Information Security & Business Continuity Governance Committee Meeting

Thursday, November 15, 2012

Location: Metcalf Trustee Center Kenmore Conference Room, 1 Silber Way, 9th FL

Time: 8:30am-10:00am

Chairs: Bill Long & Christie Talley

Support: Quinn Shamblin

Attendees: Anna Bustin, Maria Canellos, Ran Canetti, Greg DeFronzo, John Imbergamo, Eric Jacobsen, Rebecca Ginzburg, Tracy Schroeder, Ari Trachtenberg, Bill Long

Recorder: Deneena Lewis

Agenda

- FY14 Project Budget
- Current State of Disaster Recovery Plan
- IT Planning: Sample Plan Discussion
- Email Encryption Gateway

Notes:

FY14 Project Budget (Tracy Schroeder)
- There are 3-3 million dollar costs associated with IAM. It is decided to focus on updating the critically at-risk network infrastructure. Access management projects were deferred.
- Identity and access project costs were pressure tested by the team putting together the estimated cost with the vendors and providers depending on the nature of the solutions.
A contingency budget was not used. We try to strike with a realistic budget to avoid asking for money we don’t need.

There are concerns about funds being proposed for one project, but used for something else. This is not something we allow to happen.

The submitted proposal was for backup modernization, which is a continuing cost. There is a significant risk if we don’t do this.

Included in the budget are principal personnel, maintenance, and allocated operating expenses. Capital networking was not included.

There are 3 combined backup systems that will replace the very old infrastructure at a more reasonable cost.

Time entry is something we want to do in SAP but that will take some time. Being such a large project, we can’t ask that of BUworks at this time. It hasn’t come forward as a top priority.

We have an ongoing project to consolidate AD2 into AD.

Current State of Disaster Recovery Plan

- The review of the disaster recovery plan by this governance committee is an audit requirement.
- Our DR plan covers core services by IS&T. Our scope needs to be broadened and expanded.
- The plan is for a generic disaster/business infrastructure to be able to recover data in case a data center is destroyed. There are a variety of scenarios.
- With SunGuard, there is a 48 hour recovery time. They also have a subscription model that is on standby.
- In the event of a disaster, we can move the data center function to Philadelphia.
- The DR facility is a bank of resources that we can load our systems on and run from there. The systems to first be transferred are services that need to be online to protect the schools assets.
- Business continuity plans are departmental affairs. IS&T has not coordinated with these plans as of yet. It is our long-term goal to do outreach to other departments to help put their data files together.
- In the long-term, DR & BC will be promoted throughout the campus. Inputs for its improvement will be sought.
- Applications that don’t run on the mainframe are not included in the plan. The focus is to recover central services.
- Regarding Holyoak, there is a cap on the amount of non-research computing permitted. 20 percent of the data center is on generated power. Taking from
that 20 percent to do DR systems is problematic. Holyoke is for replication of research data but is not a site for the mainframe.

- We have oversight as to how the data center is run. The first step is business impact assessment for recovering from an outage. What will be our ability to access email and maintain other services to students?
- The planning process begins after the research has been completed. Testing and maintenance is the most essential piece in disaster recovery. This is where we need to be diligent.
- The next DR test is due to be completed in April. Our objective with DR is a business decision based upon an impact analysis at the highest level based on the business need.

**IT Planning: Sample Plan Discussion**

- There are two reference strategic plans: Brown University’s and Case Western University’s.
- The Brown Plan is the older of the two plans. It’s a more IT centered plan that lays out 3 basic priorities.
  - Invest in technology
  - Ensure their ability to prevent disaster
  - Develop, sustain and replace core services
- The Brown plan feels more like a remediation plan that will not be inspiring to the community. It’s more like central and local IT talking to each other. Most reactions to the plan is that it’s too in the weeds, IT centric and uninspiring.
- Improvements with uptime need to be addressed. It’s similar to the plan for SMG.
- There’s a lot of stuff in the Case three year plan. They’ve got a lot of progress indicated; BU is doing a lot of the same things. They provided a list of projects and evaluations.
- We need sustainability for this like network research. We cannot dismiss the level of planning that is needed.
- What sort of innovative collaborations can we do and how will we align ourselves with the goals of BU.
- The Case themes are focused on data and analytics. A broad initiative composed of multiple things. It includes some real voices of faculty. The content of the Brown plan is more basic.
- The Brown plan doesn’t contain much around collaboration. The Case plan is more of where we need to be focused.
- We need a plan for legacy systems.

**Email Encryption Gateway**
• We want a gateway device that plugs into our email gateway.
• A system like this would tell us if there is sensitive data being sent via email.
• The solution has the ability to get the idea of how much we’re looking at in terms of data content.
• The specific rules for this POC will be written by Quinn and sent out for discussion.