Five Tips for NERC CIP Audits

Simplifying Proof of Compliance in ICS Environments

Meeting NERC CIP compliance is a challenge that keeps industrial controls systems (ICS) operators up at night. If organizations fail their audits, the NERC organization can levy large fines and require that extensive remediation work be done to bring systems back into compliance, leading to lost productivity and revenue.

NERC (North American Electric Reliability Corporation), a part of ERO, (Electric Reliability Organization) is the self-regulating organization in charge of making sure the North American energy grid is secure. CIP refers to critical infrastructure protection. Energy is one of the 16 sectors, along with chemical, manufacturing and communications and others, the United States government has designated as critical infrastructure.

> The vision for the Electric Reliability Organization Enterprise, which is comprised of NERC and the seven Regional Entities, is a highly reliable and secure North American bulk power system. Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.
>
> — NERC

The way the NERC organization enforces NERC CIP compliance is through auditing. There are a few reasons audits can be a major stumbling block for organizations that aren't equipped with the right tools. Auditors focus on the nine standards set forth in the NERC CIP guidelines:

1. Sabotage reporting
2. Personnel and training
3. Critical cyber asset identification
4. Electronic security perimeters
5. Security management controls
6. System security management
7. Physical security of cyber assets
8. Recovery plans for critical cyber assets
9. Incident reporting and response management

In this white paper, we'll explore five key takeaways ICS operators can implement to make compliance—and the audits that enforce it—into a streamlined process that doesn't inhibit your organization's productivity.

1. Put Serious Effort into Your Reliability Standard Audit Worksheets (RSAWs)

An RSAW is how you prove to your auditor that you're compliant with a requirement by describing in narrative form how you've accomplished the control in question. Part of this is saying how you've gathered the evidence of compliance. Without automation tools, ICS operators are often left to generate evidence manually—a time-consuming and error-prone process. The system admin and SCADA engineer manually gather evidence with different levels of maturity.

For example, evidence may be generated by taking screenshots of systems and putting those images into a text document. Another common practice is writing homegrown scripts to pull evidence information in order to put it in a spreadsheet which is manually maintained and becomes outdated fast.

Because the whole audit period is in scope, evidence could be requested for the whole three-year span. The best way to ensure ongoing compliance is to ensure that RSAWs are completed thoroughly and reviewed for accuracy by independent parties.

The benefits of prioritizing RSAWs are two-fold. First off, you can identify shortcomings in your evidence or program and any potential non-compliance early, which can result in reduced fines or even Find Fix Track and Report (FFT). Second, the evidence and narratives generated for your RSAWS can be used extensively in Pre-Audit Data Requests, thereby significantly reducing the amount of work to respond to them.

Keeping up with RSAWs can be a burden, but if subject matter experts (SMEs) keep them updated after every action, it's a whole lot easier than trying to complete one from scratch at the end of the year.

2. Similarly, Don't Skimp on Pre-Audit Data Requests

The audit cycle for CIP is every three years. RSAWs are submitted annually. Ninety days prior to your audit, you will be contacted with pre-audit requests. This generally includes a massive data request for a random sampling of assets, whereby auditors request certain pieces of evidence to be generated for very specific periods of time. These are often unaffectionately referred to as the "data bomb." If you're attempting to retrieve this information manually, it can be a significant drain on your time and resources—even if you keep meticulous records.

3. Conduct Mock Interviews to Test Your SMEs

Audit interviews play a significant role in the outcome of your audit. They are typically used as an opportunity for auditors to clarify any evidence that was submitted, test SME knowledge, and even get a look at the actual environment in question. During an audit interview, you may be asked to demonstrate how you accomplish particular requirements. It's

preferable to be able to show an enterprise-class solution than something that was put together behind the scenes with a homegrown script or a spreadsheet.

4. Make the Most of Responses to Auditor Questions

During interviews, being prepared to answer open-ended questions is imperative. Being careful to not stray from the topic can be difficult, but it is equally important to answer the questions succinctly. It's possible to showcase the strongest parts of your security strategy in your answers so that your auditor knows you've done your homework.

For example, you may be asked to describe the methods and tools that you used to gather CIP-010-2 R1.1 baseline components. While explaining how your solution achieves this, take the liberty to also describe any ways the solutions you use go above and beyond to automate your processes. By steering your answer, you can show off some of the great work you're doing.

5. Present Consistent Evidence with Tripwire

Tripwire solutions don't just simplify robust ICS security—they make NERC CIP compliance much easier to prove to auditors. You can leverage Tripwire's ability to present compliance evidence in the form of clear charts rather than scouring through manual spreadsheets to find the compliance data your auditor requests. Consistency across your IT and OT environments helps paint a picture of a well-organized and proactive security posture for your entire organization.
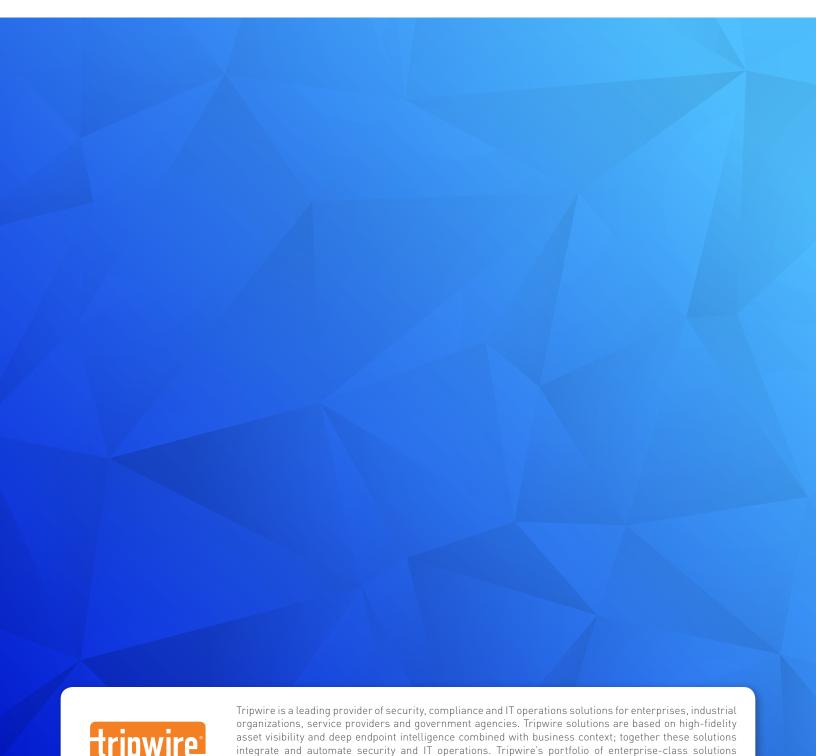
The Tripwire ICS Security Suite encompasses Tripwire® Enterprise with Tripwire Data Collector, and Tripwire® Log Center®. This suite is specifically designed to bring the industry-leading system hardening and compliance automation Tripwire is known for into ICS environments to reduce manual effort. For example, Tripwire Enterprise automates the generation of evidence you need to refer to in your RSAWs. Its integration with ICS solutions like SigmaFlow takes that coverage a step further by automating the generation of your RSAW narratives with supporting evidence as well.

Summary

Passing NERC CIP audits doesn't have to be an arduous manual process. Tripwire solutions like Tripwire Enterprise automate much of the evidence for you, so that proving compliance is simple when it comes time for your next audit. To learn more about the Tripwire ICS Security Suite, download the *Tripwire ICS Security Suite* solution brief from www. tripwire.com today.

Ready for a Demo?

Let us take you through a demo of Tripwire's security and vulnerability management products and services customized to your specific IT security and compliance needs. Visit **tripwire.com/contact/ request-demo/**

Tripwire is a leading provider of security, compliance and IT operations solutions for enterprises, industrial organizations, service providers and government agencies. Tripwire solutions are based on high-fidelity asset visibility and deep endpoint intelligence combined with business context; together these solutions integrate and automate security and IT operations. Tripwire's portfolio of enterprise-class solutions includes configuration and policy management, file integrity monitoring, vulnerability management, log management, and reporting and analytics. **Learn more at** tripwire.com

The State of Security: Security News, Trends and Insights at tripwire.com/blog
Follow us on Twitter @TripwireInc » Watch us at youtube.com/TripwireInc