How Prepared Are You for the NERC CIPv5 Audit?

ITEGRITI Guest Blog on Tripwire's "State of Security" Blog
August 20, 2017

Maybe you're ready to jump in with both feet, maybe you have no idea where to start, or maybe you're somewhere in the middle. No matter where you land, there are some best practices to help you along the way. While I can't promise to rid you of all past sins and violations, I do have pointers based on actual experience that has produced great results.

As an example, my company helped a large utility company prepare for a CIPv5 MRRE audit, with only one issue identified outside of what we already reported due to the auditors pulling evidence from a different sample set. Also, when we performed one-on-one training and solutioning sessions during a validation of three EMS environments, rework rates (areas where evidence was determined to be insufficient) were reduced from an initial 60 percent, to 30 percent, and finally down to 10 percent.

I'm happy to share lessons learned from our experiences with you. But before we proceed, you must begin with the end in mind. Let's assume that your goal is to exit the audit with zero findings, a handful of recommendations, and the respect and admiration of your management team and peers. I believe these best practices can help you meet that goal.

As you may know, the auditors are trained professionals, and they know how to assess evidence. By extension, our goal beyond being secure and compliant is to concisely present evidence that substantiates CIP compliance. Think in terms of evidence that will pass the "man on the street" test to anticipate and respond clearly to audit questions.

We termed this "quality evidence," which consists of three main attributes:

Source data – For each requirement, identify sufficient and appropriate key evidence to provide reasonable assurance that is extracted from the source and is sufficient and appropriate to support the auditors' findings and conclusions. Evidence should be attributable to the system and show when it was generated. It's helpful to provide screenshots showing both date/time and device name.

Clarity – Good evidence provides "information," not just "data." Some evidence contains so much data that the point is lost. By contrast, quality evidence is focused and contains only the elements requested by auditors. Embed information in the evidence to help provide additional explanation. For example, a concisely worded statement explaining that a signature represents approval and review of a document can reduce follow-up questions and annotation efforts.

Completeness of population – Ensure the source data is accurate and complete. Doing so can help make sure that all items in the given population are captured, addressed and identified to provide support for the auditors' findings and conclusions. Provide assurance of the evidence's accuracy and completeness by comparing different sets of data for differences and taking corrective action, when necessary, to resolve deviations.

With this in mind, here are my top five audit readiness recommendations:

1. PREPARE IN ADVANCE

I have yet to meet anyone who believed they had too much audit prep time. That being said, develop an audit preparation schedule and afford your team ample wiggle room so that, if you do find issues, they will have time to investigate, understand the extent of the found condition, perform Root Cause Analysis where errors appear systemic, develop a solution, and remediate.

2. USE THE TOOLS AVAILABLE

There are many resources available that can help in CIP audit preparation. Do not create or modify NERC's forms and templates. (Yes, we have seen actual cases where some have invested much effort in developing their own CIP reporting forms, only to have these rejected by the auditor.)

How Prepared Are You for the NERC CIPv5 Audit?

ITEGRITI Guest Blog on Tripwire's "State of Security" Blog
August 20, 2017

Instead, develop a familiarity with existing tools and embrace the "CIP v5 evidence worksheet" to build your planning and responses. We designed an assessment tool that leverages all of the available NERC information so that teams can "see" all guidance and organizational knowledge while gathering and reviewing evidence.

3. KNOW YOUR DEVICES

A fundamental element of any cybersecurity program is a comprehensive inventory all IT assets across the enterprise. No organization can plan adequate defenses from a coordinated cyberattack if it does not know the systems, programs, patch levels and types of information within its area of responsibility. You cannot secure that which you don't know exists.

With this in place, the logical next step is determining how those assets should be configured and ensuring that they stay that way. Establishing targets for secure settings for both hardware and software allows the organization to increase consistent application of cybersecurity policy.

It also allows unexpected or errant changes to be more quickly and accurately identified, as comparisons can be made against known baselines. At the same time, effective change management practices reduce the substantial risks associated with applying inappropriate changes to a production environment.

4. KNOW YOUR POSITIONS

They say the devil is in the details—they are right. It comes as no surprise that not everything CIP is binary. There are many "gotchas" in CIP V5, so where grey areas exist or where your program relies on multiple compensating controls to achieve the purpose and intent of a requirement, make sure that your team pays attention to small details and has documentation of rationale, approach and effectiveness. This is essential to audit survival.

5. PREPARE YOUR SMES

Your team is key, so help them organize, plan and establish metrics. Be methodical. Engage your subject matter experts early and often. Perform gap assessments, instruct them during one-on-one trainings, and provide mock audit preparatory sessions.

Help them understand that electric reliability and security is everyone's responsibility. Also, impress upon them the expectation that they will be respectful and helpful during the audit. They do not need to speak through an attorney, but they should address specific questions deliberately, honestly and concisely.

I hope you find these best practices helpful. Visit our website and send me an email to share your thoughts or to help me improve this list. I look forward to hearing from you.

About the Author: Michael Sanchez, CISA, is the President of ITEGRITI Corporation (www.itegriti.com) and has served NERC and CIP clients since 2006. He has more than 29 years of experience, and he has held senior IT and compliance leadership positions in the energy, oil & gas, healthcare, and transportation industries. In prior positions, Michael served as head of Commercial Cybersecurity and Compliance for a global management consulting firm, managed IT and OT for a $12-billion energy corporation, and assisted in the IT rebuild and redesign for a power company that generated 12,000 megawatts of electricity. He has experience across a wide variety of regulatory areas including NERC, NERC CIP, FERC, SOX, HIPAA, and FERPA. Michael serves as the local chapter SIG coordinator and has been a board member for the last 12 years for InfraGard Houston, a private non-profit organization serving as a public-private partnership between U.S. businesses and the FBI facilitating the sharing of information related to domestic physical and cyber threats.