ITAC Meeting  
April 12, 2012  
GSC Rm.: 2605  8:30-10:00

Attendees: David Sweeney, Tom Lyster, Willis Marti, Allison Oslund, Eric Beck, Jim Bousse, Juan Garza Jim Rossier, Adam Mikeal, Andy Bland, Ron Szabo, Becky Carr, Erin Bender, Henrick Schimideche, Fred Fisher, Andy Bland, Stephen Balfour, Becky Carr, Dr. Marchbanks, Steve Conway, Mark Harris

Guest Attendee: Student affairs: Micheal Henricks

Item 1: Approval of Minutes: Minutes approved unanimously

Item 2: Announcements: Ron Asks members to please email officers with ITAC retreat topics

IT Policy involvement of ITAC: Ron Szabo announces new ITAC role in collaborating IT Policy

- ITAC is committed to being a part of the process.
- Executive Steering Committee had further discussions with Deborah Dandridge. It was agreed ITAC will be involved in IT policy at almost point of IT policy ingress.

Methodology:

- IT Risk Management will be creating a website listing both the upcoming Saps (which follow a 3 year review) and rules (which follow a 5 year review): to allow entire campus community ability to review.
- IT Policies that are up for review will be posted 3-6 months out from date of review deadline
- Additionally on website, IT policy flowchart will be displayed
- The way to honor and commitment is to create a standing IT Policy committee which will serve as a working body ITAC standing committee will stand as liaison between ITAC to ITRM.
- As IT policy is up for a review, the subcommittee will review and decide if any necessary input, revision, or recommendations are is necessary from an ITAC operational aspect.
- Deborah Dandridge ITRM’s lead policy analyst has asked that any revisions be returned to her one month prior to policy review deadline.
- ITAC has asked for involvement, and now has 3 areas in the process to affect IT policy.
- ITRM starts the process from an enterprise level, and ITAC, reviews for an operational level at two places in the flow chart, and has a voice as well as IPC Administrative level with Henrick’s participation as ITAC’s IPC rep.
- During the process there will be back and forth sharing drafts between ITAC’s IT Policy subcommittee. IPC has indicated they welcome and will incorporate /include committee’s suggestions
- Deborah Dandridge asked ITAC to honor the return of input/recommendations 1 month prior to the review date.
IT Policy involvement of ITAC: Ron Szabo announces new ITAC role in collaborating IT Policy cont

- Ron Szabo asked to form an IT Policy subcommittee and solicits membership: Henrick Schimideche, Ron Szabo, Erin Bender, Steve Conway, and post meeting Jeff McCabe volunteered to serve on the committee.
- Steve Conway added to please, as writing SAPs, to include and be mindful of other system parts/branch rules. Willis Marti agreed that will happen and stated that heard the same request while in Qatar. There will be an attempt to develop/improve the SAP contextual composition.
- The committee will work to tweak collaboration with ITRM and IPC.

Item 3: ISAAC: Susan Cook IT Risk Management

- Susan Cook reminded folks it is ISAAC Season
- Susan requested to please submit assessment transfer request to ITRM now. For example any changes to dept., name change, consolidations, etc. (The goal is to make sure the right people receive correct assessment) Once received, ITRM will take 1-2 business to make the changes.
- Susan reminded ITAC members that exclusions are applied on a yearly basis. Susan asked members to review requirements now, and if you feel that your department received exclusion last year, and wish to do so this year, you have to reapply.
- If you have social security numbers, or have other valid business needs that might meet the outlined prerequisites for exceptions please apply promptly.
- ITRM website: exception form and other helpful information:
  

- Complete the written exceptions forms and submit, ITRM’s response turn around takes 7-10 days to process via email. The dept. IT Admin receives the reply back from ITRM. Susan explained the departments must keep that form on file as well.
- Susan reminds everyone to use net ids, all old data has been wiped, everyone start assessments over clean.
- Please proactively help faculty members with risk assessment. If they complete incorrectly, probably not going to be executed thoroughly and they will not be happy with the assessment they receive from ITRM.
- Discussion continued within the committee about confidential data, how to make sure faculty, students, staff’s assessment completed accurately.

Training

- ISAAC Training Sessions available on line: webinarlink
- Holding a training session in GSC as well as on main campus. Check ITRM’s website for dates and details.
• ISAAC: Susan Cook IT Risk Management cont.
  • Training Information will include such information about the policy relation between SAPS and TAC compliance and how to identify resources to begin assessment,
  • Susan updated ITAC that UINs are no longer confidential- considered directory information with Student name, not an exception.
  • ITRM is requesting ISAAC assessment review by May 31st if possible. Thus, ITRM can then ensure punctual feedback
  • ISAAC making some changes for next year. Training Announcements will be sent out on ISAAC list serv

General Questions or assistance please contact ITRM:
https://isaac.tamu.edu/ISAAC/2012/index.cfm
Isaac-support@tamu.edu or 979-845-0254

Item 4: IT Trends:

Committee engaged in general dialogue concerning IT Forum speaker. There were some interesting Discussion/ Comments regarding the, “Bring Your own Device (Disaster) to work presentation.” However some members felt the tools to secure the problems were not addressed. Some interesting topics were raised:

• Android users under huge attack, up 3000 percent, if download aps increase vulnerabilities- how or do we inform campus community?
• Adam Mikeal stated perhaps the need to inform community of risks of IPhone.
• A suggestion of adding a slide in the security awareness training about IPhone use
• Additionally committee is aware if there is a concern relative to research - individuals are creating own data that is not secure; further complicating/compounding problem
• Allison Oslund asks Willis Marti to decide on policy of usage
• Willis Marti questions the committee: “Do we focus on the device or the data in defining the strategy? The goal is to try to define the strategy to educate users. “

Agenda Item 5: Application Security

• Willis Marti stated after running vulnerability scans, it was determined old software is presenting/ creating a strain on the security devices. ( If possible, need to run the most the current version of software) Departments and groups have been notified.
• Willis stated he understands there are many variables that have caused this to occur: different version of software running on our devices, due to software provided from the vendor or embedded in appliance, patches provided etc.
• A question is how should CIS determine which out of date software running on host machines can create vulnerability to open ports, and how much scope does the CISO have to assist is that decision?
• How many older versions do we claim/allow hosts to run?
Application Security cont.

- David Sweeney asks, Can we categorize/ prioritize software vulnerabilities by criticality?
- Can departments receive info if these patches are critical or not? Willis Marti responded “Yes,” Common Vulnerability Data Base is an available tool - look up and see versions not critical
- David Sweeney states if there is a problem with a system, notified from security that software is weak and told need to update software; can a reasonable amount of time be put on that request that both maintains security and allows for a practical amount of time for the department to remedy, update, and patch software?
- Presently David Sweeney’s group evaluates software monthly.
- Problem is from an enterprise standpoint, it has to be realistic. Can a 1 to 2 month time frame be implemented to apply patches/upgrades unless critical?
- Willis asks ITAC to assist in deciding that policy. Mitigation always an option, firewall in front, etc.
- Willis Marti stated can determine vulnerability, come up with a useable, realistic application. Rather, Willis asking not advocating a new rule, rather wanting to define how much to enforce existing rule.
- Committee agreed criticality will define/ framework of vulnerabilities and reinforcement of existing rules. Subsequently, give a dept. a time frame to update software, applications, post patch installations, etc.
- Ron Szabo tabled further discussion and asked for committee members to come up with concrete examples for specific applications to be examined.
- Willis Marti made one last comment that once British Telecom completes scan/ audit, that will probably offer guidance to this issue.

Agenda 6: Officer Elections

- Adam Mikeal removed himself from the chair position nomination, and accepted only the vice chair nomination. Some individuals not present sent in email votes.
- Paper ballet voting system utilized, names listed based upon previous nominations. After paper ballots issued, members voted manually, and voting tabulated.
- ITAC Officers for the next 2 year term:
  - Chair: David Sweeney
  - Vice Chair: Adam Mikeal
  - Secretary: Andy Bland
Item 7: Sub Committee Reports:

- **Password Committee** disband: ITAC committee agreed
- **ID Management**: Fred Fisher suggested the committee should disband; not sure the committee ever had an impact on the process being executed by Cheryl Cato’s group.
- David Sweeney suggested the committee can have an influence.
- It was decided there would be added benefit to invite Cheryl Cato’s group for an update regarding ID Management office.
- Table disband until after Cheryl Cato’s ID Management group briefing

Current Active Sub committees:

- **Business Continuity**: Presented a draft of committee’s charter, deliverables, etc.
- **Essential Elements**: Juan working with committee refining document, and will provide feedback. Presently committee continuing work with auditor’s guidance
- **Newly formed IT Policy/ Sap Committee**