ACET IT Security Audit

DATASHEET

tracesecurity
Compliance, simplified.

877-275-3009 tracesecurity.com sales@tracesecurity

NCUA Compliance

Credit unions are required to complete an Automated Cybersecurity Examination Tool Review (ACET) every year, but now NCUA examiners are starting to request actual proof of your cybersecurity practices. The NCUA has defined five cybersecurity maturity levels that are acceptable for credit unions, which are generated from your ACET questionnaire: Baseline, Evolving, Intermediate, Advanced, or Innovative. Your target maturity level will depend on the size and complexity of your credit union's IT environment.

Most credit unions complete the questionnaire on their own, but examiners are starting to ask for actual proof that maturity levels are an accurate representation of your cybersecurity program. For true verification of your implemented security controls for NCUA Compliance, your credit union will need to start having an ACET IT Security Audit performed.

Your Maturity Level

Our ACET IT Security Audit will be based on the target maturity level of your organization. Using the maturity levels generated from your ACET Review, the ACET questions are converted into the control statements for the audit. Our analyst will provide you with a list of controls that require proof of implementation, and recommend certain artifacts for you to provide as verification.

We will determine the implementation status of each control, and provide you with a comprehensive report that includes any necessary notes or recommendations for your remediation action plan. All supporting documentation for controls is referenced in the report, proving control implementation and meeting NCUA compliance standards.

Frequently Asked Questions

What is the difference between a risk assessment and an IT audit?
A Risk Assessment looks at an organization's controls and determines their level of risk while an IT Audit verifies that stated controls are actually in place.

Are you going to look at my policies?
As part of the auditing process, some policies may require review, but for an in-depth review of all policies, we offer a policy review service.

How long will the whole process take? How much of my time will you require?
This depends very much on your responsiveness and availability. It can be done as quickly as 2 weeks if it is a remote audit.

What if we don't know where to find the documentation you are requesting or just don't have it?
We send out a sheet that lists what documentation we need. If you don't know where to find something, you can ask us. If a piece of information is missing, the control will be marked "unimplemented" or "unverified" depending on the situation.

How do you determine the controls to test during the audit?
The responses provided in the Cybersecurity Maturity portion of your ACET Review are converted into the control statements for the audit.

Can we get a preliminary report before the final audit is delivered?
Yes, but this needs to be requested up front during scoping.

An ACET IT Security Audit Gives You:

- **Verification of implemented controls**
- **Identification of control weaknesses**
- **Actionable recommendations for improvement**
- **A comprehensive report to satisfy NCUA examiners**

tracesecurity
Compliance, simplified.