Table of Contents

What is the SRAQ: .......................................................................................................................... 3
SRAQ Self-Assessment Process: ................................................................................................. 3
Four Key Areas: .......................................................................................................................... 3
Common SRAQ Misconceptions: ............................................................................................... 4
The SRAQ Document: .................................................................................................................. 4
  Section 1: Information System Name ...................................................................................... 4
  Section 2: Responsible Parties ............................................................................................... 4
  Section 3: General System Description/Purpose ..................................................................... 5
  Section 4: Information System State ...................................................................................... 5
  Section 5: System Management ............................................................................................. 5
  Section 6: System Audience .................................................................................................. 6
  Section 7: Number of Users ................................................................................................... 6
  Section 8: Information Classification ..................................................................................... 6
  Section 9: Identify Threats ...................................................................................................... 7
  Section 10: Risk Level Classification ..................................................................................... 8
  Section 11: System Architecture Diagrams .......................................................................... 8
  Section 12: Controls ................................................................................................................ 9
  Section 13: Action Plan .......................................................................................................... 10
  Section 14: Residual Risk Acceptance .................................................................................. 11
Appendix A – High-Level Control Guidance ........................................................................... 12
SRAQ User Guide

This user guide has been designed to assist individuals with completing the SRAQ. If you have additional questions that are not answered within this document please reach out to securityreviews@uci.edu.

What is the SRAQ:

SRAQ stands for Security Risk Assessment Questionnaire. It is a self-assessment tool designed to help individuals to understand the security posture of their system and to identify ways to make their systems more secure. The latest SRAQ template can be found on the security website: https://security.uci.edu/security-plan/plan-resources.html

SRAQ Self-Assessment Process:

Four Key Areas:

When filling out the SRAQ there are four key areas of the document that are the most important parts of the assessment. For the SRAQ to be fully completed these four areas need to be done:

1. Identifying Threats
2. Developing Diagrams
3. Filling in Controls
4. Creating an Action Plan
Common SRAQ Misconceptions:

There are a few common misconceptions individuals have about the SRAQ. Those misconceptions are:

- **Every question must be answered** – The SRAQ is not a one size fits all document and there are going to be some controls that don’t apply. It is okay not to fill everything out. What’s most important is you fill out the controls related to the threats and major concerns you have identified.

- **Must have action items and gaps addressed** – At the end of the SRAQ you will have a list of security gaps. An action plan needs to be developed with those security gaps, but the items within the action plan don’t have to be mitigated for the SRAQ to be completed. An action plan with action items and target dates just needs to be created.

- **Must be reviewed/signed-off by Security to be “complete”** – OIT Security does not need to review or sign-off on the SRAQ for it to be completed. The SRAQ is a self-assessment and is considered completed when the SRAQ is submitted to securityreviews@uci.edu or posted to the individual SRAQ wiki page to be cataloged.

- **One and done** – Systems are always changing and it is important for them to be re-reviewed. We recommend the SRAQ be conducted every 2 years or whenever there are any major system changes.

The SRAQ Document:

Section 1: Information System Name

- This is the name of the system.

Section 2: Responsible Parties

- **Unit Head** – This is a senior level individual on the admin side. The person who is accountable for protecting the information. They are the one who accepts any risk related to the system.

- **Proprietor** – This is a senior level individual on the admin side. The person who is responsible for classifying the data and understanding the security and legal requirements for handling the data.
• **Custodian** – This is a senior level individual on the technology side. They are the one who is responsible for implementing the technical controls. This person can be at a director level.

• **Information Security Coordinator** – This individual is the system security point of contact. They are responsible for validating that security controls are being implemented. This is usually the person who fills out the SRAQ.

• **Project Lead** – This is usually a technical individual. This person is the system lead that is delegated from the Custodian.

• **Extra Roles** – This is for any additional individuals that you feel are important to list.

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit Head</td>
<td>Responsible Party Name</td>
<td>Contact Information</td>
</tr>
<tr>
<td>Proprietor</td>
<td>Responsible Party Name</td>
<td>Contact Information</td>
</tr>
<tr>
<td>Custodian</td>
<td>Responsible Party Name</td>
<td>Contact Information</td>
</tr>
<tr>
<td>Information Security Coordinator</td>
<td>Responsible Party Name</td>
<td>Contact Information</td>
</tr>
<tr>
<td>Project Lead</td>
<td>Responsible Party Name</td>
<td>Contact Information</td>
</tr>
<tr>
<td>Extra Role</td>
<td>Responsible Party Name</td>
<td>Contact Information</td>
</tr>
<tr>
<td>Extra Role</td>
<td>Responsible Party Name</td>
<td>Contact Information</td>
</tr>
</tbody>
</table>

Section 3: General System Description/Purpose

• Sections 3 thru 7 are informational about the system. These sections help the unfamiliar reader understand the scope of the assessment.

• Under the System Description section you want to include a short paragraph about what the system does. Any important descriptive system information can be entered here. Some examples include:
  - The function or purpose of the system
  - Which Unit(s) use the system

Section 4: Information System State

• Mark whether the system is in production or under development.

• Legacy System – A system is considered a legacy system if it is no longer supported by the vendor and will be replaced in the near future, or if the system is super old and complexed and can’t be replaced because it will break something.

Section 5: System Management

• Individually managed – supported by one individual

• Department managed – supported by an individual unit or department
• Centrally managed – supported by a campus central service.

Section 6: System Audience

• This is the type of individuals who use the system. (Small Group of Users, Single Functional Unit, Campus, or the General Public).

Section 7: Number of Users

• This is the number of individuals who manage the system. The best way to tell the difference between the number of users and the system audience is to think about uci.edu. The audience for uci.edu would be the general public and the number of users would be the small group of people who actually manage and support the system.

Section 8: Information Classification

• Information Type – List out the information types for the system. Some examples would be SSNs, Financial Account Info, Student Info, etc. The SRAQ is NOT asking for the individual data elements, just the high-level data types.

• Enter the Protection Level (P1, P2, P3, or P4) and Availability Level (A1, A2, A3, or A4) for each information type.
  o Information about the different Protection Levels and Availability Levels can be found here: https://security.uci.edu/security-plan/plan-classification.html

  ▪ Protection Level Classification (P1,P2,P3,P4)
    • P1 – Publicly available data
    • P2 – Information which may not be specifically protected by statute, regulations, or other contractual obligations or mandates, but is generally not intended to be public.
    • P3 – Information protected by contract obligations, or information considered proprietary in nature such as intellectual property.
    • P4 – Information protected by contract, statute, and regulation.

  ▪ Availability Level Classification (A1,A2,A3,A4)
    • A1 – Loss of availability poses minimal impact or financial losses.
    • A2 – Loss of availability may cause minor losses or inefficiencies.
    • A3 – Loss of availability would result in moderate financial losses and/or reduced customer service.
    • A4 - Loss of availability would result in major impairment to the overall operation of the location and/or essential services, and/or cause significant financial losses.
Section 9: Identify Threats

- Threat modeling is one of the most important parts of the SRAQ. The threats that you are most concern with will help identify which security controls are the most important to focus on. You will want to focus on the controls that will protect against your biggest threats.

<table>
<thead>
<tr>
<th>Information Type</th>
<th>Protection Level Classification P1/P2/P3/P4</th>
<th>Availability Level Classification A1/A2/A3/A4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Modeling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threats</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Five generic threats are given as part of the SRAQ as a starting point. These five threats are:

- Cyber Attack
- Unauthorized Access to System or Data
- Human Errors (User, Maintenance, Operations)
- System Failure of Hardware, Software, Communication, Power, Air Conditioning...
- Environmental or Domestic Disaster (Fire, Water, Natural Disaster, Terrorism)

- Review the five threats and determine the likelihood and impact of each.
  - The **impact** would be the impact/damage if the threat occurred (low, medium, or high).
  - The **likelihood** is the likelihood that the threat can occur (low, medium, or high).
  For the likelihood you can think about the current controls in place and determine a rating based on that. If you don’t know what controls are in place you can
answer it as if no controls are implemented and then at the end of the SRAQ you can go back and adjust it. The likelihood doesn’t have to be perfect, do your best.

- You also want to identify 2 or 3 custom threats that are more specific to your system. To do this think about your system workflow, function, and process. What are a few things that could go wrong? What are the things you are most concerned about?

Section 10: Risk Level Classification

- A risk classification level of low, medium, or high will be automatically calculated. This calculation is based on the information types and likelihood/impact of the threats identified.

<table>
<thead>
<tr>
<th>Your Risk Classification is:</th>
<th>Click here to calculate your Risk Level Classification</th>
</tr>
</thead>
</table>

Section 11: System Architecture Diagrams

- Just like the identifying threats section, the diagrams are also one of the most important parts of the entire SRAQ. The diagrams help us understand how system devices are setup, how the system works, and what data is involved. Often times the diagrams help us identify key risks.

  o Here is a link to a few diagram examples: [https://wiki.oit.uci.edu/x/b4CdJQ](https://wiki.oit.uci.edu/x/b4CdJQ)
  o Things to include on the diagrams:
    - **Network Diagram**
      - Network segment subnet definitions
      - Relevant hostnames and IP addresses
      - Building routers and firewalls
      - Operating system types of hosts
      - Relationship to campus
      - Internet
      - 3rd party networks
      - Test environments
    - **Dataflow Diagram**
      - The hosts in your system that store or allow P3/P4 information to be transmitted through them
      - All data entry/exit points of the system.
      - Any flow of data within subsystems.
      - Arrows should denote the direction of data flow.
• The type of data, transport protocol, encryption, and any relevant access controls of data in transit.
• The type of data storage, encryption, and any relevant access controls of data at rest.
• Lines denoting boundaries of firewalled segments
  o When it comes to developing diagrams, the more information the better.

Section 12: Controls

• The SRAQ consist of 20 overarching security controls. The controls are prioritized in order by importance:

  o Control 1 – Inventory of Authorized and Unauthorized Devices
  o Control 2 – Inventory of Authorized and Unauthorized Software
  o Control 3 – Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
  o Control 4 – Continuous Vulnerability Assessment and Remediation
  o Control 5 – Malware Defenses
  o Control 6 – Application Software Security
  o Control 7 – Wireless Device Control
  o Control 8 – Data Recovery Capability
  o Control 9 – Security Skills Assessment and Appropriate Training to Fill Gaps
  o Control 10 – Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
  o Control 11 – Limitation and Control of Network Ports, Protocols, and Services
  o Control 12 – Controlled Use of Administrative Privileges
  o Control 13 – Boundary Defense
  o Control 14 – Maintenance, Monitoring, and Analysis of Audit Logs
  o Control 15 – Controlled Access Based on the Need to Know
  o Control 16 – Account Monitoring and Control
  o Control 17 – Data Loss Prevention
  o Control 18 – Incident Response and Management
  o Control 19 – Secure Network Engineering
  o Control 20 – Penetration Tests

• Each control is setup the same way. Below is a depiction of the control format:
The top part of the control is the main overarching control. There are 20 main controls within the SRAQ.

The comments section is where you want to provide information on what is currently being done to meet that control. If you are completing the SRAQ for a system in development you want to include information around what things are planning to be implemented.

Below the comments section are the sub-controls. Based on what is being done for each sub-control you want to select Full, Partial, None, or N/A (Not Applicable).

- Not every sub-control needs to be filled out. To the right of each sub-control is a guide based on the risk level assigned to your system from Section 10 Risk Level Classification.
  - RQ (Red) = Required = these are the controls you want to make sure to answer. These are the ones you need to be the most concern with.
  - RM (Yellow) = Recommended = these are the controls to consider based on the threats you have identified in Section 9 Identifying Threats.
  - OP (Green) = Optional = these controls are optional, but good to consider.

Section 13: Action Plan

- After going through the controls you will have a list of security gaps. These are the controls that were marked as partial and none. You don’t have to create an action item for every gap, but you want to create an action plan around the major security gaps. The major gaps are the ones that will help you protect against the threats you have identified earlier in the SRAQ process.
For the action plan to be completed you need a list of action items, an assignee for each action item, and target dates. We recommend action items to have a target date within a one year time period. The items within the action plan don’t have to be mitigated for the SRAQ to be completed. An action plan just needs to be created.

<table>
<thead>
<tr>
<th>Goals For Implementing Security Controls Reducing or Eliminating Risk</th>
<th>Related Controls</th>
<th>Assignee</th>
<th>Priority</th>
<th>Target Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Item</td>
<td>Related Controls</td>
<td>Action Assignee</td>
<td>Select one</td>
<td>Target Date</td>
</tr>
<tr>
<td>Action Item</td>
<td>Related Controls</td>
<td>Action Assignee</td>
<td>Select one</td>
<td>Target Date</td>
</tr>
<tr>
<td>Action Item</td>
<td>Related Controls</td>
<td>Action Assignee</td>
<td>Select one</td>
<td>Target Date</td>
</tr>
<tr>
<td>Action Item</td>
<td>Related Controls</td>
<td>Action Assignee</td>
<td>Select one</td>
<td>Target Date</td>
</tr>
</tbody>
</table>

Section 14: Residual Risk Acceptance

For the left over security gaps that don’t make it on the action plan, you want to pick-out 3-5 major gaps and capture them on the accepted risk table. For the SRAQ to be fully completed you want to share the results, action plan, and accepted risks with your Unit leadership and have them sign off on it.

<table>
<thead>
<tr>
<th>Lack of Security Control / Remaining Risk Description</th>
<th>Related Controls</th>
<th>Risk Acceptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Residual Risk Description</td>
<td>Related Controls</td>
<td>Risk Acceptor Name</td>
</tr>
<tr>
<td>Residual Risk Description</td>
<td>Related Controls</td>
<td>Risk Acceptor Name</td>
</tr>
<tr>
<td>Residual Risk Description</td>
<td>Related Controls</td>
<td>Risk Acceptor Name</td>
</tr>
<tr>
<td>Residual Risk Description</td>
<td>Related Controls</td>
<td>Risk Acceptor Name</td>
</tr>
<tr>
<td>Residual Risk Description</td>
<td>Related Controls</td>
<td>Risk Acceptor Name</td>
</tr>
</tbody>
</table>

Assessment Performed By: [Name, Date]
Assessment Reviewed By: [Name, Date]
Appendix A – High-Level Control Guidance

When filling out the controls you want to fill in what is currently being done. If you are completing the SRAQ for a system in development you want to include information around what things are planning to be implemented. Each control within the SRAQ has sub-controls. You can use the comment section to explain how the sub-controls are being met or partially met. Below are also a few things to think about in addition to the sub-controls when filling in the comments section of the SRAQ.

- **Control 1 – Inventory of Authorized and Unauthorized Devices**
  - Is there a device inventory of all the UCI supported devices that support your system?
  - What items are captured within the inventory? Does every device have an owner?
  - Is there a process to maintain/keep up to date the inventory?

- **Control 2 – Inventory of Authorized and Unauthorized Software**
  - Is there a software inventory?
  - What items are captured within the inventory?
  - Is there a process to maintain/keep up to date the inventory?
  - Would you be able to tell if an unauthorized software was installed on a device within your system?

- **Control 3 – Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**
  - Are there secure images for the devices that support your system?
  - Are the secure images regularly patched and reviewed for updates?
  - What happens if a device deviates from the secure image? Is there a documented process for this?
  - Is there a process/tool used to make sure the secure image hasn’t been falsely modified?

- **Control 4 – Continuous Vulnerability Assessment and Remediation**
  - Are vulnerability scans being conducted on your system devices?
  - Is there a remediation process for when vulnerabilities are identified?
  - Are system devices and software on a regular patch cycle?

- **Control 5 – Malware Defenses**
  - Is there a mechanism to detect if malware has been installed on any of the devices that support your system?
  - Are anti-virus and anti-spyware software installed on your system devices?
  - Is the anti-virus/anti-spyware software updated regularly?
• **Control 6 – Application Software Security**
  o Are your applications protected against OWASP Top 10 software vulnerabilities?
  o Is your application tested for coding errors and security vulnerabilities?
  o Is there a process to remediate findings?
  o Has developers attended a secure coding training?

• **Control 7 – Wireless Device Control**
  o Does your system use wireless? How is the wireless access point managed?

• **Control 8 – Data Recovery Capability**
  o Are backups being conducted? How often?
  o Are backups tested on a regular basis?
  o Are backups protected from unauthorized access?

• **Control 9 – Security Skills Assessment and Appropriate Training to Fill Gaps**
  o Is there any system specific security training for developers, administrators, or users?

• **Control 10 – Secure Configurations for Network Devices such as Firewalls, Routers, and Switches**
  o Are there secure configuration baselines for network devices? How are the baselines managed and maintained?
  o Do network devices use two-factor authentication?

• **Control 11 – Limitation and Control of Network Ports, Protocols, and Services**
  o Are port scans being conducted and reviewed to ensure only required ports are opened? How often are open ports reviewed?

• **Control 12 – Controlled Use of Administrative Privileges**
  o How do you manage administrative privileges and accounts?
  o Is there a review process to make sure privileges are still applicable? What happens if someone in the admin role leaves the University or changes job duties?
  o Are administrative privileged functions being monitored for anomalous behavior or misuse?
  o Is two-factor authentication being used for administrative access?
  o How are service accounts managed?

• **Control 13 – Boundary Defense**
- Are there any network filtering technologies employed to monitor and filter traffic?
- Are traffic blacklists or whitelists being utilized?
- Does remote login require two factor authentication?

**Control 14 — Maintenance, Monitoring, and Analysis of Audit Logs**
- Are logs currently being captured for your system?
- What type of logs are you capturing?
- Have alerts been setup? What happens if an alert is triggered? Is there a documented process to handling an alert?

**Control 15 — Controlled Access Based on the Need to Know**
- How do you ensure only those who need access to sensitive data has access?
- Do you know what type of data is stored on your system’s devices?
- Is the network segmented based on the risk of the information stored on your system servers?

**Control 16 — Account Monitoring and Control**
- How are accounts managed?
- Is there a review process to make sure user accounts are still applicable? What happens if someone leaves the University or change job duties?

**Control 17 — Data Loss Prevention**
- How is data protected within your system?
- Is P4 data encrypted during transit and rest?
- How are physical copies of data protected?

**Control 18 — Incident Response and Management**
- Does your team have an incident response plan?
- What happens if an incident occurs? How do you know when to contract security?

**Control 19 — Secure Network Engineering**
- Is your network segmented into multiple levels based on risk?

**Control 20 — Penetration Tests**
- Do you conduct penetration tests against your system? Has a penetration test ever been conducted?
- Is there a remediation process for when findings are identified?