Straighten Up Your Risk Posture: How to Brace Your IT Procurement Practices

Presented by:

Neal Fisch, Director of Enterprise Solutions & Security, California State University Channel Islands
Peter Mosinskis, Director of IT Strategy, California State University Channel Islands

October 31, 2017
Educause Annual Conference
Philadelphia, PA
Cal State Channel Islands is located about 50 miles north of Los Angeles. We are a 4-year public university with ~7200 students and ~1000 employees. We are also the newest campus in the 23 campus California State University system.
Icebreaker!
Icebreaker

Introduce yourself to your tablemates and share:

one thing that no one else probably knows about you
Neal is a huge fan of SciFi and classic Warner Bros. cartoons.
Over the last year Peter started bottling my own hot sauce from very hot peppers ("ghost peppers") that he grew in his garden!
Exercise 2

Spend 5 minutes and write down your procurement pain points on the giant Post-It page

Request procurement pain points; complete stickies and post on flip chart
Here were the results from today’s exercise regarding procurement pain points:

1. Decentralized purchasing with no risk review, especially for research-related procurements (e.g., grant projects)
2. Managing budget autonomy vs. security control & viability of product: if divisions or departments have budget authority to purchase IT, how can we make good decisions about the security of products & their viability in the University environment
3. Innovation vs. procurement bureaucracy: how to balance agile procurement that supports innovation vs. required paperwork to manage risk
4. Moving from implementers to contract managers: creating a transparent process
5. Predicting cloud demand/sizing
6. Vetting cloud security, especially for classified and/or government-specific clouds
7. When & how to engage with your purchase requestors: getting the timing right for your organization, so that people aren’t blindsided and can move through quickly.
8. Purchase cards: how to create policy/practice around purchase cards to manage risk
9. Standardization of assessment documentation, and standardization of
procurement process: where are assessments stored & how are they shared so that people are aware of product availability, and can re-use previous assessments.
The model that was built at CSU Channel Islands was done to improve the procurement process and address a specific set of problems:

1. Blindsided by procurements (not meeting security/risk/compliance guidelines/requirements);
2. Perception of IT as a roadblock – Going around IT processes due to the misconception of the answer always be “No you can’t do this”.
3. Vague accountability regarding security and risk being aware of systems/services in the organization and subsequently the risk to the enterprise.
4. How we scaled our procurements was opaque; procurements were being treated inconsistently; no process was documented so the process was not regular and repeatable. Some procurements took a long time even though they were small; other large procurements weren’t sufficiently reviewed which created re-work.
5. We didn’t have easy access to shared metrics that we could use to gauge the efficiency of our IT procurement process
We implemented various processes, which we’ve now abstracted as a model with 4 components. It’s not the only option, but we believe it’s scalable to fit different organization sizes and cultures.
The IT procurement model has 4 components: buckets, rubrics, thresholds & workflows
First component is the idea of procurement “buckets”
Buckets were inspired by Rob England’s book “Plus!” Rob is an IT service management thought leader and consultant who lives in New Zealand. “Plus” applies the idea of case management (used in healthcare, legal and other sectors) to reframe how we deal with service requests.
By differentiating procurements into different buckets, we can start thinking about how the process for those procurements can be made more repeatable and efficient, even though the procurements themselves may or may not be standard.
We propose that the easiest approach is starting with two buckets: standard and "non-standard” (a.k.a. custom, or "case").

Standard procurements are regularly repeating, commodity procurements that have a very fixed, established risk and impact. Think standard desktops, laptops, etc.

As time goes on, add more items to standard.

Custom procurement
Exercise 3

1. Take the provided BLUE cards; each card represents a possible procurement.

2. Group them into “standard” and “custom” buckets (2 columns).

Examples:

Desktop computer for a computer lab
New drone purchase
Printer

Desktops
Laptops
Printers
Phones
Software etc.
Discussion

Who would like to share their list of standard items?

Which items overlap into both groups?

What issues did you discover?

What if your custom items were renewals? Would you categorize those differently? If so, why?
This is how CSU Channel Islands breaks down its technology procurements.

Standard items include any commodity items.

Custom are one-offs, such as custom hardware (anything from a custom laptop to a one-off network switch) or other non-standard equipment or services.
Here’s an example of the standard procurement pages on our web site; we list quotes for our standard equipment, and provide instructions for how to order.
Over the past fiscal year, at CSU Channel Islands there is approximately a 60/40 breakdown between custom & standard procurements (424 total IT procurements). In the first 6 months of the process, it appeared close to 50/50, so we expect these figures to stay about the same.
Takeaways

• Make it easy for your organization to procure standard items

• Make it clear what is standard and what is not

• Constantly update and communicate out your list of standard items
It’s the custom ones that cause problems and that need careful evaluation, because they are altogether new and/or unfamiliar to the IT environment.
The 2\textsuperscript{nd} part of the model involves rubrics.
A coherent set of criteria for grading or scoring

The definition of a rubric: A coherent set of criteria for grading or scoring
Rubrics are frequently used in academia as a way to measure learning outcomes. They are also convenient for measuring risk and impact.
You might want/need to know about:

- Security & Risk
- Accessibility
- Data & Interface
- Infrastructure
- User support
- Funding
- ???

There are different aspects of IT products and services that you want to evaluate to manage risk and impact: security, accessibility, data integration with other systems, infrastructure impact, support impact, funding impact (how much one-time vs. ongoing cost) and other factors.

It’s convenient to develop and use a rubric to help measure some of these factors in a consistent, repeatable way.
Rubric Exercise – Part 1

1. Take the stack of MULTICOLORED cards.

2. Sort questions in order of priority (top: most important questions)...try to reach consensus. It may help to group questions into “critical” and “nice to know” categories.

3. Write in additional questions if necessary and re-sort

Rubric Question Seeds - White, grey, green, orange, blue
Rubric Exercise – Part 2

1. Pick your top 6 MULTICOLORED CARDS
2. Add questions to first column
3. Add answers to questions
We’ve pre-set your numeric scoring model
Place question cards in first column
Write answers on Post-Its, and place on grid.
Adjust answers & scoring model as desired
Rubric Exercise – Part 2

1. Pick your top 6 MULTICOLORED CARDS
2. Add questions to first column
3. Add answers to questions

White, grey, green, orange, blue
Discussion

What were your top questions?

Were there any that were missing?

Did you ask questions from each category?

Were you able to reach consensus on scoring?

Do you think this scoring model could be effective in your organization?
   If not, how could we make it more effective?
How CSU Channel Islands tackled this issue
Neal uses a 60-question security questionnaire; it can be a challenge to get vendors to answer longer documents!

Currently transitioning to the EDUCAUSE HECVAT (Higher Education Cloud Vendor Assessment Tool)  
https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool

CSU Channel Islands is currently evaluating migration to the HECVAT Tool provided by HEISC.  
https://library.educause.edu/resources/2016/10/higher-education-cloud-vendor-assessment-tool
For accessibility evaluation, Peter uses the ITPIA. You can try it out for yourself here: 

go.csuci.edu/ITPIA
Behind the scenes, the ITPIA calculates a numeric score like the previous exercise. From there, some action is taken based on the maximum score.
Fibonacci numbers are used for scoring in our model because they are a convenient way to scale risk and impact; these numbers are often used in Scrum evaluation of work effort, and translate gracefully to the rubric for gauging impact.

It’s important to test the rubric that you create & tweak it! CSUCI piloted the rubric for 3 months before it was finalized, with 20+ procurements. Any rubric should be aligned with individual and/or group “gut checks” to ensure that the results match your expectations (e.g., I expected this product with its given use to be high impact, did the score indicated match up with this?)
Rubric Scoring
Exercise 3 – Rubric Scoring Part 1

1. On your own, run through each test case
2. Calculate a total score
3. Write score down on Rubric Scoring Sheet
4. Discuss your scores at your table
Discussion

Which were the most difficult or contentious?

Which procurement would be the most controversial at your campus and why?

Do you think this scoring model could be effective in your organization?
  If not, how could you make it more effective?
Discussion

For each question, which third of scoring did it fall:

- **12-24**
- **25-36**
- **37-48**

White, grey, green, orange, blue
Scores that had the most consensus indicate that generally people agree that a certain procurement is low (or high) impact.

Outliers are interesting because they reveal how even with a rubric, interpretations vary based on a person’s understanding of the product, its use and impact.
The final parts of the model are thresholds and workflow.
With the score from your rubric, select a convenient, reasonable “cutoff” point (aka threshold) that will determine what action you will take.
Workflow is the set of actions that your organization will take based on whether the score was above or below the threshold.

At CSUCI we take different action for standard vs. custom procurements, also small custom vs. large custom procurements.

This is a visual diagram of the custom IT procurement workflow that CSUCI uses in TeamDynamix, which is the ticketing and service request system that we use to gather all IT procurement requests. Each step assigns a unique ticket to a person and/or group; parallel steps must all be completed before moving on to the next step.
For this exercise, the MEDIAN will be your threshold point

But in your organization, you will have to determine what your threshold point will be...
(median? Top 3rd? Top 20%? Bottom third?)
Threshold & Workflow Exercise – Part 1

1. **Pick two items** that you evaluated: 1 above and 1 below the threshold.

2. Your handout has a list of possible steps in a workflow (shown on the following screen); feel free to add any if necessary.

White, grey, green, orange, blue
These are possible workflow actions you may use for items above or below the workflow. Select those which make the most sense to your organizational culture!

<table>
<thead>
<tr>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement moves forward</td>
</tr>
<tr>
<td>Procurement is blocked until review &amp; analysis is complete</td>
</tr>
<tr>
<td>Procurement moves forward with retroactive review</td>
</tr>
<tr>
<td>Gather additional info from customer</td>
</tr>
<tr>
<td>Gather additional info from vendor</td>
</tr>
<tr>
<td>Get approval of ISO</td>
</tr>
<tr>
<td>Get approval of risk manager</td>
</tr>
<tr>
<td>Get approval of general counsel</td>
</tr>
<tr>
<td>Get CIO approval</td>
</tr>
<tr>
<td>Get approval of Infrastructure manager</td>
</tr>
<tr>
<td>Get approval of data steward</td>
</tr>
</tbody>
</table>
Threshold & Workflow Exercise – Part 2

1. What will your workflow be for scores **above** the threshold?

2. What will your workflow be for scores **below** the threshold?
<table>
<thead>
<tr>
<th>Sharing with whole group:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. How do you think this will scale for different types of procurements, and where might you run into hurdles?</td>
</tr>
<tr>
<td>2. How long do you think it would take to complete the process below the threshold? Above the threshold?</td>
</tr>
<tr>
<td>3. Did you do anything to shortcut or expedite your workflow? If so, why?</td>
</tr>
<tr>
<td>4. Are these workflows realistic for your organization? Why or why not?</td>
</tr>
</tbody>
</table>
Food for thought

1. Who owns the rubric questions, thresholds & workflow?
2. Who owns the evaluation process?

In CSUCI’s case, the technical evaluation process is owned by IT; contract review and issuing of purchase orders is Procurement’s responsibility; budget analysts are responsible for placing orders in the system; and it’s the product requestor’s responsibility to articulate why an item is being purchased and how it will be used.

So in this sense, the IT procurement process must be “owned” and shared by all those involved.

It’s key to have your C-level leaders buy in to foundational IT procurement policies/practices, such as “IT must approve all IT procurements” and “No IT products or services can be bought on a purchase card/company credit card unless approved in advance by IT leadership”
We wouldn’t have had a successful process unless we partnered closely with Procurement and our budget analysts, and that we regularly meet to refine and continuously improve the process. You must repeat the same message a lot, and you must make it conceptually simple to understand (hence two flavors “standard” & “custom” to start with)

You must constantly review & adjust the process. Standards must be regularly reviewed & updated as new standards emerge from custom procurement repeats, or old standards get out-of-date.

It’s not perfect; it’s continuous gradual improvement. As with agile techniques, you can get more value from IT procurement by applying a “minimum viable product” approach to creating your IT procurement practice. Start with something small & easy, and then expand it when it makes sense to. For example, making standard procurements more efficient could reap huge rewards (standard IT procurements are probably 40-50% of all your procurements!)
Neal & I are happy to meet with you individually to demonstrate CSUCI’s system in more detail.

Hopefully this seminar will inspire you to take steps to make your IT procurement process more transparent, repeatable, predictable and efficient.

Please let us know about your successes, challenges, or any questions that you may have about this model, we’d love to hear from you!

Neal Fisch, neal.fisch@csuci.edu
Peter Mosinskis, peter.mosinskis@csuci.edu

Information about CSU Channel Islands’ IT procurement process: 
www.csuci.edu/ti/purchasing/