

# Research Computing Advisory Committee

Minutes Sep 10, 2018 (taken by Erik Deumens)

**Present:** Paul Avery, S. Balachandar, Brad Barbazuk, Peter Barnes, Hai-Ping Cheng, Erik Deumens, Lauren McIntyre, Alberto Riva, Plato Smith, Jack Stenner

**Guest:** Chad Young (Information Security Office)

## Agenda

1. Presentation by Chad Young from the Information Security Office in UFIT on
  - a. the IRM (Integrated Risk Management) program,
  - b. the plans for phase 2.0 of the IRM website <https://irm.ufl.edu> to provide a guided search capability for researchers to classify data and find resources and services that are approved to work with the selected type of data, and
  - c. the plans to streamline and simplify the data gathering from multiple systems (UFIRTS, myIRB, etc) into the risk management tool (Archer) so that people are not asked the same questions multiple times.

Chad Young offered to come back to the committee with updates.

2. Conclusion of the review and discussion, over the summer from the July and (virtual) August meetings, of the drafts for revised policy and two standards pertaining to IT risk assessments. The current policies can be found at

1. Risk management policy v2.0 -> v3.0

<https://it.ufl.edu/policies/information-security/risk-management-policy/>

2. Information Security Risk Assessment Standard v1.0 – v 2.0

<https://it.ufl.edu/policies/information-security/related-standards-and-documents/risk-assessment-standard/>

3. System Security Plan Standard v1.0 -> no changes suggested yet

<https://it.ufl.edu/policies/information-security/related-standards-and-documents/system-security-plans-standard/>

## Discussion

**IRM presentation** The committee is looking forward to the search capability on the IRM website. However, the committee cautioned against making things more complicated and suggested an approach that would gather information from multiple tools for risk assessment instead of putting risk assessment at the head of the workflow. The committee welcomed updates as the work progresses and would like to participate actively in the process.

**IRM Policies** The committee discussed and approved the drafts to go forward to other committees and forums, such as ISAC (Information Security Advisory Committee), IT@UF directors of distributed IT units, Faculty Senate IT Committee, etc. When the final draft is ready, RCAC will look at it again before it will be established and published as the new policy.

Because the previous policy led to implementations with significant impact, the committee wanted to make sure that such things do not happen again. A 5 business day limit for getting a preliminary report for advanced assessment was put in the standard. The committee considered that as the organization matures and the various use cases have been explored, it will be possible to give a quick preliminary assessment that has a very small probability to overlook something that cannot be effectively remedied after projects have started.

### **Summary of changes from the existing policy**

The current policy has scope that can and has been interpreted very broadly such that its implementation became very obstructive to business processes of the university, especially the ones involving research and in particular research without any restricted data, where the risk is minimal and the value of risk assessment imposed by the policy is questionable. That consideration is the main motivation for the proposed changes, with the goal to make the process more focused and less burdensome.

- The new policy draft identifies two classes of risk assessment: basic and advanced. Basic risk assessment does not require a request in Archer; advanced risk assessment is mainly triggered by the presence of restricted data and does require a request.
- The requests should primarily be filled out by ISM and security specialists with minimal burden on faculty and staff.
- The risk assessment standard is clarified and made more explicit.
- The system security plan standard should be NIST 800-18. The document can be removed, or simply state that NIST 800-18 is the standard.

### **Organization**

- Next meeting will be on Monday October 1, 2018 in the usual conference room NPB 2304 from 1:30 – 2:30 pm. The meeting will be Zoom enabled for virtual attendance.