. What the Working Group is NOT

- A policy committee
- A technical committee
- Theoretical
- Prescriptive

4. Proposed Meeting Schedule

- Meeting #1 - Tuesday, March 24,2pm to 4pm, Simcoe Hall, Governing Council Chambers
    - *Introductions and planning*
- Meeting #2 - Tuesday, April 21, 10am to Noon, Simcoe Hall, Governing Council Chambers
    - *Review work already done at the University in the area of information risk*
- Meeting #3 - Tuesday, May 26, 10am to Noon, Simcoe Hall, President's Boardroom #132
    - *Review industry standards of information risk management*
- Meeting #4 - Wednesday, June 24, 3pm to 5pm, Medical Science room #3175
    - *Identify and review successful IR initiatives at comparable academic institutions*
- Meeting #5 - Tuesday, July 14, 2pm to 4pm Simcoe Hall, President's Boardroom #132
    - *Produce a set of standards and procedures that can be adapted by divisions*
- Meeting #6 - Wednesday, August 19, 3pm to 5pm, Simcoe Hall, President's Boardroom #132
    - *Develop proposed Terms of Reference for the Information Security Council (ISC)*

5. Proposed Principles and Definitions: Risk Management (see attached)

6. Reading Package

Proposed Principles and Definitions: Risk Management

A. Risk Itself

- Risk is the possibility of something bad (or good) happening, depending on the decisions one makes, in a given (and possibly very complex) context
- Risk must be transparent—risk management decisions cannot be made if risk is not known
- Risk must be coherent—within an organization, risk cannot be transparent if different definitions or metrics are used to measure it
- Risk must be managed—it's accepted or not in proportion to the risk an asset owner is prepared to accept

B. Risk Management

- Risk management is about increasing the likelihood of achieving value and avoiding loss
- Risk management is about taking opportunities as well as avoiding negative consequences
- Risk management must support the goals of the organization: risk management doesn't exist in a vacuum, it must bring value and be relevant to everyone
- Risk management must be measurable: relative or otherwise, risk management can't be shown to bring value if it can't be measured
- Risk management must reflect the context in which the organization operates: its strategic goals, contractual, legal, and ethical obligations

C. Risk in the Organization

- Assets at risk must have the same value throughout the organization (for example, PII or PHI)
- Risk management activities need to be accountable and repeatable—they need to be reported up to the top of the management hierarchy, reviewed, and acknowledged.
- Risk management activities need to be reviewed regularly and revised as necessary, to determine if we are doing too little, too much, and whether we are doing the right things.
- The goal is to know whether risk is increasing or decreasing; not just the absolute value

D. Information Security and Information Risk (ISO 27001/2/5)

- Information security is defined as the preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.
- An Information Security Management System (ISMS) is a set of policies, processes and working arrangements that help an organization exercise a degree of control to provide assurance of the organization's confidentiality, availability, and integrity.
- It is not our intention to be ISO 27001/2/5 certified. Our goal is simply to choose a reasonably comprehensive risk-focused standard against which to measure ourselves and our progress. In addition, we are entitled to take parts from 27001/2/5 as we're ready to—we don't have to adopt it in whole, nor at depth.

Reading Package: Contents