Committee Name: Information Security and Privacy Risk Council

Date of Meeting, Time, Location: 9/19/2011, 2-4 PM, Poplars 017, Video Bridge 223739

Attendees in person: Tom Davis (Chair), Merri Beth Lavagnino (Co-chair), Eric Cosens (staff), Kim Milford, Dan Rives, Jim Kennedy, Jill Schunk (guest), Doug Wasitis, Jeff Lambright, Joan Hagen

Attendees via video: Marcia Gonzales, Joe Scodro

Attendees via audio: Mike Gardner

Absent: Philip Cochran, MaryFrances McCourt, Chris Viers

---

**Agenda/Discussion**

**Call to Order and Approval of Minutes** – The meeting was called to order. Minutes from the previous meeting were approved as submitted.

**Old Business and New Business**

- It is understood that going through and reviewing the program domains will take some time, but that it is foundational to the council’s understanding of the program. We will try to speed these overviews up as much as we can (may require some off-meeting reading/review). It was proposed that the council continue meeting every 4-6 wks until we get thru domains. There were no questions or objections.
- Coordination with other groups – The IS&P Risk council will coordinate with other university groups as appropriate (ex. CDS, BI, PAC, ERM, etc.). Internal Audit is involved (Gardner is a member and presented on risk management at the last meeting). Kim Milford is acting as liaison with the Committee of Data Stewards. If council members know of/or learn of other groups with which the council should coordinate, please let the chair know. No other groups were mentioned during the meeting.

**Domains 1 & 2 – Review and Prioritization of Gaps**

- During last meeting domains 1 and 2 were reviewed (Risk Assessment & Treatment, and Policy Administration respectively). Merri Beth sent an email as a reminder on things to do with those (ex. identify gaps), and for us to compare formats of domains 1&2 and let us know which is preferred.
- Comments on Domains 1 & 2 were called for: Wasitis prefers the domain 2, graph/table format rather than the prose. Hagen agreed that it flows better and makes it easier to get the structure. Milford suggested that the table format will make it easier to track where we are in terms of implementation. There was consensus on the table format, although Milford questioned whether the subject matter of all the domains would lend itself to table format. Some may not.
• General thoughts/comments about the domain content were sought: Wasitis pointed out the “consideration of cost/benefit” language in D1, under the “Treating Security and Privacy Risk” section, 3rd bullet point, and wondered how this language intersected with required compliance (i.e. situations where cost/benefit is moot). Maybe some clarification would be good here, such as, “certain safeguards must be implemented due to compliance requirements,” or “many factors MAY (must) be considered”, or strike first 2 words – were all suggested. Lavagnino will work on the language. Scodro, with reference to the second set of bullet points in D1, brought up question of whether risk can really be transferred. Milford pointed out that our risk approach for a particular risk may vary over time. Gardner commented that this is pretty appropriate/standard language in the risk management profession. Scodro asked whether audit reports are shared with state. Gardner says that audit reports are routinely reviewed by the state board of accounts. The risk transfer language also appears in the risk treatment section of D1.

• Domain 2 Comments: Scodro asked, “Who’s going to read all this stuff besides us?” Lavagnino pointed out that part of the purpose of this is to provide documentation for external audits, etc. - to show we are compliant with x, y, z requirements. Schunk asked if the program might lead to the development of policy that doesn’t yet exist. Lavagnino confirmed that the gaps would suggest future policy development. Gonzales added that sometimes research sponsors/contracts want examples of existing policy. Having a program documented like this to point them to will be helpful.

• GAPS Exercise: council members paired up for 5 minutes to discuss the D1&2 gaps they came up with and to identify the top 3 gaps. The results were turned in and will be compiled. The gaps list will be ongoing, and exercises like this will help us prioritize our work to address the gaps. Gardner was participating via audio only and will provide his gap feedback after the meeting.

Domains 3 Overview – Organization

• Lavagnino reviewed domain 3 with the council. One gap is the lack of a real roles/responsibility policy. Another gap is the lack of a definition of “internal” vs. “external.” What’s an “internal unit?” Who’s an “external partner?” This can sometimes be blurry in a higher education setting. In Lavagnino’s opinion, a philosophy document is needed. Gonzales pointed out that sometimes a person’s role comes into play in addition to organizational issues. Are those in question acting on behalf of IU or someone else at any particular time? Scodro shared some interesting examples of situations where the relationship isn’t clear. It has to do with who is responsible for data security/privacy, and in determining when someone is affiliated enough with the university to manage the relationship in some fashion. It’s not a question that leads itself to an easy answer in some cases (which take lots of shapes/sizes/forms). The way we’ve approached some situations is by asking, “Who owns the data?” If it’s the university, then maybe the affiliation doesn’t matter as much. Who employs the individual(s)? What’s the data being used for? In some cases, the data may not be ours, but it’s being used in support of our mission, or maybe it’s our data that’s being used by another entity for a different purpose, etc. Often - IT DEPENDS!! It can be complex issue. Gonzales suggested other helpful questions: “What was the original purpose of collecting the data?” “Who has the obligation to secure the information?” Milford suggested that perhaps the idea of shared governance can come into play as well.
• Schunk – reviewed D3 with respect to external parties. It has been a hot topic. Purchasing has been working with UIPO/UISO to get proper language into contracts. The number of contracts has exploded in recent years. We need to decide where the ownership of this lies. Some things that address this are in purchasing policies, and some are in treasury policies. Schunk is not convinced purchasing should be the owner in this area. Perhaps another group should own such as the Committee of Data Stewards. Clearly we have some gaps. We’ve developed data security language for contracts that involve “risky” data. Purchasing / Treasury have a role to play when they’re aware of a situation, however, in many cases the only people really aware of what information is traversing are people in the departments (p-card purchased services for example). But often, they have a “conflict” balancing the “want” of whatever service they “need” with the sensitivity/risk of the information involved. A key point in this section is who has this responsibility? Schunk shared the CDS proposed policy that says 3rd party involvement with critical data has to be identified by department and involve a data security procedure. For Limited access/restricted information – the appropriate language would simply be added to the contract. For Critical information – UISO would do a security assessment which would be reviewed and approved/disapproved by a data steward. The process is currently very focused on procurement being the responsible party. But, because there are many situations that don’t involve procurement we should consider changing the focus. Davis remarked that it makes sense to make the department more responsible than they are today. They need to be aware of how they need to handle critical data. Lavagnino pointed out the roles and responsibilities document and read key responsibilities: unit people, and purchasing. If we could figure out what we’re supposed to say, we could tweak that document to reflect it. Schunk – what we’ve found over the years is that the data security issues are much broader than just those in which purchasing is involved. Bottom line – the department must identify sensitivity of data involved and how it needs to be handled.

Domain 4 Overview – Asset Management

• Davis & Milford led an overview of Domain 4 – Davis emphasized the domain covers both physical and informational assets, and that asset management depends on risk (i.e. we can’t manage all assets exhaustively – but must focus on valuable/risky assets). Milford said that the CDS is responsible for the institutional data piece. The CDS is organized by sector, but is also responsible for thinking from an institutional perspective. The four data/information classifications were reviewed and examples of data elements classified on the datamgmt.iu.edu site were pointed out. Milford shared a current issue involving reconsideration of potentially re-classifying the university ID number [has since been determined to remain classified as university-internal]. Also brought up the Business Intelligence (BI) initiative and how the combination of existing data elements may raise the risk/classification of the combination of elements. Davis pointed out that from the perspective of the program, data classification covers MORE than the CDS does (i.e. institutional data only), like intellectual property, etc. Kennedy – pointed out need to balance security/privacy with the widespread and appropriate access to information.

Wrap-up and next steps - We received got lots of good feedback from this meeting. For our next meeting, be looking at D3 & D4 for gaps. We will do an exercise similar to what we did today at our next
meeting to identify and prioritize gaps for these domains. Please fill out your feedback form for this meeting. Please provide feedback on other groups with which you think this council should collaborate. Thank you!

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

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

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

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

A7: COMPLETED. Lavagnino will work on revising the “cost/benefit” language in Domain 1.

A8: COMPLETED. Lavagnino/Davis will compile/maintain domain gaps list/prioritization.

A9: COMPLETED. Delegates were requested to complete the meeting feedback survey and send to Merri Beth.

A10: Delegates were requested to review Domains 3 & 4 for feedback on the content at our next meeting, and to identify gaps.

A11: Delegates were asked to think about other groups with which it might make sense for this council to coordinate.

**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](http://protect.iu.edu/privacy/program)