AssurX

WHITEPAPER

Are Your NERC Internal Controls Out of Control?

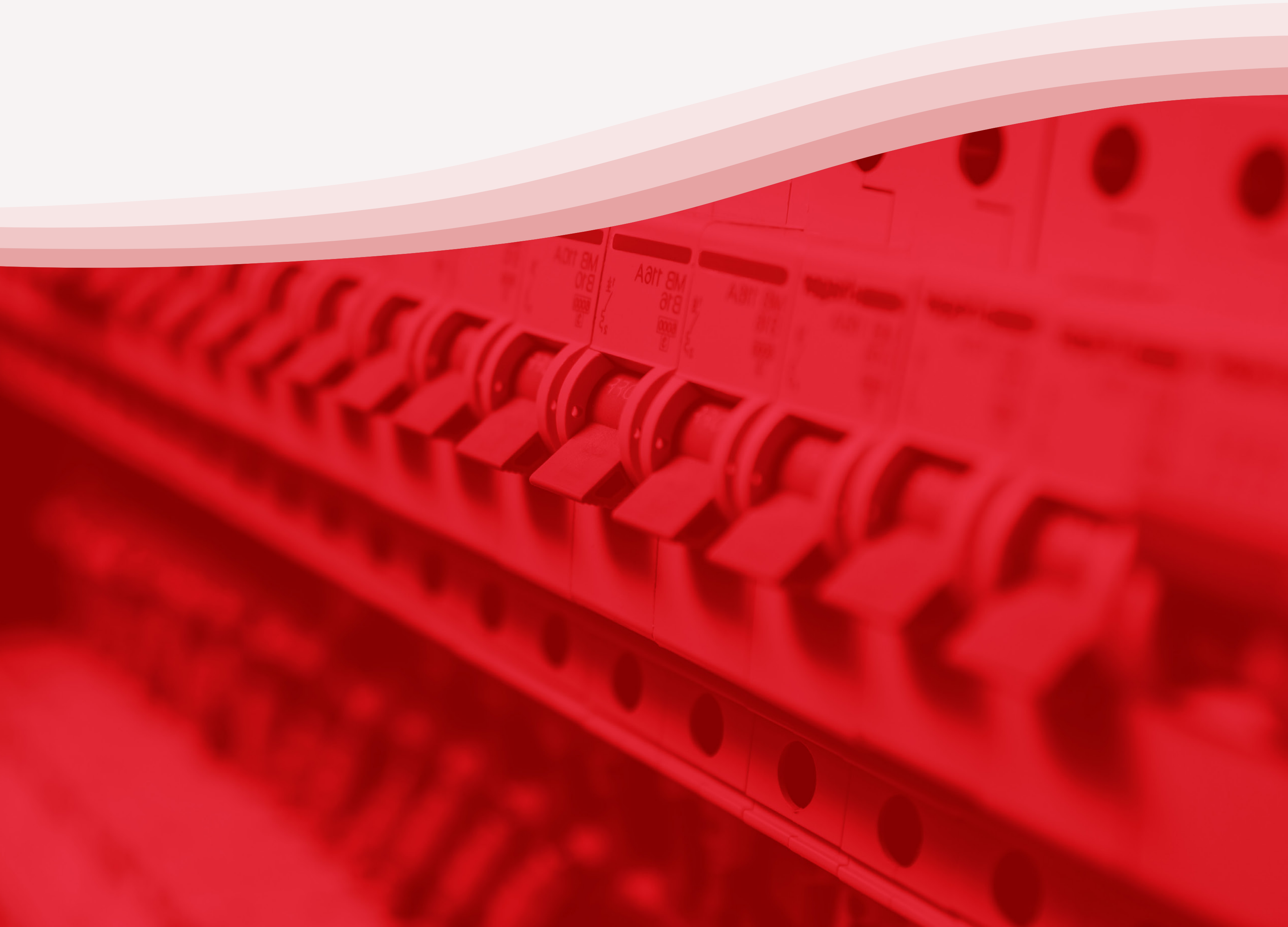


Table of Contents

Are Your NERC Internal Controls Out of Control?

Imagine a health inspector visiting two restaurants. The first has a spotless, well-organized kitchen, with clearly labeled sanitation procedures and cleaning records posted on the walls.

The second is messy and disorganized, with the manager having to look in several places to find documentation that food safety procedures are being followed.

Which one do you think will be scrutinized more heavily? Obviously, it's the second restaurant.

The same concept applies to NERC audits, where regional entities are increasingly focusing on Internal Controls as a measuring stick for overall compliance performance.

Let's look at what this means for utilities, including what to expect during a NERC audit and how to build rock-solid Internal Controls with automated compliance management software.

Understanding NERC Internal Controls

The term internal controls originates from the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework created in 1992 for the financial industry. The COSO framework provides a standardized approach to developing internal controls to ensure processes are followed and documented, focusing on areas such as risk management, control activities and monitoring.

Decades later, NERC adapted the concept for its own definition of Internal Controls (capitalized) focused specifically on electric utility processes to ensure NERC compliance. This Internal Controls program is separate from, for example, controls in a general sense or internal controls established within the organization.

NERC's Compliance Monitoring and Enforcement Program (CMEP) has evolved over the years towards a risk-based model that looks at entity-specific factors in developing each utility's Compliance Oversight Plan (COP).

Under this approach, the strength of an entity's Internal Controls program directly impacts the frequency and scope of NERC monitoring activities.

The simple observation underlying NERC's compliance monitoring strategy: Those utilities with strong Internal Controls are far less likely to commit compliance violations.

Reducing Your Audit Scope with Strong Internal Controls

NERC views Internal Controls as a barometer for the strength of an entity's compliance performance as a whole. This is the idea behind NERC's Internal Controls Evaluation (ICE) process, which allows utilities to potentially reduce the scope of their annual audit by undergoing a review of their Internal Controls.

The Challenge of Perfection

The fundamental challenge of managing NERC Internal Controls comes from the sheer volume and complexity of requirements that utilities must comply with. Utilities must execute and document thousands of tasks to achieve compliance, from software patching to password changes, employee training, vegetation management, and more.

For example, to comply with CIP-004, CIP-007, and CIP-010 alone, a medium size utility may need to track and document over 50,000 individual compliance items. The number of items would depend on the size of the entity, but its typically a vast amount of documents. Each NERC requirement also has very strict timelines for completing and documenting tasks, whether monthly, quarterly, annually, or other specified frequency.

What raises the stakes is that NERC expects perfect compliance every single time. Compliance violations can result in steep penalties of up to $1 million per day, or worse—a threat to grid reliability .

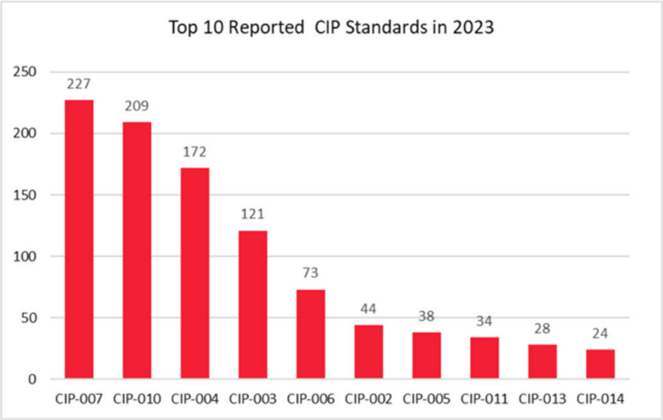


Figure 6: CIP Noncompliance Reported in 2023

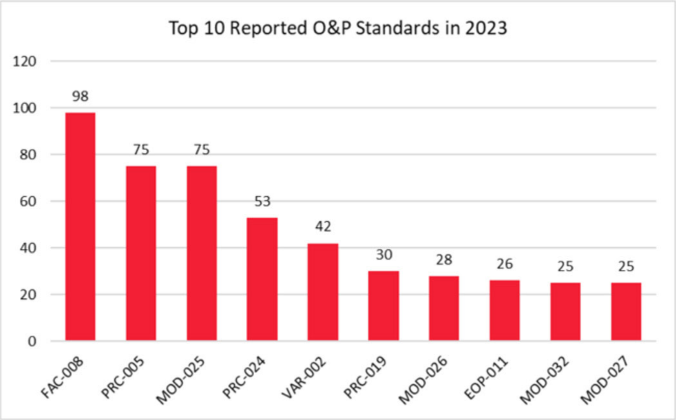


Figure 7: O&P Noncompliance Reported in 2023

Making matters even more complicated is the fact that utilities are continually evolving. New technologies, employee turnover, new compliance requirements, and an ever-expanding threat landscape all make maintaining flawless Internal Controls harder.

Then there are the inevitable communication challenges between departments and the potential for human error, which are typically the weakest links in any compliance system.

Trying to keep up with it all through traditional methods like calendar reminders and spreadsheets is a recipe for failure, with thousands of opportunities for mistakes.

What to Expect During a NERC Audit

In recent years, there's been a shift in the auditor's focus away from checking compliance items on a detailed level. Today, it's a utility's Internal Controls program that is under the microscope, focusing on higher-level processes and safeguards.

Common compliance gaps identified during NERC audits include:

Inadequate Documentation

You may have a process, but if it's not documented, you can't find it, and/or people aren't following it, it's not really a process. If you can't produce documentation as proof of compliance, the control may as well not exist at all as far as the auditor is concerned.

Inconsistent Application of Controls

Even well-designed controls may be poorly implemented or consistently applied across the organization.

Change Management

When things change in the organization, do you have mechanisms in place to keep up with it in terms of maintaining compliance? Auditors will want to see how you're managing to change to address and prevent new risks.

If you can demonstrate that you have a failsafe system for ensuring compliance, auditors will likely focus their attention on other areas. Poorly implemented controls, on the other hand, are likely to result in increased scrutiny, particularly for high-risk areas like CIP standards.

Viewed through this lens, your Internal Controls program must be built specifically to prevent anything from falling through the cracks. For many, the missing element in being able to successfully juggle all the moving parts throughout the organization is automation.

Automation + Integration = Compliance

The key to achieving perfection in your Internal Controls is building an automated system that replaces manual steps with automated workflows and system oversight. Integration with other systems is also essential to strengthening those controls and eliminating potential compliance gaps.

Let's look at an example.

CIP-007 requires certain systems to require employees to change their passwords at least once every 15 calendar months, with documented evidence to demonstrate compliance. The big question is, what controls do you use to enforce this?

Companies that track compliance tasks manually might send out an email to remind employees to change their passwords. Software that automatically expires the password after 15 months would be a stronger control, since it eliminates the chance that someone will forget to update their password.

Layer in tens of thousands of these types of compliance tasks, and it's clear that automation is a necessary ingredient for building a failsafe process.

Integration is the second piece in the puzzle, eliminating the inherent communication gaps that often lead to compliance violations.

For instance, asset configuration management tools like Tripwire can monitor system changes and alert the team if unauthorized software is detected. From there, an investigation can be launched and documented within the compliance management system to prevent a security breach and ensure compliance.

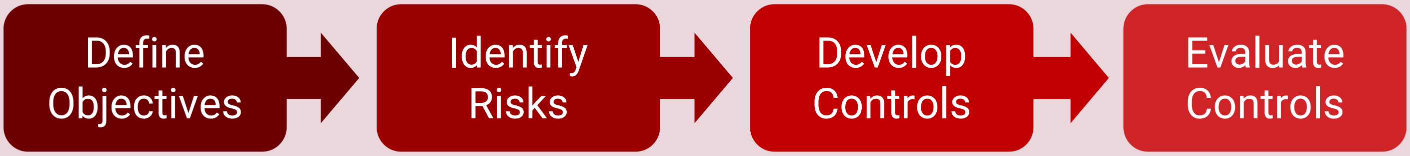
Another example would be integrating the software with your learning management system (LMS), where:

- The compliance system automatically communicates with the LMS to initiate training before certificates expire.
- The LMS delivers the training and documents completion.
- The LMS automatically populates the compliance management system with the required evidence.

Internal Controls: The Risk Management Perspective

Internal Controls are an important part of enterprise risk management (ERM). Going back to the original COSO framework, an ERM approach expands risk assessment into three separate components: objective setting, event identification, and risk assessment.

Working from this enterprise risk model, the process of developing Internal Controls is comprised of four basic steps:



Define Objectives

Identify Risks

Develop Controls

Evaluate Controls

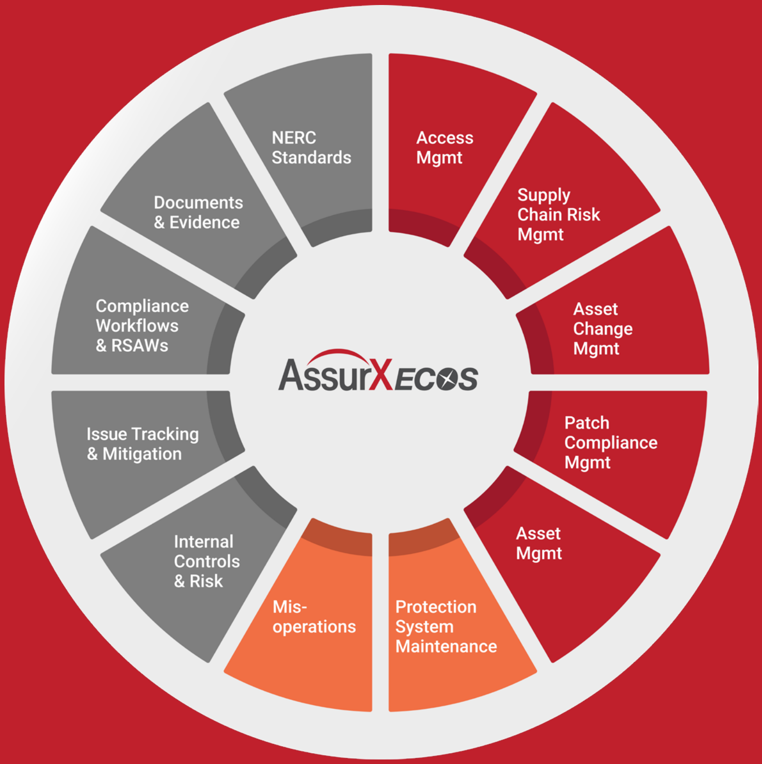
The first step in the risk management process is to identify the assets you need to protect.

This step involves a threat assessment, a vulnerability assessment, and calculating the probability that the vulnerability will be exploited. This involves evaluating policies, procedures, standards, employee training, physical security, quality control, and technical security. You also need to calculate the impact, whether through qualitative or quantitative analysis, that each threat would have on each asset.

Here is where you identify, select, and implement appropriate controls based on factors such as productivity impacts, cost-effectiveness, and value of the asset.

Internal Controls must be regularly reevaluated to ensure they're working and adjusted to account for the current risk environment. Cyberthreats, for example, are constantly evolving, such that controls that were effective a year ago may no longer be enough.

Software Feature	Key Capabilities
Requirements and Evidence Documentation	● Link evidence and documentation to each NERC requirement ● Pre-loaded with NERC requirements, including regional standards ● Configure additional entity-specific requirements as needed
Accountability	● Assign tasks to individuals at defined frequencies ● Document evidence
Risk Management	● Define risks ● Perform risk assessments ● Identify controls ● Evaluate control effectiveness ● Prioritize actions based on risk
Accountability	● Reminders when tasks are approaching due dates ● Escalation when tasks are overdue
Visibility	● Clear, comprehensive view of compliance activities organization-wide ● Custom dashboards showing risks, action items, business analytics, AI and more



From an external auditor's perspective, evaluating an entity with a proven compliance management solution in place builds confidence in the reliability of your operations. The result is more goodwill and less scrutiny throughout the audit process. In many cases, having this type of software is likely to reduce your NERC audit scope, since you can show that you have all the elements needed to create failsafe Internal Controls.

Selecting the Right Vendor Partner

Implementing a NERC compliance system is a crucial decision, and one that requires careful thought in terms of selecting the right software vendor. Two vital questions to ask here are:

1. How much expertise does the vendor have in electric utility compliance? Look for a partner with expertise in NERC requirements, both on the O&P side as well as with CIP requirements. NERC experts will know the right questions to ask, build the right requirements, and provide them with the Internal Controls needed for both compliance and security.

2. Does the vendor have high customer support ratings? Vendor support can make or break your software implementation. When questions arise, you don't want to be left waiting, or worse—sending your requests into a black hole. Here you want to evaluate what previous customers have to say about the level of vendor support provided.

Looking Beyond Basic Compliance

Maintaining a flawless Internal Controls program is no small feat, but it's one that must be achieved to avoid penalties and maintain grid reliability for customers.

Those utilities that are most successful from a compliance perspective don't implement these systems just to achieve basic compliance. Rather, their overarching aim is to be safe, resilient and reliable—compliance is just a byproduct of that goal.

One basic challenge underlying these issues is resource constraints as NERC requirements become more numerous and stringent each year. Automated software helps utilities handle the growing workload, manage change effectively with existing staff resources, and improve system reliability overall.