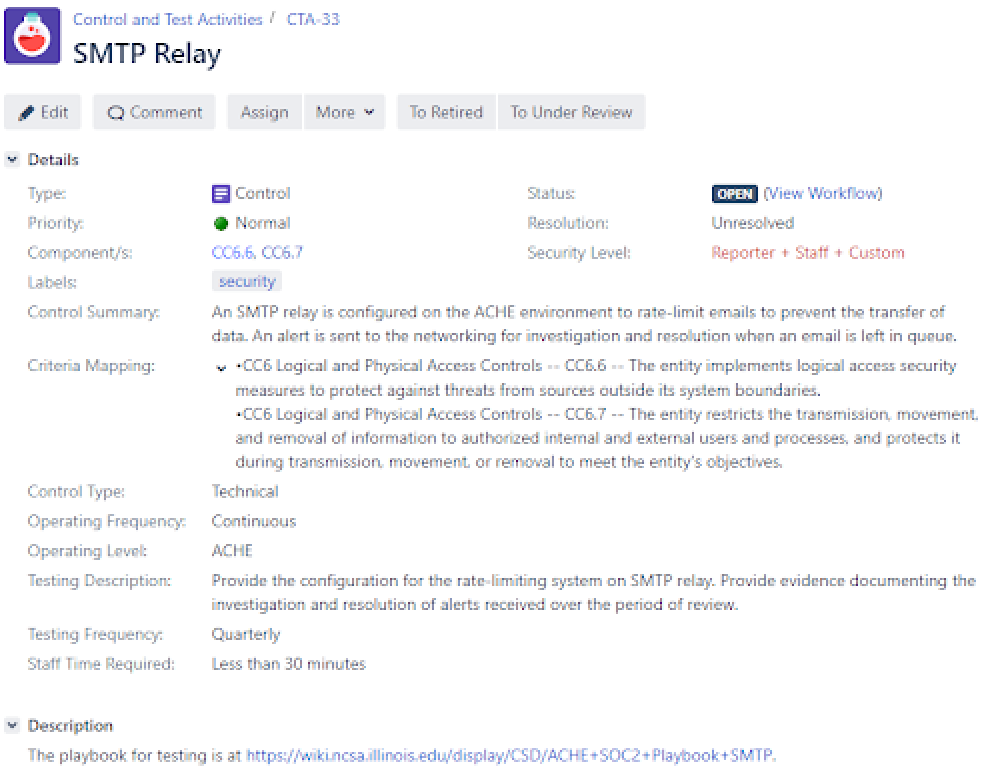
NCSA SOC 2: Using JIRA to track controls

In this installment of NCSA's blog series on SOC2 we will discuss how we've implemented our SOC2 Internal Testing Workflow. NCSA uses Atlassian's JIRA product for a variety of purposes ranging from IT incident tracking to project management. It's general design as a workflow framework suited it for use as our internal testing workflow for tracking and testing our controls. There are a variety of products available specifically for this purpose, however the cost and lack of knowledge and resources required to deploy these solutions required us to leverage our existing JIRA system.

The best way to illustrate how we use JIRA to track and test our controls is to provide an example of one of these controls. The first control is a simple control that requires outbound SMTP be rate limited on the SMTP relay:



SMTP Relay

Type: Control

Status: OPEN (View Workflow)

Priority: Normal

Resolution: Unresolved

Component/s: CC6.6, CC6.7

Security Level: Reporter + Staff + Custom

Labels: security

Control Summary: An SMTP relay is configured on the ACHE environment to rate-limit emails to prevent the transfer of data. An alert is sent to the networking for investigation and resolution when an email is left in queue.

Criteria Mapping:
- •CC6 Logical and Physical Access Controls -- CC6.6 -- The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
- •CC6 Logical and Physical Access Controls -- CC6.7 -- The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

Control Type: Technical

Operating Frequency: Continuous

Operating Level: ACHE

Testing Description: Provide the configuration for the rate-limiting system on SMTP relay. Provide evidence documenting the investigation and resolution of alerts received over the period of review.

Testing Frequency: Quarterly

Staff Time Required: Less than 30 minutes

The playbook for testing is at https://wiki.ncsa.illinois.edu/display/CSD/ACHE+SOC2+Playbook+SMTP.

This snapshot of the JIRA issue tracking the SMTP rate limit control has several fields that should be pointed out and explained. The "Control Summary" field describes briefly our control. The "Criteria Mapping" shows which Trust Services Criteria our control is mapped onto. In this particular example it is mapped onto CC6.6 and CC6.7 of the Trust Services Criteria:

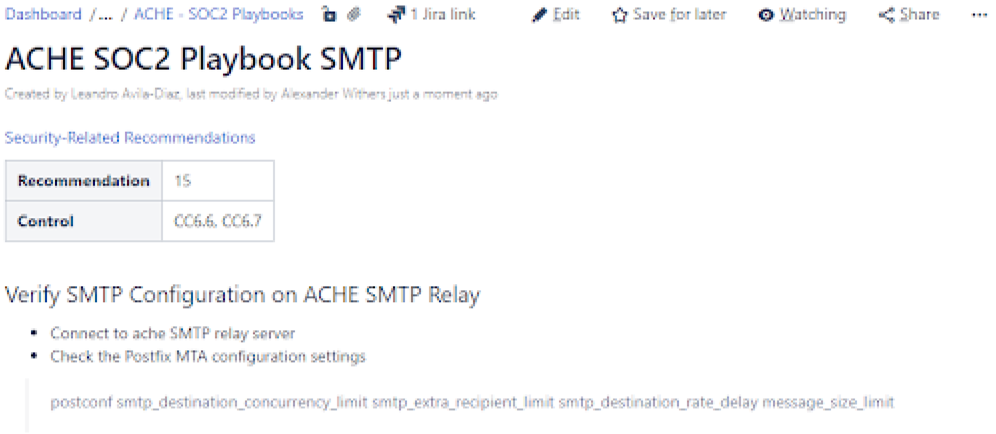
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

Recall that this mapping is part of NCSA's system description document provided during the SOC2 examination. During the examination this control, along with the others, is examined for the suitability of design and operating effectiveness of the controls in the system description. The "Components" field provides a reference that collects and displays all other NCSA controls mapped to Trust Services Criteria CC6.6 and CC6.7. This allows us to quickly identify and examine all other test controls for those specific criteria.

The other fields towards the bottom of the JIRA issue describe the control type, operating/testing frequency, and time required to complete the test. These fields are specific to our internal testing workflow and have nothing to do with SOC2, but do allow us to understand both the level of effort the testing takes and how often the control should be tested.

Lastly, the description of this JIRA issue links to a playbook. Because the control is a "Technical" Control Type, the playbook is written and maintained by the administrators who administer the SMTP relay of which this control is the focus. The playbook provides a step-by-step procedure for testing the rate limiting and alerting capabilities of the SMTP relay and how that test's outcome can be captured. The playbook is written in such a manner as to allow anyone authorized administrator to perform the test.

Below is a snippet of the playbook document.



ACHE SOC2 Playbook SMTP

Created by Leandro Avila-Diaz, last modified by Alexander Withers just a moment ago

Security-Related Recommendations

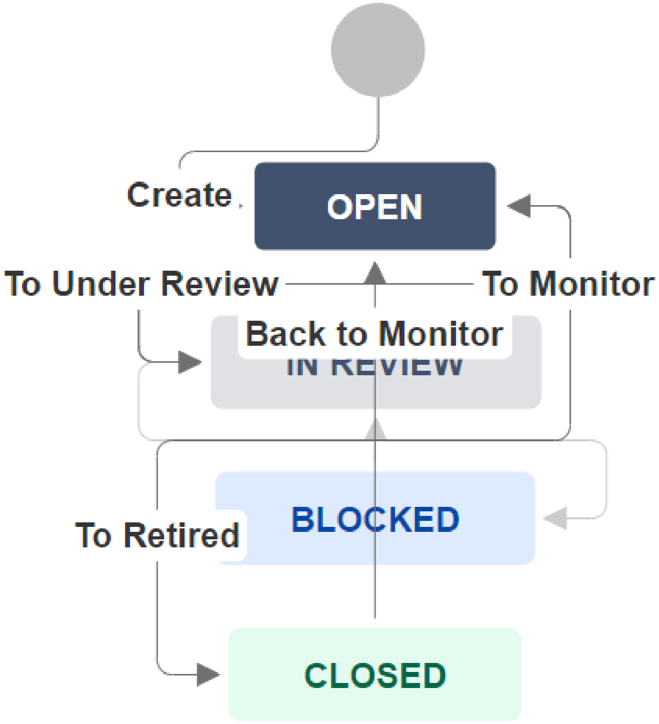
Recommendation	15
Control	CC6.6, CC6.7

Verify SMTP Configuration on ACHE SMTP Relay

- Connect to ache SMTP relay server
- Check the Postfix MTA configuration settings

```
postconf smtp_destination_concurrency_limit smtp_extra_recipient_limit smtp_destination_rate_delay message_size_limit
```

When this test is performed, the JIRA issue for this control implements the workflow described in the previous section:



This creates a JIRA sub-issue and places the control “In Review”. Assuming the test went well, evidence of a satisfactory test of the SMTP relay is attached to this sub-issue and it closed placing the control back into it’s open state.

In some circumstances, the evidence attached to the sub-issue can be used during a SOC2 examination. But more importantly, this internal test workflow ensures that, at any given time, we can demonstrate the operating effectiveness of our controls. Periodic testing allows us to ensure that we’re collecting the proper evidence, it ensures that the control is working and it allows us to identify inefficiencies that may consume more staff time than is necessary.

It should be noted that there are drawbacks to using JIRA for implementing this type of internal test workflow. JIRA is an issue tracking product at its core and is not designed for these types of looped workflows. JIRA also does not provide good options for managing or changing an issue’s state based on a time cadence. Options do exist by implementing this feature externally through an API but that assumes proper developer and JIRA know-how. Also, while JIRA does provide for extensive customization of an issue’s fields, there are many fields that are immutable. Take for example the “Resolution” field in SMTP relay control above. It is set to “Unresolved” which can be confusing for an issue that is currently in the “Monitor” state waiting to be tested. In order to overcome these drawbacks, a fair amount of manual intervention is needed to monitor and shepherd the issues through the internal test workflow. Additionally, documentation and training materials have to be created and maintained if staff are expected to be assigned these control tests and execute them properly.