Frequently Asked Questions about the UCI Security Risk Assessment Questionnaire (SRAQ)

- **What is the SRAQ?**
  - The SRAQ is a tool (Word document with macros) to guide you through the security risk assessment and review process for a system, to help you think about and document the classification, threats, countermeasures, and other key information required when assessing risk. It also provides a worksheet for risk acceptance and action items for risk reduction. It is primarily used as a self-assessment tool, but gathers the information required for external audits and security reviews. It can also be given to a vendor during an RFP or contracting phase for them to document how they will protect your data.

- **What is the scope of an SRAQ?**
  - Whatever you want it to be, keeping in mind the broader the scope, the more detail and nuance you'll have to describe in the control description fields to be accurate. But a "system" could mean a single server, application, or database, or a system could mean a composite of all the related elements that together achieve a specific business need.

- **Where can I download the tool?**
  - [http://security.uci.edu/security-plan/plan-resources.html](http://security.uci.edu/security-plan/plan-resources.html)

- **What is the "LITE" version vs the regular version?**
  - The "LITE" version is the same document except has the detailed items under each control section removed to lower the number of pages. It may be used for a low or medium risk system, however any high risk system should use the full version. Also even for low/medium risk assessments, having the detailed items help explain each control section and can help answer questions people have filling it out, even if they don't choose to address each detail.

- **Responsible Parties: Who is the Proprietor, Custodian, and Information Security Coordinator?**
  - [http://security.uci.edu/security-plan/plan-roles.html](http://security.uci.edu/security-plan/plan-roles.html)

- **Information Classification: Which data elements do I need to include?**
  - At a minimum include all data elements in the system that are classified as "P4" or "P3" based on [http://security.uci.edu/security-plan/plan-classification.html](http://security.uci.edu/security-plan/plan-classification.html). You can also include "P2" or "P1" classified data as space permits, especially if it has special availability requirements (downtime tolerance of hours or less).

- **What is the purpose of the Identify Threats section?**
  - This section allows you to think about the different ways an attacker could compromise your system specifically and identify exactly what you are trying to protect the system from. Then later you can tailor security safeguards specifically for those threats rather than blindly applying generic ones of possibly little value.

- **Which threats should I consider?**
  - Default Threats: The first five threats are generic security threats that commonly apply to systems that are included by default.
  - Custom Threats: Other threats specific to your system or more detailed specifics to the default threats that are important to highlight for your system.

- **How do I properly complete the Identify Threats section?**
  - Activate the checkbox on the left for each threat that is relevant to your system.
  - Impact- select high/medium/low to describe the impact to the campus if the threat was successfully realized.
  - Likelihood- select high/medium/low to describe the likelihood of the threat being successfully realized.

- **How does the Risk Level Classification work?**
- A macro is run to calculate an overall risk level of the system based on the data classification, downtime tolerance, threat impact, and threat likelihood.

**Are there sample network and data flow diagram templates I can use?**
- Yes, sample diagrams can be found here: https://wiki.oit.uci.edu/x/b4CdJQ

**What is a Control?**
- Control is just a fancy term in the information security domain to refer to any safeguard or countermeasure that reduces or eliminates risk imposed by a threat. They could be technical, physical, administrative, preventative, detective, and/or corrective in nature.

**Controls: What do the High/Med/Low mean in the detail columns?**
- Use the column based on the overall risk level classification for your system.

**Controls: What do the RQ/RM/OP mean in the detail columns?**
- These denote whether that specific control is required, recommended, or optional to implement in your system based on the applicable risk classification column. RQ means Required, RM means Recommended, OP means Optional.

**What should I include in the “Comments” field for each Control?**
- Write in detail about what you have in place that addresses that control, if the scope is larger and that control applies to multiple parts of the system, talk about each part. For any control details marked as "Partial" make it clear what is being done and also what isn't being done.

**What are the Action Plan and Residual Risk Acceptance sections for?**
- Each Control that is Required for your risk level classification but not fully met (“Partial” or “None” status) should either have an associated action item defined for it in the Action Plan section or formal residual risk acceptance in the Residual Risk Acceptance section.

**What is “residual risk”?**
- Residual risk is the risk remaining after a security control is implemented or chosen not to implement.

**Who is appropriate to be the Risk Acceptor for residual risk?**
- It should be the appropriate risk decision maker for the system and data, keeping in mind the person is usually the Proprietor / data owner, not the IT person. It is important to actually name them and make them aware of it.

**What if I don't meet all the requirements, am I being graded?**
- No, this isn't an exam you are being graded on. It is an honest analysis of the security risks in your system, documenting what you are doing about them, identifying gaps, and putting together a plan to address those gaps. There is no perfect system and no perfect SRAQ.

**Someone else handles (fill in the blank), do I have to worry about it or can I just assume it is getting done and mark the Control "Full"?**
- Yes, you need to worry about it and don't assume anything. Often we find that the biggest gaps on campus are when groups assume or take for granted that someone else is doing something when they aren't fully. Even in the world of IT commoditization, including the central services that OIT provides, the system or data owner must verify that the group they are outsourcing responsibility to is doing what you need them to do from a security perspective. Unless the scope was extremely small, a single person cannot complete an SRAQ in a vacuum. You must communicate with all of the various responsible parties and validate, sometimes even asking for evidence, that they are fulfilling the controls they are required to for you as a customer. Ideally these security controls would be a part of every SLA/OLA/MOU that each central commodity service has that you could easily refer to and periodically verify, but for now you will need to ask for that information each time.

**How do I export data from the SRAQ into text format?**
- You can execute a macro that exports the SRAQ form data into text/csv format by doing Ctrl-Shift-E. It saves it to a file with the same name as the Word doc but with a .txt. extension.

**How can I add extra rows to the Action Plan and Residual Risk Acceptance tables, or otherwise add any extra content?**
- By default, the SRAQ tool is restricted to only allow you to enter information in the specified form fields. If you need extra rows you may consider just linking to another document, or you can edit the
What is the Application Security Checklist, does it replace the SRAQ?

- No it doesn't replace the SRAQ, it is to be used as a supplemental resource and goes into more detail about what is needed to address SRAQ Control #6. It is geared toward software developers when reviewing their application code, and action items can be rolled up into the overall SRAQ. It also links to a lot of external OWASP and CWE/SANS resources as a training reference for programmers who aren't familiar with secure application development.