Committee Name: Information Security and Privacy Risk Council

Date of Meeting, Time, Location: 8/9/2011, 1-3 PM, Poplars 017

Attendees in person: Tom Davis (Chair), Michael Gardner, Joan Hagen, Jeff Lambright, Merri Beth Lavagnino, MaryFrances McCourt, Dan Rives, Jim Kennedy, Chris Viers, Eric Cosens (staff), Sherrie L. Denney (staff), Scott Wilson (staff),

Attendees via video: Philip Cochran, Marcia Gonzales, Joe Scodro, Doug Wasitis

Attendees via audio: none

Absent: Kim Milford

Agenda/Discussion

1. Call to Order and Approval of 9/27/11 Minutes
   a. Previous meeting’s minutes were received and approved.
   b. Discussed feedback from the last meeting and noted there will be an opportunity to provide feedback after all meetings.
   c. Members suggested that a pre-meeting tickler be sent to the members to review meeting handouts and minutes, one day prior.

2. Presentation – “Risk and Risk Assessments” – (Gardner)
   a. Michael shared the Internal Audit perspective on risk and risk assessment for the benefit of the Council, and to build a common understanding and vocabulary surrounding risk.
   b. Risk assessment, risk treatment, and the promotion of effective and efficient use of resources are vital from an Internal Audit perspective.
   c. A Definition of Risk – things that can go wrong.
   d. A Definition of Risk Management – things that keep things from going wrong.
   e. Overview of the COSO Risk Management Framework – key take away - risk management activities have to span all levels of an organization and all its activities.
   f. The State of Risk Management at IU - no formal integrated, coordinated, risk management process is currently in place at IU although risks are managed within silos (i.e. functional, dept, campus, school, etc.). How are risks that cross functional areas, depts., campuses, schools, etc. being addressed?
   g. Risk Management Activities & Tools from Internal Audit perspective – Internal Audit addresses risks through identification (using org charts & objectives, risk assessment
templates, and rating risk factors and descriptions), assessment, and mitigation. Audits are performed to assess the effectiveness of mitigating controls and residual risk.

h. Suggested applications for the IS&P Risk Council:
   i. Identify “significant” risks.
   ii. Assess those risks (i.e. likelihood, impact, speed of onset, mitigations, preparedness, residual risk).
   iii. Govern management of risks.

3. Information Security and Privacy Program – Overview of Domain 1: Risk Assessment and Treatment – (Davis)
   a. Tom gave an overview of the first domain of the IS&P Program on Risk Assessment and Treatment and asked that council members review the domain and provide feedback, especially on any noted gaps, for the next meeting.
   b. The intended audience is information/technology managers, key business function owners/representatives, compliance people, researchers, and auditors.
   c. Remember that one purpose of the program is to serve as a resource to document how certain compliance objectives are being met.

4. Enterprise Risk Management (ERM) Project Overview – (Lavagnino)
   a. Merri Beth gave an update and overview of the ERM project due to its relationship to our Domain 1.
   b. There has been increasing interest/pressure from Trustees to look at risk. President McRobbie and Dottie Frapwell are driving the initiative.
   c. The project Executive Committee consists of: John Applegate, Karen Adams, Mark Bruhn, Dottie Frapwell, Jennifer Kincaid, and Doug Priest.
   d. Huron Consulting Group was asked to help us study the state of ERM at IU and an overview of the Huron study is on the Oncourse site.
      i. Huron interviewed 70-80 people at IU about risk mgmt.
      ii. Huron is identifying our 5 top risks.
      iii. Huron didn’t find any significant risk management gaps, which answered the important question “what don’t we know”?
      iv. A collaborative model for addressing enterprise risk management at IU is being proposed.
   e. Gardner pointed out that most effective ERMs aren’t associated with a particular function, but are rather “above the fray” as it were and report to top executives.

5. Policy Advisory Council – (Lavagnino)
   a. Merri Beth briefly presented about our information security and privacy policy hierarchy, and the university-wide Policy Advisory Council, which inform our Domain 2 activities.
b. Jenny Kincaid – Dir of Policy Administration and Applegate’s chief of staff, is chairing the Policy Advisory Council. It is working to organize policy activity for the university.

c. A handout was provided to attendees that included the charge and membership of council (reps from every campus and every VP’s area/office).

d. The charge of the council is to assist with the “further improvement of the policy development process; the review and distribution of new or revised policies where appropriate; and the improvement of the structure and organization for maintaining, updating, and accessing policies” – for university-wide policies.

e. The council is working to develop a “policy on policies,” a standard policy template, a tool that would help us organize/index university policies (might be ready in the next couple of months), a system of taxonomy/terms, an a-z index, a category index, and search function for policies, and a one-sentence overview of each policy when a user “hovers” over the policy link.

f. It was noted that authority for university-wide policy rests with the Board of Trustees, President, Vice Presidents, and Faculty Council.


a. Eric gave an overview of the second domain of the IS&P Program on Policy and asked that Council members review the domain and provide feedback, especially on any noted gaps for the next meeting. Also note the difference in format between Domain 1 and Domain 2. Which do the council members prefer?

b. Remember, the program domains are based on ISO standards but have been tweaked and added to, in order to address any weaknesses in ISO coverage.

c. This purpose of the policy domain is not to address specific policies, but rather to address the governance structure and the process by which policies are developed, reviewed, approved, documented, administrated, and communicated.

d. Briefly discussed process by which Information Policies are developed including identification of need, feedback/input from a broad group of stakeholders, and approval.

e. We glanced at a list of the gaps that we know of, such as the need for a communication plan for new policies. For example could we use Onestart and other enterprise tool menus and popups to inform employees of new or critical policies? A process needs to be developed for using such tools to promulgate policy information.

7. Round Table Discussion of Risk and Compliance as it Relates to Each Member’s Sector/Area of Responsibility – (all)

a. Each member talked about risk and compliance as related to their sector/area of responsibility.
b. Jeff Lambright is concerned about donor information, and what safeguards are needed when it’s released “internally” to employees with a need to know within the university.

c. Chris Viers is concerned about compliance with regulations surrounding visiting foreign students, employees, and faculty, including Department of Homeland Security, Department of Labor, and Department of State. Interestingly most of these require IU to report about people, rather than regulate how to protect their information.

d. Jim Kennedy is concerned about the increase of regulations that affect the university that are often tied to financial aid. He is concerned with HEOA, Program Integrity Rules, Gramm-Leach-Bliley, Red Flags, consumer banking, etc.

e. Joan Hagen is concerned with electronic storage/transmission of information, payroll compliance/sensitive data, controls over disbursements, tax compliance, new regulations, sensitive data, reporting/distribution of information, and federal costing/procurement regulations. More and more activities involve electronic methods.

f. Marsha Gonzales is concerned with research related regulations, NRC regulations, export controls, HIPAA, OHRP, Medicare, Medicaid, lab animal regulations, sunshine act, FDA, fraud and abuse statutes, research misconduct, radiation safety, NIH regulations, and conflict of interest (NIH and IN statute), etc.

g. Joe Scodro and Michael Gardner are concerned about everything.

h. Doug Wasitis has an institutional focus, particularly as federal regulations are developed and the university has an opportunity to provide input during that process.

i. Phil Cochran [we had difficulties hearing Phil – can you please provide us a phrase or two to add here?]

j. Dan Rives is concerned with anything that relates to human resources processes. Hiring (EEO rules – age, ethnicity, gender, etc.), form I-9s, e-verify (lots of compliance issues w/these), SSNs, intersection with open records law, fair labor standards act (hours worked records requirements), HIPAA intersection with our medical plans & associated relationships/agreements with sponsors of plans, and SEC regulations with respect to retirements plans were all highlighted by Dan as examples.

k. Mary Frances is concerned with compliance issues as they related to debt, private user tax, revenue processing, banking operations, bursar & student loan initiation, SEC, and PCI-DSS.

8. Wrap-up and Next Steps – Feedback on meeting was called for. Meeting was adjourned.

**Action Items/Assignments**
A1: COMPLETED. Philip Cochran and Joe Scodro volunteered to identify a central, face-to-face meeting location for IUPUI attendees. Determined that Phil was going to continue to join from his office and the admin assistants for Joe and Marcia are handling obtaining a room for them.

A2: COMPLETED. Delegates were requested to complete the meeting feedback survey and send to Merri Beth.

A3: Review Domain 1 – provide feedback and identify gaps – (all).

A4: Review Domain 2 – provide feedback and identify gaps – (all).

A5: Look at the different formats of Domain 1 and Domain 2 (paragraph vs. table). Which format do you prefer? (all)

A6: Send a pre-meeting reminder about 24 hours before each meeting to the council members to review meeting handouts and minutes. (co-chairs)

Parking lot

P1. Discuss how to best publicize this Council.

P2: Discuss how to improve communication about new policies, critical policies, etc., for example, could we use a Onestart popup?

P3: Discuss how we avoid losing valuable historical data which is only in employee’s personal email accounts.

P4: Discuss how risks that cross functional areas, depts., campuses, schools, etc. are being addressed.

P5: Suggested Risk Domain applications for the IS&P Risk Council:

   i. Identify “significant” risks.
   ii. Assess those risks (i.e. likelihood, impact, speed of onset, mitigations, preparedness, residual risk). Use an agreed upon process and tool.
   iii. Govern management of risks.

Attachments

See Oncourse for meeting handouts.

See IS&P Program at - http://protect.iu.edu/privacy/program