IT Governance Committee
Meeting Minutes
02.01.2018

Members in Attendance:
John Charles, Vice President for Information Systems and Technology
Professor Karen Gleason, Associate Provost (Co-Chair)
Professor M. Frans Kaashoek, Department of Electrical Engineering & Computer Science
Anthony Sharon, Deputy Executive Vice President (Chair)
Robert Solis, Head, Information Services Department, Lincoln Laboratory (new member)
Glen Shor, Vice President for Finance

Guests:
Christopher Bunn, Director of Business Operations, Information Systems and Technology
Emma Levett, Software Asset Manager, Information Systems and Technology
Christina Lo, Director of Strategic Sourcing and Contracts, Office of the Vice President for Finance
Michael Moody, Institute Auditor
Eamon Kearns, Senior Director, Emerging Solutions, Information Systems and Technology
Mark Silis, Associate Vice President for Information Systems and Technology
Garry Zacheiss, Director, Platform & Systems Integration, Information Systems and Technology

I. Meeting Minutes 9.12.17 Approval (Approved)

John Charles gave an update on action items.

1. Robert Redwine, Chair of the IT Policy Committee, is closing the loop with Whitney Espich of the Alumni Association on two action items from the last meeting.
   - Request to allow MIT alumni to keep their mit.edu email addresses, instead of being provided alum.mit.edu addresses
   - Request to allow MIT alumni to keep mit.edu websites created as class assignments (or for other reasons) while they were students
2. Robert Redwine continues to work with Nate Nickerson, Vice President for Communications, on a draft policy statement for Google Analytics.

The minutes from the 9.12.17 meeting were approved.

II. Steering Committee Projects and Spending Updates (Discussion)

Eamon Kearns gave an overview of spending on Administrative Systems Steering Committee (ASSC) and Student Systems Steering Committee (SSSC) projects.

1. The ASSC portfolio is forecast to come in at around $2.3 million instead of the budgeted $3 million; some projects were slow getting started. At an ASSC meeting on January 8, 2018, the group approved the release of $200K for new requests.
2. On the SSSC side, the portfolio is forecast to come in at a little over $1.5 million instead of the budgeted $3 million. Similar to ASSC, some projects didn't get started when targeted. Ian Waitz, Vice Chancellor, also asked to reduce costs on some projects and helped make related scope decisions. Tony Sharon noted that Ian Waitz is going through the SSSC portfolio and reprioritizing it.
3. IS&T is also doing work on sponsor-funded projects, with funding provided by those making the requests. The forecasted budget for these projects is $1.5 million.

III. Modernization Funding Plan Adjustments for FY18 and FY19 (Endorsement)

Tony Sharon is working on the FY19 budget with input from Ian Waitz and EVPT Executive Director Robin Elices. The plan is to recommend to Provost Schmidt and

EVPT Ruiz, that modernization spending be trimmed until decisions are made on how to work the recurring costs from past modernization efforts into the General Institute Budget (GIB), as well as deal with the escalation in Dropbox charges.

1. Any carry-forward dollars can be kept by the ASSC and SSSC and they will manage them.
2. Some requests should be funded by individual units, because the work is unique to them (e.g., Facilities scheduling and capital projects).
3. Ian Waitz has called for a faculty committee with representatives from MITx and each of the five schools to look at commercial learning management systems to replace Stellar. The MIT Sloan School of Management is piloting Canvas and has written a report about it. Eamon Kearns are looking at the one-time and recurring costs of moving to a commercial system.

- **Discussion:** Frans Kaashoek asked how budget plans around modernization affect the IS&T budget. Tony Sharon noted that most of IS&T's modernization work is being done by consultants, a term-limited workforce.

IV. **Software Funding Model Update** (Consultation)

IS&T has been asked to come up with a software funding model and has put together an initial proposal that will need fine-tuning. John Charles described the "new normal," an industry-wide shift from software licenses ("buy it and own it") that can be run on premise to cloud-based subscription models with annual operating expenses. This model gives vendors greater control. There are upsides and downsides to this new model and different control levers for MIT. Emma Levett talked about the Microsoft (MS) licensing model as an example.

1. In the current model, MIT buys perpetual licenses for faculty, students and staff based on an FTE calculation (a total quantity based on whether they are full-time or part-time). These licenses provide access to a suite of MS products and back-end services.
2. With the shift to the cloud, either this June or next year, MIT will buy subscriptions on a 1:1 per user basis, with a few different bundle options.
    - Office 365 A1 (free to light users, such as students)
    - Office 365 A3 or A5 for "knowledge workers," those doing intensive administrative work and in need of advanced features and services. The biggest differences between A3 and A5 relate to telephony and security.

   Chris Bunn noted this shift will require more active management from IS&T to assign users to appropriate bundles and keep track if their role changes.
3. OneDrive (a MS hosting service similar to Dropbox, but with MS integration hooks) comes standard with these packages, though the level of storage varies depending on the bundle.

- **Discussion:** Karen Gleason asked about the difference in cost between the A3 and A5 bundles. Emma Levett responded that while the specifics aren't known yet, the A5 is expected to cost a lot more. John Charles noted that companies often won't give quotes until IS&T tells them the number of users. Other schools have moved to Office 365, but not to the new bundle model. MIT (like other institutions) has the option to extend the current model for one year beyond June.

Chris Bunn next talked about the future of software funding and the impact of the "new normal" on cloud-based subscriptions.

1. The culture choices at MIT makes standardization difficult. There is a plethora of tools in use on campus (e.g.,10 to 15 different statistical computing tools). Since community members are comfortable with what they're using, it's hard to standardize. For example, IS&T implemented Qualtrics as an enterprise survey

tool, but many are still using SurveyMonkey. That's the culture here – if you have the funding, you can use what you want.

2. Other challenges involve rapidly increasing costs along with the shift to cost-per-user licenses. Examples include the following:
    - The cost for Adobe Creative Cloud has increased 30%, with no increase in the number of licenses. MIT has already reached its cap.
    - Admissions has moved from Stargate, with a fixed maintenance cost, to Learning Machines, a cloud model with a cost per application. Tony Sharon commented that this cost could be added to the application fee.
    - CrashPlan, a cloud-based option that replaced the TSM service for desktop backups, has been so popular that IS&T has seen four times more growth than originally anticipated. Despite creative work with licensing, there's been a 300% increase in cost since IS&T first started providing it. If everyone on campus came on board, the number of licenses could double from 20,000 to 40,000.
3. Over the past few months, IS&T has been exploring new funding model options and scenarios for recovering increased costs and accounting for future growth. IS&T has:
    - Flagged 10 to 30 opportunities for strategic procurement.
    - Classified software into five tiers: Tier 0 (IS&T only, back end); Tier 1 (the MIT community); and three other community-based tiers. Chris Bunn discussed the differences between the five tiers and acknowledged that the list of software sorted by tier is a work in progress.
    - If there's enough buy-in and IS&T can identify a funding source, some software might shift tiers to become more widely available (e.g., Slack).

- **Discussion:** Tony Sharon noted that a role of the new Steering Committees may be to judge when software should be funded centrally or left with departments, labs and centers (DLCs). Karen Gleason asked about this process in light of the FY19 budget process. Tony Sharon wants to work with others to decide which software packages should be centrally funded through IS&T in FY19 and then educate DLCs about the costs involved, for future reference. Karen Gleason then asked if peer institutions like Stanford and Harvard are going through this same exercise. John Charles responded that he's talked to the CIOs there and at other schools and none have moved as quickly to the cloud. Other schools also have more offsets and are not as centrally operated as MIT.

  Frans Kaashoek asked about the repercussions of reduced FTE on IS&T, which means the department can deliver fewer services and less innovation. Tony Sharon commented that with software as a service (SaaS), modernization is being done at the vendor level. John Charles noted that while some FTEs are offset by the move to the cloud, IS&T does need more employees for work higher up in the technology stack (e.g., integration, APIs, data science and analytics). John Charles observed that IS&T has used consultants for much of the project work done with modernization dollars. Mark Silis concurred that IS&T needs less staff, but the skillset of the staff needs to change (e.g., replace the data center operator with a DevOps engineer.) He also noted that it is hard to change IS&T's staffing profile through natural attrition.

  Tony Sharon then discussed affiliates in relation to software allocation and costs. If the costs of Tiers 0 and 1 (80% of the costs) are spread by headcount, affiliates represent about a third of the total. Karen Gleason noted that affiliates are not supposed to be on campus, so it's not clear that they should have automatic access. She suggested that by default they should have to apply for it; she and Tony Sharon both noted that the definition of affiliate needs to be clarified. Several ITGC members agreed that there should be a fee for affiliate status (like at Stanford). Christina Lo said that from a risk and contract perspective, it's also important to define employee. With respect to alumni, IS&T provides email forwarding for life and subsidizes software for the first six months after they graduate.

V. **Dropbox Quota** (Endorsement)
Chris Bunn provided an overview related to the new Dropbox quota. At the last ITGC meeting the committee discussed how to implement a Dropbox storage quota without putting IS&T's budget at risk, now that the department is responsible for buying storage packs. There are almost 21,000 licensed Dropbox users at MIT. Originally Dropbox offered MIT unlimited storage, but there will be a capped quota starting December 2018 (extended by Dropbox from an original date of July 2018).

IS&T does an annual decommissioning of accounts for those who have left MIT, but based on growth over the last 12 months, the department will need to pay Dropbox $500,000 for additional storage in December. If growth continues at the current pace for another year, IS&T would have to add another $1 million storage pack, for a per-year cost of $2.4 million.

If a quota of 200 GB per user was set today, 90% of users would not be impacted and MIT would only be using 800 terabytes (TB) or 40% of total capacity. About 2,000 accounts do exceed 200 GB, so IS&T would have to plan for them. The more realistic option may be to offer storage packs to users at terabyte levels. IS&T does have quotas for other services, such as Office, Gmail, and Exchange.

If IS&T does grassroots outreach to high-end users and finds other solutions for them, it may circumvent the purchase of the $500,000 storage pack in December. Other ways to limit storage exposure include pop-up notifications for users exceeding their quota and more frequent decommissioning on the administrative side. Other options would require more outreach, including decommissioning student accounts one month after graduation (instead of six months); capping users who are exceeding the quota; and enforcing a quota earlier than October (the current plan), to get users used to the new norm. IS&T would need ITGC to endorse any or all of these options before moving forward.

Discussion: Tony Sharon commented that the word about a Dropbox quota is getting out, so it won't be a surprise, but IS&T will need to offer some options. Frans Kaashoek observed that a lot of the extra storage needed for research can be built into the research contracts. Chris Bunn noted that IS&T hasn't worked out all the mechanisms for chargebacks and how that would be handled, but would expect an annual commitment for storage purchases, whether bundled at the user, department or school level.

Tony Sharon's approach would be to send a memo to Provost Schmidt and EVPT Ruiz about these plans and ask if he should make a presentation at Academic Council and review the timeline for enforcing quotas. Another possibility is that the Provost would provide funding for the year-end storage pack. Frans Kaashoek stated that going to a quota system is key, to raise end user awareness. The top 40 users might have funding to pay for their storage. Gary Zacheiss noted that the top 10 users (10 TB and up) are all faculty or senior research scientists, while the average user is well under 100 GB. It would make sense to reach out to the top 10 to 30 users to explore other storage solutions. John Charles commented that he has been in discussion with the MIT Libraries about data management plans for MIT research projects and has told them that Dropbox is not an option.

Action Items: Tony Sharon summed up by outlining three action items:

1. He will discuss a proposed plan of action with Provost Schmidt.
2. IS&T will talk to the top 10 to 30 users about quotas and options.
3. He will get input about communication to the wider set on campus, either through Academic Council or the school councils.

VI. Cybersecurity Updates (Discussion)

John Charles discussed three topics: cybersecurity proactive measures, response to recent cybersecurity vulnerabilities, and emerging cybersecurity issues.

1. *Cybersecurity Proactive Measures*. There are two types of breaches IS&T needs to focus on:
   - Data breaches
   - System integrity breaches

   John Charles reviewed the Cybersecurity Proactive Measures chart, which outlines protection, detection and response measures currently in place and planned.
   Discussion: Tony Sharon suggested proactively giving the Corporation's Risk and Audit Committee an update on these measures. Frans Kaashoek asked how IS&T will inform the community about planned scans of publicly facing files (Dropbox, OneDrive, Athena's AFS) for personally identifiable information (PII), since it could be a sensitive issue; he referenced how communication to the community about Google Analytics could have been better. Mark Silis stated that IS&T will only do content scanning on information that is publicly accessible; it will not do any scans that require superuser permissions. These scans have been discussed and approved at the IT Policy Committee (ITPC) meeting. Frans Kaashoek advocated for proactive communication; Mark Silis suggested that the email be sent from the ITGC rather than IS&T.
2. *Response to Recent Cybersecurity Vulnerabilities*. John Charles spoke about Meltdown and Spectre and news of the exposure of confidential data on Stanford's AFS system.
   - Vendors have been releasing patches for the Meltdown and Spectre vulnerabilities, but then recalling them. IS&T is dealing with this in a very deliberate way, testing what vendors provide to make sure it doesn't cause other problems. The issues won't be fully remediated until hardware vendors provide new chips. Frans Kaashoek commented that this issue has been overhyped in the press. The message should be "Don't panic." Mark Silis agreed, given that our network doesn't have shared tenancy.
   - In response to the news of Stanford's data breach, IS&T did a scan of its AFS system and identified PII for 10 people; the Office of the General Counsel (OGC) sent them notification letters. IS&T now has an automated scan in place that incrementally looks for any changes and plans to do the same for Dropbox and OneDrive.
3. *Emerging Cybersecurity Issues*. Three standards/protocols have recently required significant attention: the NIST 800-171 Controlled Unclassified Information (CUI) data management standards; the European Union's General Data Protection Regulation (EU GDPR); and a security protocol for endeavors involving high-risk entities.
   - IS&T is working with the Office of Sponsored Programs (OSP) to provide assistance to researchers/PIs who need to comply with new NIST 800-171 standards required in federal contracts.
   - OGC and Risk Management and Compliance Services are holding meetings with many DLCs and offices across MIT about the European Union's GDPR.
   - OSP has conferred with IS&T about faculty interested in doing work that involves using equipment donated by suppliers on the federal government's "do not use" list. IS&T has reviewed Stanford's protocol on this and provided a draft protocol for review by the ITPC.

Discussion: Mark Silis noted, as an example, that the Research Lab of Electronics (RLE) is using Huawei technology because they gave it to them, but Huawei is on the "do not use" list. He commented that there are legitimate threats out there and gave the example of Kaspersky Lab software that was exploited. MIT will likely see more of these exploits and doesn't have a process in place to advise the community about accepting tech donations or buying IT equipment / software. John Charles observed that components from some of these "do not use" companies are embedded in other products with a different vendor label. OSP has asked IS&T if there are measures to guarantee that all products from Huawei or other "do not use" vendors are secure. IS&T's Information Security Officer, Jessica Murray, told them there is no way to do that. Frans Kaashoek noted two jeopardies: the equipment and the vendors wanting to donate money to research projects. There are also alumni at other companies who want to collaborate with MIT. The donation and collaboration decisions will fall to the Office of the Vice President for Research (VPR)/Provost.

VII. Infrastructure Projects Updates (Discussion)

Mark Silis discussed plans for Building W91, IS&T's main data center since about 1981.

1. IS&T hosted most of its enterprise computing in W91 until moving it to OC11 in Downtown Crossing in 2008/2009 and more recently to the cloud.
2. In the last couple years, IS&T has migrated about 3000 virtual servers to vCloud Air: a success story.
3. IS&T is evolving its cost model to get greater return on its investment, in terms of space and power. Space in Cambridge is very valuable and MIT is in the midst of a space crunch. IS&T is looking at its data facilities portfolio and how to chart its future. W91 presents an opportunity to return additional space to the Institute. The W91 datacenter is used today mostly for co-location services, hosting research computing for DLCs. IS&T has about 75 racks in W91.
   - About 52% of rack space is taken up by research (storage arrays, computer clusters, a mix of things)
   - 23% of rack space is used for redundancy, DLCs that want another site for their systems as backup (their primary system may be at OC11); Sloan is a good example with its online learning systems, with a primary presence at the OC11 facility and a backup system in W91.
   - The remaining 25% is a mix of things, such as Facilities' Andover Controls system.
4. There are a couple of options in terms of migration strategies moving forward:
   - With respect to research computing, leverage the Massachusetts Green High Performance Computing Center (MGHPCC) investment out in Holyoke. The MGHPCC efforts have been very successful for MIT: over five years, MIT has almost filled its entire initial footprint. To relocate W91 services to MGHPCC would require an additional investment. Harvard recently made that decision, adding two new pods over six months. Part of the discussion is how to do these expansions in terms of technology, for example, kilowatts per rack. MIT could add about two pods of growth; beyond that, options might include subleasing from other MGHPCC tenants or using space in outside containers.
   - Cloud services in two flavors: vCloud Air hosting service (third party with its own cost structure) and providing private cloud services on campus using OpenStack
   - To come up with a comprehensive model for MIT, IS&T will need to engage the current tenants of the data facility in W91 and collaborate with Chris Hill at MGHPCC as he charts its course over the next couple of years.

VIII. Next Generation MITnet Update (Discussion)

Mark Silis noted that conversations on this project continue, including detailed discussions with Frans Kaashoek, Nickolai Zeldovich, and Dave Clark. IS&T has also reached out to the Media Lab and its IT director, Michail Bletsas, to discuss the best approach.

1. The Media Lab uses Network Address Translation (NAT) in their environment internally, but Bletsas thinks MIT students should be required to operate on a no-NAT, no-firewall environment to learn about risks. NAT is appropriate for administrative and finance staff. There will be a follow-up meeting with SIPB members next week.
2. In terms of MIT's contract with Amazon, there's a milestone coming up at the end of June. John Charles and Christina Lo have been working to come up with contingency plans to reduce MIT's liability in the event of not making that milestone. They have made progress in reducing the potential penalties down to a proportionate share of what isn't delivered. IS&T's network team is identifying what the department is likely to have ready for Amazon in June and before Back to School in September. IS&T's goal is to complete the first phase NLT Back to School.
3. One of the efforts has been to deploy Dynamic Host Configuration Protocol (DHCP) on current IP addresses; DITR staff have been making the rounds on campus doing this.
4. The Media Lab is recommending a hybrid (dual stack) strategy; once CSAIL and SIPB are in alignment, Tony Sharon and Mark Silis will send a follow-up summary.