UWIAC	**Date: 10-18-2016** **Time:** **Place:**

Agenda

1. Final Phase 2 Scope
    a. Review of success of Phase I
    b. Security Program
    c. Development of additional polices & procedures
    d. Address costs and campus resource availability
2. Phase 1 Implementation report
3. Information Security Awareness report
4. ITMC

Meeting Notes

Topic: Final Phase 2 Scope

Decisions	***Action items (who, what, when):***	***Open Issues:***

TOPIC: Phase 1 Implementation report

TOPIC: Information Security Awareness report		
Decisions	***Action items (who, what, when):***	***Open Issues:***
TOPIC: ITMC		
Decisions	***Action items (who, what, when):***	***Open Issues:***

I'm at the annual Gartner Symposium and took the opportunity to have a 30 minute 1-1 session with one of their security analysts. Bob Beck joined me for the last 10 minutes or so.

I posed for the analyst a few of the balances that we've been trying to achieve.

- Write More Policies vs. Implement Existing Policies

His advice was that it was better to have fewer, enforceable policies.

- Apply the Policies to our Bigger Systems or First Do an Inventory of Distributed Systems to Look for Risk?

His advice was to try and first do a high level inventory, the kind of thing that would only take a few days to a week. He said very few organizations have implemented configuration management tools and he would not recommend that we stop to do that. His suggestion was along the lines of some basic scanning to look for systems outside of central IT followed by some interviewing to find out who is managing them.

- Should the advice that's contained in what we have been calling the program document be mandatory or not?

He recommended that the information security program is the sum total of the policies, procedures, guidelines, activities, etc. The kinds of materials in our 'program document' should not carry the same compliance requirements as policies. That document is not the same as the overall program.

- I asked for advice on implementing the existing policies and procedures.

He suggested starting with a couple of the institutions to learn about what it actually takes, instead of doing all institutions at once by a certain date.

- I for his feedback on the compensating control language in the procedures.

He suggested that controls that would *only* affect the risk profile at one campus could perhaps be signed off by that campus. I countered that our discussions have revolved around how a risk to one campus could potentially also affect other campuses via the network. I expressed a bit of surprise that the institutions have not been asking for compensating controls. He said that he expected that the institutions would not pay attention to compensating controls until they were audited and found to be without any, or at least without documentation for their compensating controls.

A number of times he cautioned against mandating what cannot be accomplished because such policies and procedures would simply be bypassed.

He suggested that there be common systemwide policies and that the institutions create their own policies for what the systemwide policies don't cover. I stressed that Internal Audit has said that they will audit against the systemwide policies (first), not campus policies, which he thought made sense.

He recommended that auditors focus their attention on the resource owners. Then, if those owners have compliance issues IT can be part of the solution.

Please let me know if you have any questions.

— David

David Stack PhD
Interim Associate Vice President & CIO
University of Wisconsin System
1552 Van Hise Hall
1220 Linden Drive
Madison, WI 53706
(608) 265-4622