By Lew Folkerth, Principal Reliability Consultant

How to Excel at a CIP Audit

Your path to an excellent CIP audit begins with an excellent operational security program, which means your security program must exceed the Requirements of the CIP Standards. Keep in mind that the CIP Standards are intended as a baseline that all Responsible Entities must meet. If you do not exceed that baseline, you are almost certainly leaving your systems exposed to unnecessary risk.

I have provided, and will continue to provide, pointers on how to improve your security program in other articles in this series, but now let's concentrate on how you demonstrate your excellent security program to an audit team.

In order to document and maintain an excellent security program, you must also have an excellent compliance program. The true function of a compliance program is to monitor and document your security program. In addition, an excellent compliance program will help your security program "adapt to shifting environments, evolving demands, changing risks, and new priorities" (from GAO-14-704G Federal Internal Control Standards, Page 1). This is the definition of an internal controls program.

In this recurring column, I explore various questions and concerns related to the NERC Critical Infrastructure Protection (CIP) Standards. I share my views and opinions with you, which are not binding. Rather, this information is intended to provoke discussion within your entity. It may also help you and your entity as you strive to improve your compliance posture and work toward continuous improvement in the reliability, security, resiliency and sustainability of your CIP compliance programs. There are times that I also may discuss areas of the Standards that other Entities may be struggling with and share my ideas to overcome their known issues. As with lighthouses, I can't steer your ship for you, but perhaps I can help shed light on the sometimes stormy waters of CIP compliance.

What I'm saying here is that an excellent compliance program is really an excellent internal controls program with some additional functions to generate compliance evidence. See Figure 1 for how this should work.

Figure 1 (on the next page) shows my concept of a modern compliance system and how it may be audited. The Compliance Audit will consist of a review of the compliance evidence. To help obtain reasonable assurance of compliance, the Internal Controls Assessment may review the internal controls associated with the Requirement being reviewed.

If the internal controls are strong and comprehensive, this will add strength to the compliance evidence. The Security Risk Review will assess the effectiveness of your security controls in protecting your systems. This assessment may reference published guidance, security guidelines, accepted security practice, and other sources to ensure a valid review.

With the foundation of an excellent security program monitored by an excellent internal controls program and documented by an excellent compliance program, you should be well on your way to achieving excellence at audit. To make the most of these foundations I want to ensure that you understand the basics of an audit and are ready to supply the information an audit team will need to obtain reasonable assurance of your compliance.

Audit Concepts

To excel at a CIP audit, you need to understand what information the audit team is looking for and provide that information in a clear, concise manner. Compliance audits are performed according to the Generally Accepted Government Auditing Standards (GAGAS, available here).

When you read GAGAS you can ignore Chapters 6 and 7, as these do not

White River Light Station, White Hall, Michigan – Photo: Lew Folkerth

Continued on page 8

Continued from page 7

pertain to a Performance Audit. In reading Chapter 8, Fieldwork Standards for Performance Audits, you should understand these concepts.

Sufficient, appropriate evidence:

Evidence is the key to a successful audit. Your goal in submitting evidence is to provide the audit team with reasonable assurance that you are complying with the Requirement in question. In most cases the CIP Evidence Request Tool (ERT) will be your guide to gathering, formatting and submitting evidence. Auditors must obtain sufficient, appropriate evidence to support their conclusions.

Appropriate evidence is relevant, valid and reliable. Sufficient evidence provides enough appropriate evidence to address the audit objectives and to support the findings of the audit team. Evidence from more than one source may be used to support the audit team's review. This is known as "stacking evidence."

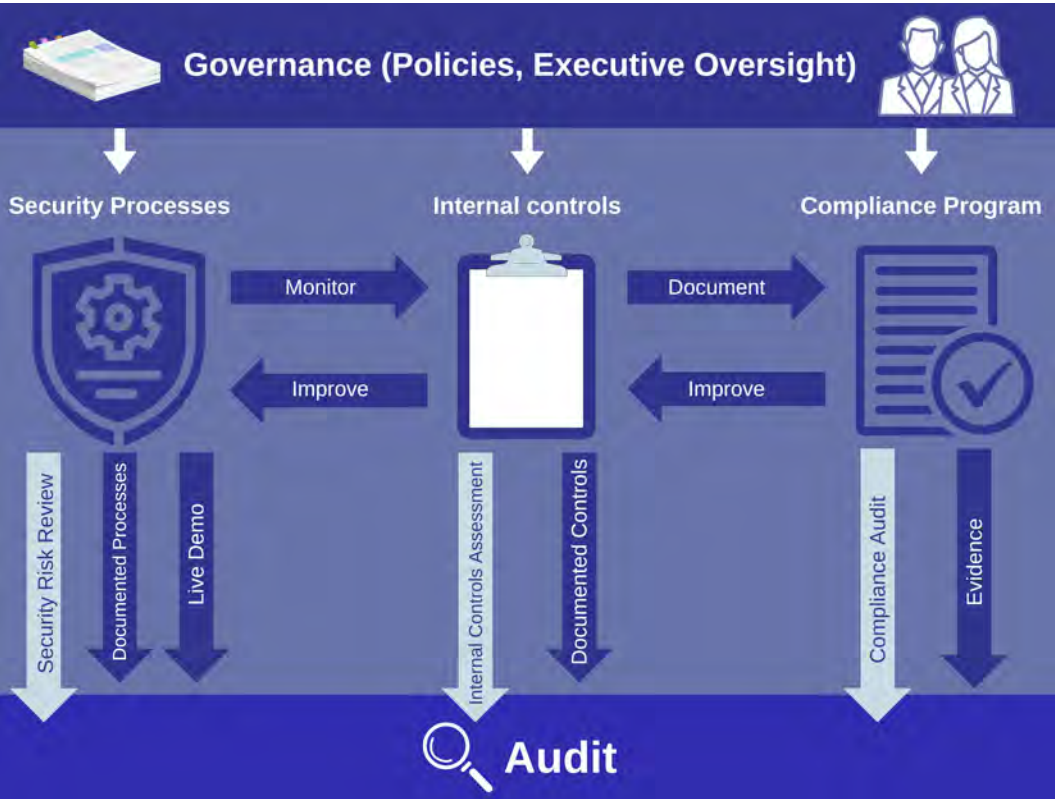

Figure 1

Effective evidence is also clear, complete and concise. It should clearly demonstrate compliance with the Requirement. It should be complete, so the audit team doesn't need to request additional evidence, and it should be concise to eliminate unnecessary information. Another way of looking at effective evidence is that it should tell the story of how you maintain compliance with the Requirement.

Your narrative of how you perform this task can be included in the Reliability Standard Auditor Worksheet (RSAW) in the Compliance Narrative section for the applicable Requirement or Part.

Professional judgment:

Auditors are expected to use professional judgment when reviewing your performance. Professional judgment includes exercising reasonable care (acting in accordance with professional standards and ethical principles) and professional skepticism (having a questioning mind, awareness of relevant conditions, and performing a critical assessment of evidence).

This means you need to give the auditors confidence in your ability to protect your CIP assets and maintain reliability, resilience and security. You establish your credibility with the audit team by being open and forthcoming. You and your SMEs should be proud of what you do, and that pride should show in your interactions with the audit team.

The audit team

Your audit team will consist of an Audit Team Lead (ATL), one or more sub-teams, and possibly observers. The ATL is your point of contact for all things related to the audit. Each sub-team will have at least a lead and a scribe. The sub-team lead guides the review of the sub-team's assigned Requirements. The scribe documents the review and coordinates additional evidence requests. Observers may include staff or management from FERC, NERC or Regions. The observers may vary in their level of participation, but in no case does an observer influence the team's findings.

Contrary to popular belief, an ERO Enterprise audit team's primary purpose is to find you compliant with the Standards and will work with you if necessary to help you demonstrate compliance. It is only when this joint effort fails that an audit finding will result. As SERC's Robert Vaughn says in

Continued on page 9

Continued from page 8

"Your audit team is a team of seasoned professionals with diverse backgrounds in cybersecurity, including patch management, remote access, physical security, etc. They are available to answer questions and help walk you through the process. Please work directly with them regarding expectations for when they arrive on site regarding the agenda, anticipated questions, and discussion points to ensure that the right SMEs are present to lead discussions and demonstrate your programs. Please pick venues that match the time, duration and needs for the discussions including appropriate A/V settings and a table/chair setup that is conducive to the upcoming conversations."

Brian Thiry
RF Director and former O&P Auditor

"Good documentation is auditor kryptonite."

Robert Vaughn
CIP Auditor, SERC

the sidebar quote, good documentation is essential to a good outcome.

Remember to keep the audit at a conversational and cooperative level to achieve the best results. (See "Defense Against the Dark Auditor," Lighthouse #22, Sep/Oct 2017, available here.)

The audit process

The audit will begin with an opening briefing by the ATL, followed by your opening presentation. It will be helpful, but not essential, to have your presentation delivered by a senior executive. This helps demonstrate executive commitment to the operational cyber security program. The major portion of the audit will be subject matter expert (SME) interviews and site visits. The ATL will close out the on-site portion of the audit with a preliminary exit briefing.

During the audit it is essential to get the right SMEs in front of the auditors. The SMEs you choose should be the people who actually do the work of implementing your security processes. Your SMEs should be briefed on what to expect and should understand that their interaction with the auditors will be interviews, not testimony. The interviews should be conducted as a conversation and should not be confrontational. Your SMEs should be open and honest with the audit team to establish their credibility. During their interviews, they should:

- Describe how security processes are followed;
- Show how the security processes protect your systems and meet compliance requirements;
- Show how documented internal controls ensure consistency and sustainability in these processes; and
- Explain how the evidence demonstrates that the processes are performed without exception. In complex cases, you may want an SME to perform a live demo of a system to show how it functions.

Another key to a successful compliance audit is constant audit readiness. According to the Compliance Monitoring and Enforcement Program (CMEP, NERC Rules of Procedure Attachment 4C) Section 4.1.2, an unscheduled audit can be initiated with a prior notification of 10 business days. If your processes are not in constant readiness to produce compliance evidence, you will have a very rough time if an unscheduled audit of your entity is initiated.

Audit findings

During the exit briefing, you will be given the preliminary results of your audit. Here are the possible audit findings, coupled with my understanding of their current meaning:

- Potential Noncompliance (PNC) – The audit team has not been able to obtain reasonable assurance that you are in compliance with the Requirement cited. A PNC, if sustained by RF Management and Enforcement reviews, will enter you into the Enforcement and Mitigation processes.
- Area of Concern (AoC) – The audit team is concerned that your compliance with the cited Requirement may not be sustainable or effective in adequately protecting your systems.
- Recommendation – An audit team suggestion to improve your program.
- Positive Observation – The audit team's feedback to you on things you are doing particularly well.

Continued on page 10

Continued from page 9

Audit tools

Be familiar with the tools the auditors will use. Unlike other types of audits, you are provided with a full list of information the auditors will ask for, making an audit more like an open-book test. Here are the tools you will need:

- Align – Organizes the information about your entity and facilitates the compliance engagement.
- Secure Evidence Locker (SEL) – Stores your compliance evidence during the audit.
- Reliability Standard Auditor Worksheet (RSAW) – Auditor tool used to organize the review of your evidence. The compliance narrative section is used for you to tell your story of how you approach compliance with a Requirement or Part. The narrative should be informative but concise.
- CIP Evidence Request Tool (ERT) – Tells what evidence is needed and establishes populations of evidence for sampling. The ERT is available here, and the ERT User Guide is here.

Conclusion

"Our overall goal as auditors is to have reasonable assurance that you have a sound security program. We do this through the evidence review process and asking questions around your internal controls program. We ask that you concisely tell your compliance story on engagements and that you demonstrate the pride you have in your program as we want to see you going above the standards."

Jim Kubrak, RF Manager, O&P Compliance Monitoring, and
Zack Brinkman, RF Manager, CIP Compliance Monitoring

Requests for assistance

If you are an entity registered within the RF Region and believe you need assistance in sorting your way through this or any compliance-related issue, remember RF has the Assist Visit program. Submit an Assist Visit Request via the RF website here.

Be sure to request any assistance you want well before your audit begins. Your audit becomes active when you receive the audit notification letter and remains active until your exit briefing.

During the time your audit is active, RF is restricted in how we can assist you. In particular, the Assist Visit program will be unavailable to you during your audit period.

Previous issues of The Lighthouse, expanded articles and supporting documents are available in the RF CIP Knowledge Center.

Coda

On this occasion of the 50th issue of The Lighthouse, I wish to thank all the people who have made this series possible. As with any ERO document, it is not the product of just one person. While I am solely responsible for the content of each article, I wish to thank those who have contributed to the success of this column over the years. I thank my publication staff and my review teams: technical, legal and editorial.

And my thanks to RF as a whole for providing me this opportunity.

Lew Folkerth and Entity Engagement Director Brian Thiry

Feedback

Please provide any feedback you may have on these articles. Suggestions for topics are always welcome and appreciated.

Lew Folkerth, Principal Reliability Consultant, can be reached here.