<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>What Do I Need to Know to Submit an SRA Request?</td>
<td>2</td>
</tr>
<tr>
<td>SRA Process Overview</td>
<td>3</td>
</tr>
<tr>
<td>How to Request an Archer Account</td>
<td>4</td>
</tr>
<tr>
<td>How to Login to Archer</td>
<td>5</td>
</tr>
<tr>
<td>Introduction to the User Workspace</td>
<td>6</td>
</tr>
<tr>
<td>The Technical Contact Dashboard</td>
<td>7</td>
</tr>
<tr>
<td>Completing the Security Questionnaire</td>
<td>8</td>
</tr>
<tr>
<td>What if the Security Questionnaire is Rejected?</td>
<td>9</td>
</tr>
<tr>
<td>Corrective Action Plan (CAP) Overview</td>
<td>10</td>
</tr>
<tr>
<td>How to Locate a Finding</td>
<td>11</td>
</tr>
<tr>
<td>Adding a CAP</td>
<td>12</td>
</tr>
<tr>
<td>Documenting a CAP</td>
<td>13</td>
</tr>
<tr>
<td>Completing a CAP</td>
<td>14</td>
</tr>
<tr>
<td>Submitting the Finding</td>
<td>15</td>
</tr>
<tr>
<td>Rejected CAP</td>
<td>16</td>
</tr>
</tbody>
</table>
Welcome!

Welcome to the Privacy and Information Security Office’s implementation of Archer! Archer is Sutter Health’s Governance, Risk and Compliance (GRC) software used for creating and managing Security Risk Assessments (SRA) and associated risk findings.

Why the SRA?

The Security Management Process standard in the HIPAA Security Rule requires organizations to “implement policies and procedures to prevent, detect, contain, and correct security violations.” (45 C.F.R. § 164.308(a)(1).) Risk analysis is one of four required implementation specifications that provide instructions to implement the Security Management Process standard. Sutter Health’s SRA process is designed to ensure the confidentiality, integrity and availability of Protected Health Information (PHI) and other sensitive company data.

How do I know if I need an SRA?

If Sutter Health is implementing products (e.g., hardware), services (e.g., billing services, consulting services), or applications (e.g., software) that create, receive, maintain or transmit Sutter Health confidential data (such as Protected Health Information or other sensitive company data), an SRA is required.

How do I find more information about the SRA process?

Documentation (including this guide) can be found on the Sutter Health Privacy and Information Security Risk Assessment intranet page:

http://mysutter/Resources/PI/Pages/SRA.aspx

Note that this page is not accessible outside of the Sutter Health network. If you are an outside vendor and would like further information, contact your Sutter Health business requester or visit the Vendor SRA portal page located at:

https://www.sutterhealth.org/for-vendors/archer-grc
What Do I Need to Know to Submit an SRA Request?

Key Contacts

To request an SRA, the Sutter Health Business Requester will need to identify the following individuals and request an Archer account if one has not previously been provisioned:

Business Requester – The business requester should be familiar with the product, service, or application for which an SRA is requested. The business requester is required to provide responses to several (non-technical) questions relating to the product, service or application during the SRA process. Requires an Archer account.

Vendor and/or Sutter Health Technical Contact – The Vendor and/or Sutter Health technical contact should be familiar with the implementation details and associated security safeguards (controls) related to the product, service or application. As a rule of thumb, if a Vendor will be receiving or have access to sensitive data, you must specify the Vendor as the Main Technical Contact Type. For products, services or applications (and associated data) that are implemented or provided wholly within Sutter Health, you may select a Sutter Health Technical Contact as your Main Technical Contact Type. Requires an Archer account.

Executive Business Sponsor – The executive business sponsor is typically a Director or VP and has oversight responsibility for the product, service or application, including remediation of any identified security findings. SRA results will be delivered by the authoring PI Risk Team Analyst via email and phone call to this individual. Does not require an Archer account.
**SRA Process Overview**

The diagram above depicts a summarized view of our SRA process:

1. Visit [http://mysutter/Resources/PI/Pages/SRA.aspx](http://mysutter/Resources/PI/Pages/SRA.aspx) to request accounts for the Business Requester, Vendor Technical Lead and/or Sutter Health Technical Lead. If you are a Vendor Technical Contact, contact your Business Requester to request an account. If you already have the appropriate accounts, proceed to step 2.

2. The Business Requester logs into Archer and completes both SRA Record and Intake Form questionnaires.

3, 4. Once submitted to the PI Risk Team Analyst, the Business Requester will receive an email inviting them to complete a short Inherent Risk Assessment (IRA) questionnaire. Upon completing this short questionnaire, a second email will be sent to the Vendor/SH Technical Contact alerting them to log into Archer and complete their portion of the IRA. Once the IRA questions have been completed, the Vendor/SH Technical Contact can proceed to answer various information security control questions. When the questionnaire is completed, it is submitted to the PI Risk Team Analyst.

5. The PI Risk Team Analyst will review the questionnaire responses and identify control deficiencies, known as risk findings. The SRA Report Summary and associated findings are delivered to the Executive Business Sponsor via email and phone.

6. The Business Requester and Vendor/SH Technical Contact will receive an email requesting the creation of a Corrective Action Plan for each finding identified.

7. Once all CAPs have been identified and completed by the Business Requester and/or Vendor/SH Technical Contact, the PI Risk Analyst will validate and close the findings, ending the SRA process.
To Request an Archer account for any of the three account types:

1. Visit the SRA Portal at: [http://mysutter/Resources/PI/Pages/SRA.aspx](http://mysutter/Resources/PI/Pages/SRA.aspx)

2. Click on the appropriate Account request button (green buttons).

3. Complete the email form and click Send.

Your account will be created and an email notification will be sent to you with your initial password.

**NOTE:** If you are an outside vendor and need a Vendor Technical Contact account, please contact your Sutter Health business requester to request the account for you. Further information for vendors on the SRA process can be found on the Vendor SRA portal page, located at: [https://www.sutterhealth.org/for-vendors/archer-grc](https://www.sutterhealth.org/for-vendors/archer-grc)
To log into Archer, follow these steps:

1. Open Internet Explorer and enter:
   
   ![https://grc.archer.rsa.com/](https://grc.archer.rsa.com/)

2. Enter your user name, the instance ID (20171), and your password. If this is your first time logging into Archer, you will be prompted to change your password.

3. Click the Login button to log in.

**NOTE:** If you forget your password, you can click the “Reset Password” link that appears after you attempt to log in using an incorrect password.
The workspace display is the first screen you see upon logging into Archer.

1. Clicking the home button from anywhere in Archer will return you to your workspace.

2. Clicking on the SRA Management menu will take you to your dashboard (more on this on the next page.)

3. A list of tasks awaiting completion can be found in this area.

4. A running list of actions and notifications can be found in this area.

5. You can use Archer’s search functionality to search for SRAs (and associated findings and corrective action plans (more on this later).

6. When you’re finished in Archer, you can log out of your session by clicking here and selecting “Logout.”
The technical contact dashboard view contains two main windows. Each window contains several reports you can select that enable you to view various reports:

1. **Security Questionnaire Reports**: This dashboard window contains all of the security questionnaires that the technical contact has yet to complete:

   **IRQ-In Progress**: The Inherent Risk Questionnaire (IRQ) represents the initial ~20 questions in the questionnaire and is less technical in nature.

   **Controls Attestation-In Progress**: This second portion of the questionnaire contains control questions that are more technical in nature.

2. **Findings Reports**: This dashboard window contains various reports that list findings that are due to be remediated. You can view open findings pending remediation that are due in one week or all open findings for which you are the technical contact.
To complete the Technical Contact’s inherent risk assessment portion of the Security Questionnaire, locate the questionnaire using one of the methods described on the previous page of this guide. Once you’ve accessed the questionnaire record:

1. Click on the ✍ EDIT button to begin filling out the questionnaire. (Button not shown here).

2. Scroll down past the Business IRA Question Section until you see the Vendor IRA Question Section. Answer each question. Note that your responses may result in additional questions.

3. If you would like to add a comment or clarification as part of your response, you can click the coment icon to add a comment. Save the comment, then click the ✗ icon in the upper right corner to close the comment and return to the questionnaire.

4. Once you’ve answered all questions, click the button to complete the first portion of the security questionnaire. Directions for the second portion (control questions) are on the next page.
To complete the Technical Contact’s control question portion of the Security Questionnaire, locate the questionnaire using one of the methods described on the previous page of this guide. Once you’ve accessed the questionnaire record:

1. Click on the `EDIT` button to begin filling out the questionnaire. (Button not shown here).

2. Scroll down past the IRA Question Sections until you see the control questions grouped by tab. Answer each question in each tab. You may save your progress by clicking the `SAVE` button. If you’d like to return to Archer to finish your control questionnaire later, visit your dashboard and select the “Controls Attestation – In Progress” to locate the questionnaire.

3. You may also add any general comments and/or file attachments (such as data flow or design diagrams) in the “Vendor Comments and Attachments” section.

4. Once you’ve answered all questions, click the `Confirm Responses` button to confirm your responses. Finally, click the `Submit Control Questions` button (not shown) to complete the questionnaire.

Do not click the `Confirm Responses` button until you have answered all questions as you will no longer be able to save your progress and must answer all remaining questions.
1. If the control question responses are rejected (because a response is unclear, for example), you will receive an email notification as shown. You can click the link in the email to be taken directly to the questionnaire.

2. Alternatively, log into Archer and view the “Controls Attestation – In Progress” report in your dashboard to select the questionnaire.

3. Scroll down to the bottom of the questionnaire and read the “TPRM Analyst Review” comments. Follow the directions in the comments and resubmit the questionnaire by clicking the button.
Corrective Action Plans (CAP) Overview

Once the security questionnaire responses have been accepted by the Risk Analyst, he/she will author the SRA report and deliver a summary of the report along with any risk findings to the Executive Business Sponsor and Business Requester. The Risk Analyst will schedule a brief discussion with the Executive Business Sponsor and the Business Requester regarding possible corrective actions that can be implemented to remediate the findings. At this point, the Business Requester and Vendor Technical Contact/Sutter Health Technical Contact can collaborate on appropriate CAPs that can be entered into Archer as shown on the following pages. Once (one or more) CAPs have been entered and actions taken have been documented and uploaded to Archer, the Risk Analyst can verify and close each finding. Once all findings are closed, the SRA process is complete.

The decision of who will enter the CAP into Archer depends on who is remediating the finding. If the Business Requester is remediating the finding, they should create and manage the CAP. If the Vendor/SH Technical Contact is remediating the finding, they should create and manage the CAP.
To add a CAP for each finding, locate the finding using one of the following methods:

1. The Technical Contact (Vendor/SH) and Business Requester will receive an email for each finding with a link that will take you to the finding.

2. Alternatively, log into your account and visit your dashboard. In the Findings Report area, select the report “Findings – Open Items – Pending Remediation.”

3. Select the appropriate finding to be taken to that finding.

Dear Test, VendorTechnicalContact5, and Test, BusinessRequester5,

This Finding FND-386 has Corrective Action Plan that is due on 1/2/2018. Please use the link below to login, access the record and create/update the Corrective Action Plan.

https://grcb.archer.rea.com/default.aspx?requestUrl=%2fGenericContent%2fRecord.aspx%3fd%3d22898%2fmoduleid%3d167

Thank You,
Privacy & Information Security Risk Management Team
1. To add a CAP, click the Add New button. Further instructions on filling out the CAP are on the next page of this guide.

2. If you need an extension of time to remediate the finding, click the Edit (not shown here), then select a new remediation due date, provide a justification for the request, and click the Request Extension button to submit your request. You will receive an email granting or denying your request upon Risk Analyst review.
1. To document your CAP, click the button (not shown here).

2. Add a name for your CAP (e.g., Implement Two Factor Authentication).

3. Select a CAP type. Types available are:
   a) Control - A security control is a countermeasure implemented to avoid, detect, counteract, or minimize a risk.
   b) Policy - A policy is a written description of how the organization plans to protect their physical and information technology (IT) assets.

4. Describe your corrective action and select estimated start and completion dates.

5. Add any comments or attachments to support your CAP using the button.

6. To finish documenting your CAP, check the Yes box under the “Finalize Corrective Action Plan” area and click the button.
1. To complete your CAP, click the button (not shown here).

2. Select that you’ve completed the remediation and describe the remediation action(s) you’ve taken.

3. Add any additional comments and attachments that would assist us in validating your CAP (e.g., screenshots for software controls, policies/procedures, etc.).

4. Once you’ve sufficiently documented the corrective actions you’ve implemented, check the “Yes” box under the “Submit Remediation” section.

5. Click the button to submit your CAP remediation.

Be sure to submit the finding for review as described on the next page.
Once you’ve finished implementing all CAPs associated with your finding, you must submit the Finding for review. To do so, first return to the finding (you can locate the finding in your dashboard). Once you’ve returned to the finding:

1. Click the **EDIT** button to edit the finding (not shown here).

2. Ensure that the status of each CAP is “Submitted for Review”. If CAP status is “In Progress” this indicates the CAP has not been completed.

3. Click the **Submit** button to submit the finding.
After you submit your CAP and Finding for review, the Risk Analyst will review it to assess whether or not the CAP will sufficiently remediate the finding. If your CAP is rejected:

1. You will receive a rejection email similar to the one shown. You can follow the link to the finding or locate it using your dashboard.

2. Select the CAP that was rejected to open the CAP.

3. Once in the CAP, click the **EDIT** button and modify your CAP based on the Risk Analyst feedback located in the comments section of the CAP.

4. After updating your CAP, click the **SAVE** button and resubmit the finding as before.