Sutter Health
Privacy and Information Security

Archer Training Tutorial Series

Slide 1

No audio. Music only. Title page—Lesson 6: Creating Corrective Action Plans

This lesson contains audio a PDF of the script is available.

Sutter Health Privacy and Information Security logo

Slide 2

Welcome to the sixth instructional video for Archer - Sutter Health's Governance, Risk, and Compliance tool for security risk assessments.

This video will walk the Sutter Health business requester and technical contacts through how to add a Corrective Action Plan, or CAP, to a risk finding using the Archer environment.

Slide 3

After your security questionnaire is accepted by the Risk Analyst, he or she will examine your responses and identify any missing security controls.

These missing controls are known as risk findings and can be categorized as either low, moderate, or high risk.

Slide 4

Risk findings that are ranked as high risk require remediation within 30 days of identification. Risk findings that are ranked as moderate risk require remediation within 120 days of identification. Finally, risk findings that are ranked as low risk do not require remediation, but remediation is encouraged.

Slide 5

To remediate a finding, the business requester or technical contact must add one or more corrective action plans to the finding that outlines how the finding will be remediated.

For example, if a finding is identified for lack of multi-factor authentication, the technical contact may add a corrective action plan indicating that a multifactor authentication solution will be deployed.

Note that there is often more than one acceptable way to remediate a finding – you are encouraged to discuss your corrective action plans with the risk analyst assigned to your SRA.

Slide 6

If one or more risk findings are identified in your Security Risk Assessment, the business requester, and technical contacts will receive an email inviting them to log into Archer to create or update the CAP.

Slide 7

To do this, the business requester or technical contacts may follow the link in the email to navigate to the finding, or locate the finding in their dashboard.

Slide 8

To locate the finding in your dashboard, log into Archer using your Business Requester user account at: https://grc.archer.rsa.com.

Slide 9

After logging in, click on SRA Management button to visit your dashboard.

All unresolved findings will be listed in the "Findings Report" panel under the "Findings – Open Items Pending Remediation" report.

Click on the link to go to the finding.

Slide 10

To add one or more CAPs to the finding, click the "Edit" button.

Scroll down to the Corrective Action Plan section of the finding record and click the "Add New" link on the right side of the record.

Slide 11

To begin documenting your CAP, enter a CAP name.

Next, select a CAP type –you can choose a control-based CAP or a policy-based CAP. Examples for each of these CAP types are listed in the directions at the top of the record.

Next, describe your CAP in detail in the "Corrective Action Plan" textbox and select your estimated start and completion dates.

Slide 12

Finally, add any comments or attachments to your CAP, such as a policy document or technical control specification document.

Once you are satisfied with your CAP details, check the "Yes" checkbox under the Finalize Corrective Action Plan section of the record, then click the Save button.

Slide 13

Once you've implemented the corrective action, locate the finding in your dashboard as before, then scroll down in the finding record and click on your CAP.

Slide 14

Once in your CAP record, click the Edit button then select "Yes" in the Remediation section of the CAP.

A textbox will appear where you can provide remediation details surrounding what you implemented to remediate the finding. After you've provided those details, select your actual start and completion dates for your CAP.

Slide 15

Finally, add any final comments or attachments that will help your risk analyst assess your CAP. Some examples include configuration screenshots, policy documentation, and other documentation that show your functioning CAP.

Slide 16

Review your entries, then when satisfied, check the “Yes” checkbox under the Submit Remediation section of the CAP record and click the “Save” button.

Return to your finding by clicking the blue X at the top of the CAP record.

You can also click on the finding number in your CAP record or locate your finding in your dashboard.

Slide 17

Once you’ve returned to the finding, click the Edit button and scroll down to the Correction Action Plan section of the record. Note that your CAP status is now “Submitted for Review.”

Slide 18

It is important to note that you can have more than one CAP associated with each finding. If multiple CAPs are added to one finding, all CAPs must be submitted for review before the finding can be submitted for risk analyst review.

If all of your CAPs are in a submitted for review state, click the “Submit” button to submit the finding and associated CAPs for review.

Slide 19

The Risk Analyst assigned to your SRA will review the finding and the remediation steps you’ve described in your CAPs. If the finding is sufficiently remediated, it will be closed and no further action will be required.

Slide 20

If your Corrective Action Plan is rejected, you will receive an email notification.

Locate the finding in your dashboard and review the Risk Analyst comments at the bottom of the finding for instructions on updating the CAP.

Slide 21

To modify the CAP, scroll back up and click the CAP Name to revisit your CAP.

Click the Edit button on the CAP.

Once you’ve made the requested modifications, save the CAP as before and submit the finding for review.

Slide 22

If you cannot remediate the finding by the Remediation Due Date listed on the finding, you may request an extension. To do this, visit the finding record and click the “Edit” button.

Slide 23

At the bottom of the finding record, you will see an “Extension Request” section where you can request a new finding remediation due date.

To do this, select the requested new remediation due date, enter a justification regarding why an extension is necessary, then click the “Request Extension” button at the top of the finding record. Your request will be reviewed and you will receive an email reply granting or denying your extension request.

Slide 24

We hope you’ve found the Archer training videos helpful and invite you to visit our SRA portal or send us an email at SRAHelp@sutterhealth.org if you have further questions.