|  |  |
| --- | --- |
| **Meeting Date** | Wednesday August 19th, 2015 3:00 – 5:00 p.m. |
| **Meeting Attendees:** | John Di Marco, Rafael Eskenazi, Rachael Ferenbok, Martin Loeffler (Co-chair), Sue McGlashan, , Sian Miekle, Paul Morrison, Daniel Ottini, Zoran Piljevic, Philip Poulos, Vicki Vokas, Philip Wright, Heidi Bohaker, Dan Hutt, *,* Susan Senese (*missed presentation on Educause)* |
| **Regrets:** | Leslie Shade (on leave), Sven Dickinson (on leave), Kumar Murty, Sam Chan, Glenn Cumming, Alex Tichine, Gian Medves, John Kerr |
| **Guest:** | Dan Pettigrew for Alex Tichine |
| **Location:** | The President’s Boardroom, 1st Floor @ Simcoe Hall, 27 King’s College Circle |
| **Notes taken by:** | Andrea Eccleston |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Agenda Item** | | **Discussion** | | | |
| 1. **Meeting Updates** | | The minutes of the previous meeting (Tuesday, June 14th, 2015) were approved with the following amendments.  **Agenda Item 3: Discussion of criteria to inform the Adoption of a possible framework.**  Two lines were added. John DiMarco suggested that the words “simplicity but not too simple” should be added to the comments  – all agreed that same.  **Agenda Item 4: Consideration of a Specific**  **Framework –**“actionable in the USA” was scratched from John DiMarco’s comment.  **MOTION**  Motion by Phillip, seconded by Phil Poulos to approve the Minutes as amended. Motion unanimously carried. | | | |
| **Action Items** | | **Status** | **Who** | **Due By** | | |
|  | |  |  |  | | |
| **Agenda Item** | | **Discussion** | | | | |
| 1. **Further Consideration and Discussion of a Framework for Recommended Adoption**    1. Educause    2. COBIT 5    3. NIST    4. UCISA    5. Oxford University    6. ISO27000 | | Martin prefaced the presentations by noting that the goal of the meeting is to put forward a motion to accept one of these frameworks as a recommendation to the ISC as a basis for the next information security baseline.  **Q:** Would this framework act as a guide or as a lock-in?  A: The guildeine would be locked in and extended but it remains a recommendation.  Sue presented research materials from Educause available for adoption. Educause templates are based on ISO27000 standard, chosen because it is the only internationally recognized standard.  **Discussion:**  Heidi cited the Audit Cmte terms of reference and asked Daniel to confirm their expectations.  Discussion ensued with Daniel Ottini indicating that the Audit Committee would accept anything that was reasonable and would not be prescriptive. The University would determine the level of success once it decides on a level of maturity.  Daniel Ottini presentedthe COBIT 5 framework noting that it is a large standard and toolkit generally used by auditors.  In response to Philip Wright, Daniel confirmed that COBIT 5 is very committed to mapping to ISO standards.  Given that COBIT is an umbrella framework how do you see this functioning at an academic level?  Can see its applicability at enterprise – how would this function in a typical academic department?  A.  Some functions are really up to governance but once we take those off the table. Part of challenge is there is not always a clear **delineation o**f responsibilities at the Department and at the central level. From an audit perspective, if it is clear then it is clear and it is straight forward. However, the concern is when there is a gap such as when the centre and the division are not clear on who is doing what. Where there is a lack of clarity, part to the Auditors duty is to escalate this discussion at the presidential level by way of an audit report with executive summary. This is not relevant to minor issue – but where it creates risks this is escalated. Process to look at conflict – more applicable at the enterprise level than at the divisional level.  All standards take what is given is going to be derivative to what dept./division and center should do.  Rafael – Can delineate pieces of information, for example, student and HR data etc., faculty and research – organization more type of info and what controls, laws or regulations that drives the information – with anything legislation trumps everything.  Where does the responsibility rest?  Department versus Center is more policy based  Phillip in all large framework – align with other so that can navigate – COBIT – control structure – how interoperable is COBIT with ISO framework?  In term of mapping? ASAKA is multinational thus, able to translate into an audit that makes sense.  Dan - from an operational point of view, if I am supposed to do something you define those requirements – then you audit against that  Daniel - challenge in this environment and where often staff fail is that they do not immediately see the areas which are not defined – gray area – what is reasonable?  In the absence of rule – what is reasonable? Like is it reasonable to have password if system has info you want to protect? What is the risk that will occur of there is no password? That is the way to bridge that gap. If have to Audit against policy, would not have too many audit reports.  Dan - Look at the work, and then provide standards and then audit against that for certification. University should provide that requirement to Admin or Academic division we can understand and interpret.  Daniel – Any type of standard or framework would help. To reiterate what was said at the last meeting, if I had to choose one framework under discussion today, I would go with the ISO because of the fact that it is widest, it touches on all of the other frameworks and in terms of usefulness to the University. Better to start wide and then narrow down.  **ACTION:**  Daniel Ottini to check if ok to distribute the pdf copy of COBIT document.  John DiMarco presented on the NIST framework, noting that it is the framework of framework, not a substitute for the other standards can plug into whenever standard that fits your needs. He added that it is easy to understand, cost effective and not one size fits all. NIST is in response to inadequacy of the other standards – they are too huge, many pages. NIST is deliberately a smaller standard and reference in details to the other standards, in other words it is umbrella of standards.  If pick one you have a default winner for example if you pick COBIT you are committed to COBIT approach – with cyber security framework of NIST can look at each sub-category individually using different frameworks. It allows Daniel and Martin to be at the table on equal footing – fit into NIST framework – look at the merits of each framework to make a decision.  Discussion  Q.  Susan - how is that easier? Given that there is the requirement to understand all the standards/framework.  John – No,  Susan - Decide which standard or framework to pick  John – allows you to adjust each subcategory to address that issues  ISO can address in whatever way see fit – flexible – easy way – pick a standard – that is not an effective Committee and Council  Language to take to faculty members   * Fully compatible with and cross-reference to COBIT /ISO etc take your pieces out of that * Under same umbrella level of coherence and coordination – to manage own system – big and small divisions – * Danger – ISO and COBIT – multiple standard all are allowed and can multiple ways * diversity a key aspect with coordination * NIST does not explicitly detail but provide pointers – different but also compliant, coherent and consistent * Council will have the freedom – going to use language that come from COBIT or ISO * What is excluded – they are comprehensive but need to prioritize – all the other frameworks have this issue – still need to draw on thing sense of priority and areas for higher tiers. * It is an enabler but still have work to be done.   Phillip provided the following presentation on UCISA toolkit and the Oxford University. UofT is at a low level of maturity processes and especially collaborative – that needs to be built need to model new kinds of processes and government processes. The UCISA and Oxford bridge this gap for otherwise start from ground up. He added that UK has done the work for us, it is the standard for UK Higher Ed space, a way to get down to much more practical implication and discussion. He noted that what we get, lower cost speedup implementation community of best practices as well as get connected to an international platform - resource available online. CISA – root map – lays out the stages – foundation of guidance of all stages. Activities and objectives – despite lack of maturity. Governance structure interesting as Oxford built like UofT.  Policy and toolkit – independent unit level risk assessment – not part of other framework – open source. Risk assessment – template available from oxford site. Layer of expertise, Network and system security. Since 2012 – actual working guidance available. Presented an ISC Governance Model based on the Oxford model. He concluded that it is a rich robust tookkit – ripe for implementing.  Q.  Daniel noted that all the standards contain essentially the same stuff.  He expressed the concern about the lack of maturity of this framework given that it has been in force since 2012 which is not a long time.  He also asked enforcement process at a divisional level. Concern is what get on the headline “the University of Toronto” not the department/division. How is that dealt with? Would there be a sanction, in the absence of a sanction how responsible?  Rafael added that do we want to impose someone else’s standard?  Do we want to adopt a standard someone else has created  Phillip responded that the issue is that Oxford gets closer to conversation –we spend limited resource on that kind of question rather than figure out.  Dan: Not the place to determine discipline when not followed  Daniel: As an auditor if there is no threat of sanction the often priority would be lower.  Dan that has to come from governance not from security – not addressed in the standard.  Daniel: Since we are taking this from Oxford, then it follow that it might be useful that we should take what they do. Has that ever happen and what happened?  Phillip - ISO standard has guidance on all of these things, it is at a very high level. UCISA takes that standards and builds and reduces and boils it down for Higher Ed applicability, have not lost anything but rather gain something. Oxford implementation takes it one step further (have not lost anything). We gained their wisdom and the templates that are available. What we do with it is up to UofT. What is recommended is that it gets to where we can ask those questions in a meaningful way for our Higher Ed solutions  Question: How does sanction work in other areas, for example finance?  Sanctions are beyond scope of ISC and handled at a higher level  Guidance at operational level and handled at a higher level.  Daniel rephrased his concern noting that he recognized the risk of turning responsible for compliance over to a different area.  Phillip: The accountability structure of Oxford and accountability structured advanced by the UofT draft plan is very clear that individual unit heads are responsible. That is the end of it.  Raphael – Difficult to come to an agreement because of these questions of divisional or central responsibility, we cannot continue doing what we are doing regarding. Part of reason we are engaging in this process. We are doing a to disservice the idea of diversity, idea of having a template available to look at is great and appreciate that Oxford have done this work but looking at this process and how we are operating we need to create something for ourselves. I also think just looking at this process and how we are operating that we do owe to our various constituents that we represent. The recommendation of the one standard might not fit well with some departments.  Phillip clarified all frameworks including the Oxford model is an active discussion – what is being presented is a model that gets us closer to where we want to be as an academic institution – this is being offered as guidance to be layered on top of any other framework.  Daniel clarified that his comment was to understand how it works on the ground at Oxford.  In wrapping up Martin said there is the recognition that there are many approaches noting that he was not going to speak directly to the ISO family of standards, but as is evident from all the presentations ISO seemed to be the ground upon which all the other standards are built. It is evident that there are more standards and frameworks than what was discussed today. In part or in whole goal is to create something that the University can review its own progress against and use as a marker.  Martin opened floor noting that members were welcome to submit as many motions as possible. The motion with the greatest number of votes in support of will be the option recommended in moving forward as the place to start.  It was proposed that group decide on a framework and then decide on how to package same and what toolbox will be used. Motion was advanced to separate the standard from the toolbox.  ACTION:  Vicki will circulate all document at the end of the meeting  **Motion:**  Motion by Sue to make a recommendation for a standard not the toolbox or implementation. Seconded by Raphael  **Motion failed.**  **Suggestion was also advanced for the use of a straw poll, look at the other alternatives.**   * 1. Educause   2. COBIT 5   3. NIST   4. UCISA   5. Oxford University   6. ISO27000   **More discussion on the strength and weaknesses of each proposal and why is required?**  Suzanne suggested that she required a better understanding of the urgency, cost and risk profile in order to pick and vote on a solution.  It was decided that the Committee required more time to review and discuss the available options presented with the intention to vote on the matter. | | | | |
| **Agenda Item** | | **Discussion** | | | | |
| **5. Adjournment** | | There being no further business to come before the committee, the meeting was adjourned at 5:10 p.m. | | | | |