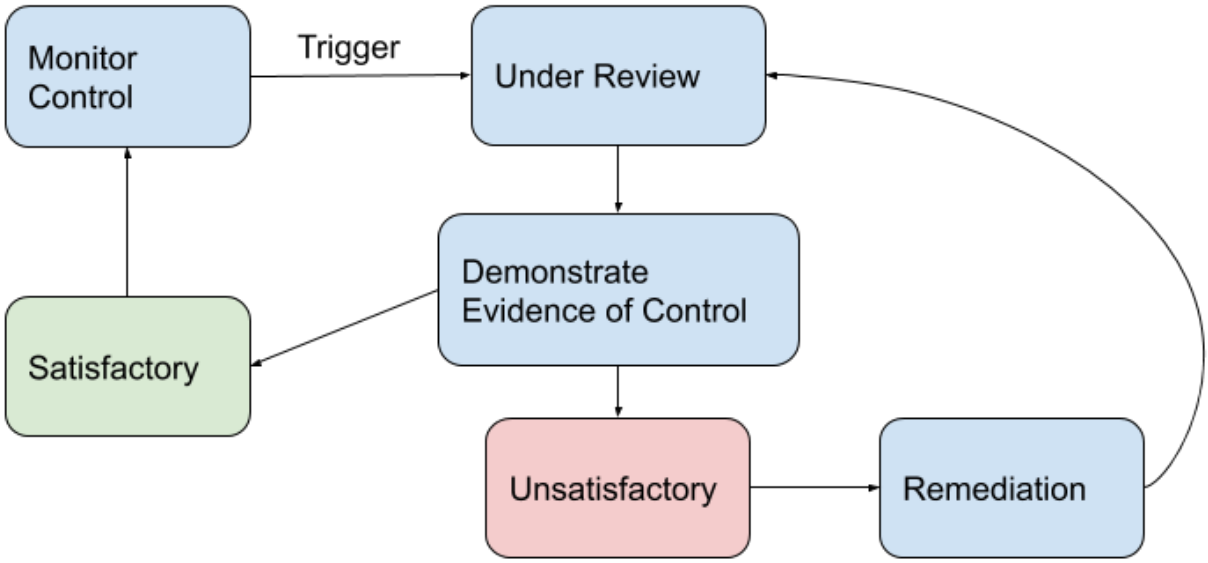
NCSA's SOC 2 Internal Testing Workflow

As described in our previous blog post, our approach to SOC 2 relies on establishing internal processes, building a platform to manage our controls and tests, the participation of our staff to implement the controls, and provide evidence of its operation. We have designed a compliance and internal auditing workflow to manage the lifecycle of controls and testing activities. This workflow is depicted in the figure below.



All controls begin in the state “monitor,” meaning they are designed to meet requirements, are documented, and expected to be operating as designed. Control Owners are responsible for ensuring that controls are being monitored. At certain times, a trigger moves a control into a review state, indicating that the control is ready for an internal test. A trigger might be an established periodic testing frequency, such as a quarterly review; a formal change to the system that affects the design of a control; a remediation of an incident that indicates a control is not operating as expected; or a third-party evaluation, such as the SOC 2 assessment.

A control under review initiates a test activity, which is a request for demonstration that the control is operating as expected. Test Owners execute the test and provide evidence of operation. When a test is complete, the Control Owner reviews the results of the test.

If the results sufficiently demonstrate the control is operating as expected and fulfills the scope of the control, the test is deemed “satisfactory.” The test activity is resolved and the control is moved back to the monitor state until the next test activity is triggered.

However, if the results are insufficient, then the test is marked “unsatisfactory.” A test could prove unsatisfactory for a variety of reasons; for example, if the instructions for demonstration are incomplete or the control is not implemented properly. In this case, the system is considered to be operating out of compliance with the control requirements and a remediation is needed. The Control Owner works with the Test Owner and other staff to plan and implement the remediation activity.

When the remediation is completed, another test activity is performed to demonstrate that the control is now operating as expected. The workflow repeats: the control is moved to “under review,” and a test is initiated, executed by the Test Owner, and reviewed by the Control Owner. Once the test results are satisfactory, the control is moved back to "monitor."

This simple workflow allows us to manage continuous internal testing and specify staff roles and responsibilities in the compliance management process. More importantly, when we undergo a SOC 2 evaluation we will be able to rely on this workflow and the evidence collected from all of the previous tests.