CoALS Technology Security and Compliance Committee
October 21st, 2021
1:00 p.m.

Attendance:

Members			
Kerry Pickens (Manager Policy & Compliance)	Tim Ramsey (Associate Director of IT)	Mitchell Morgan (Manager Service Area 3)	Keith Wicker -Chair (Information Security Officer)
Gene Curtiss (Manager Systems & Infrastructure)	Barry Stratta (Manager Software & Applications)	Sushant Patil (Security Analyst – Security & Risk)	Michael R. Foggitt (System Administrator II)
Omar Valenzuela (IT Manager II)	Aaron Rodriquez (Manager Service Area 2)	_	_ name (Title)

Also in Attendance:

Sarah Hoving -IT Governance Coordinator

Minutes

Item 1: **Approval of Minutes**
Description: Review and approval of minutes from previous meeting.

Item 2: **New Business / Special Topics (15 mins)**
Presenter: Keith Wicker
Description: Reorganization of AgriLife IT Security and Compliance Team – review of team member areas of focus

- New AIT Security Group position approved – primary focus CoALS Ivanti / Nessus support
- Kerry will continue to focus on policy and compliance/ Risk Assessments for CoALS and Agency side
- Sushant- has agreed to take on the Research Migration Project with the help of Tim: on project planning phase (Will ramp up starting January of 2022)
- Cade- Primarily SMP Nessus; very high-level knowledge on instrumentation and putting together exceptions and counseling; providing guidance and counseling, to researchers to maintain compliance in that area
- Phillip- Sophos Antivirus administrator and we recently have gotten Phillip access to crowd strike.

Item 3: **Status Update (15 mins)**
Presenter: Kerry Pickens
Description:

- **FY21 Non-IT Professional Risk Assessment**: Report from ALP of users with admin rights have been uploaded to TAMU IT RA Google drive. Deadline had been extended to October 30th.
    - Report included admin rights to the desktops, not the servers or applications
    - We did find that there were two faculty that had completed server assessments and Gene was not aware that those two people had completed the server assessments.
    - One being a researcher that was not required to do that assessment. Have been told that there weren't any faculty in codes that had admin rights to the server, so it was good that we were able to find that out.
- **Prioritization of Risk Remediation** – consolidated the RA remediation tasks, identifying resources, understanding complexity (determines number of people involved in completing the remediation), risk level, realistic timeframes (by quarter).
- **Refresher on Risk Assessment Phases**
    - Phase I - Inventory
    - Phase II – Assessment
        - next risk assessment will start in February and we should find out in November with the schedule for that will be
    - Phase III – Report
        - when discussing prioritization of risk remediations, talking about the risk remediations for the IT professionals
        - Report will be provided to Patrick Stover, Alan, Keith

Presenter: Keith Wicker

- **Ivanti Status for CoALS workstation migration** – To date, the number of workstations migrated with Ivanti installed (For 02 Assets)
    - Reminder Invanti is just in monitoring mode right now, remediation will start probably first or second quarter 2022
    - College PCs in Ivanti: 327
    - College PCs in Domain: 671
    - College PCs remaining: 344
    - Overall Percent Complete: 48.7%

- **Crowdstrike** - Security Team (Philip) now has view access to begin monitoring TAMU CrowdStrike tenant for CoALS / working with build team to install on new CoALS Mac OS devices for end point protection

- **Inventory Ad Loc cleanup**: 02 (academic mission) vs 06 (research) assets - scheduled to begin 1st quarter 2022. – Asset inventory Ad Loc determines which CISO office asset is beholden to for policy / standards: TAMU IT CISO (02) or AgriLife CISO (06). Inventory is also Phase II of FY22 RA.
    - Want to clean up the inventory such that any asset that's in O2, any that has the smallest amount or any amount of research activity use, is going to be moved over into 06. It has to be 100% proven that it's used for academic purposes for it to remain in O2. We want to maximize moving all of the assets that we can't over to 06

- **Research Migration Project** –
    - Description: Meet with PIs to discuss research computing environment, inventory research assets, install Ivanti assessment tool, install Sophos AV, review SMP requirements, IT Policy Guide, and introduce ARC
    - SMP updates to support CoALS Researchers - Cade
    - Project Manager: Sushant
    - Project Phase: Planning
    - Target begin date is Jan 2022
    - AgriLife Research IT Policy Guide update - Kerry

- **BCBP Firewall install - Risk remediation project** by the server team: BIOBIO - PCs paired with NMR devices – Gene / Jeff / Mike
    - **Focused on risk remediation**

Item 4: **Policy Update (15 mins)**
Presenter: Keith Wicker

TX-RAMP – DIR certification program for cloud vendors – similar to FedRAMP – focus primarily on SaaS vendors with **mission critical / confidential data** -- all cloud apps utilized must be TX-RAMP certified by Jan 2022. Yet…the TX-RAMP program requirements document is still in draft for comment from CIOs / CISOs from around the state.

- Most important action now is for CIOs to renew any cloud contracts classified mission critical and confidential data before Jan 2022. Expected TX-RAMP publication date by end of

2021. More details hopefully to come next month.

- One of the challenges with cloud based applications is that we don't typically have much visibility into their security and compliance, policy practices
- With TX-Ramp, transfers the risk from Texas A&M Agrilife over to the vendor, meaning the vendor has to continually prove that they are compliant with Texas DIR controls.

TAMU System - Revised Incident Reporting Standard (IR-6):
Based on recommendations from System Internal Audit, the incident reporting standard (IR-6) has been revised, published 10/15/21.

- (Unchanged) Any events where the confidentiality, integrity, or availability of a major system-owned or -managed information system, or a system processing confidential information, is potentially compromised are reportable.
- (Clarified) This includes privacy incidents that do not impact the availability of information systems and any incidents involving industrial control systems or operational technology.
- **(Added) Initial notification for security incidents must occur within four hours of discovery by the system member or notification to the member by the SOC.**
- **(Added) Initial notification must be made via the Information Security Incident Reporting Portal at https://cyber-infosharing.tamus.edu**

Item 5: **Action Item Summary**
Description: List of action items, assignee, objective, due date.
A. Provide TAMU Network Upgrade Project Status – Tim

Item 6: **Close**
Description: Adjourn meeting on time noting actions and conclusions of meeting.