2018 THEMES AND LESSONS LEARNED

MITIGATING RISKS BEHIND THE CRITICAL INFRASTRUCTURE PROTECTION RELIABILITY STANDARDS

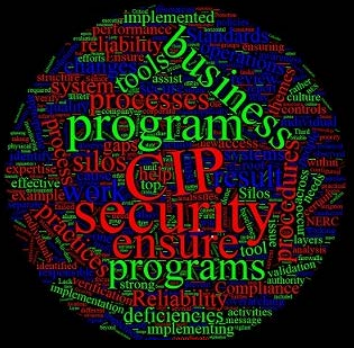
SECOND EDITION

PREAMBLE AND LIMITATION OF PURPOSE

Through their compliance monitoring and enforcement activities, and in coordination with North American Electric Reliability Corporation ("NERC"), ReliabilityFirst Corporation ("RF"), Western Electricity Coordination Counsel, and SERC Reliability Corporation (collectively, the "Regions") have identified risk themes that have made it difficult for some entities to mitigate against risks associated with the Critical Infrastructure Protection ("CIP") Reliability Standards.[1] The purpose of this report is to communicate these themes, and possible resolutions to them, so that we can work together to continuously assure the reliability of the Bulk Electric System ("BES"). While there are many discrete valuable lessons learned published by NERC and Regional Entities to promote strong CIP performance, this report is intended to identify and share broader themes.

The suggestions for possible resolutions in this report are not, and should in no way be construed as, directives to industry to undertake any actions. Rather, most of these possible resolutions are merely approaches that have been successful for those certain entities. However, these possible resolutions may not be the best approach for every entity because the impact of the resolutions is largely driven by variables such as an entity's size, corporate structure, workforce, technology, culture, and other factors. Thus, before expending any resources to implement any of these possible resolutions, the Regions suggest that the entity perform a cost/benefit analysis that considers both the practical realities of their operations and themes identified in this report.

[1] The power industry is subject to mandatory Reliability Standards for Critical Infrastructure Protection. The entities discussed in this Report have worked with the Regions to resolve and mitigate any noncompliance with the CIP Reliability Standards. More importantly, many of these entities have voluntarily agreed to take actions that go above and beyond what is required to be compliant with the CIP Reliability Standards to further enhance the security of their operations.



EXECUTIVE SUMMARY

To combat the ever-changing physical and cyber-threats landscape, entities continue to improve their tools, expertise, and defense strategies. Yet, despite these efforts to stay ahead of security threats, entities are sometimes held back by deficiencies or limitations in their corporate structure, culture, or resources.

In 2014, RF, in coordination with NERC and several stakeholders, began analyzing data around potential themes in these deficiencies and released its findings in early 2015 in the first edition of this report.

Since then, the Regions have coordinated to continue to analyze data relating to entities' ability to mitigate risks behind the CIP Standards. In recent years, the Regions have seen improvement and maturation with most entities' CIP programs. However, some entities continue to experience challenges with implementing CIP compliance programs. Thus, in the spirit of continuous improvement, the Regions are issuing this Second Edition of this CIP themes report in order to help drive entities to continue to assess and strengthen their CIP programs and thus mitigate security risks.

The main themes the Regions have identified are:

1. development of organizational silos;
2. disassociation between compliance and security;
3. lack of awareness of an entity's needs or deficiencies; and
4. inadequate tools or ineffective use of tools.

Since the start of mandatory compliance for CIP Standards, the Regions have resolved approximately 4600 violations. Figure 1 represents only the violations that comprise what the Regions consider the more significant CIP compliance program deficiencies reported or identified in their Regions between 2010 and 2017.

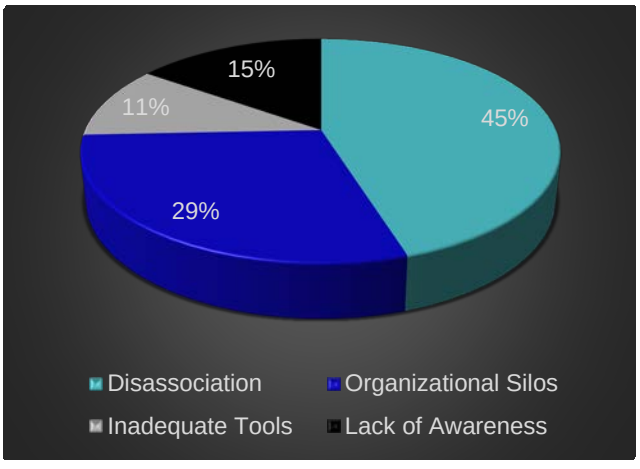


Figure 1: CIP themes associated with significant compliance program deficiencies.

Generally, significant CIP compliance deficiencies are the result of multiple causes that overlap and are interrelated. So, while the themes discussed in this report are distinguished for ease of explanation, they are often comingled when analyzing an individual entity's CIP compliance program deficiencies.

The Regions determined the significant CIP compliance deficiencies through consideration of the number and nature of violations per entity combined with the severity of the risks posed by the violations individually or in the aggregate. As Figure 1 indicates, most of the violations are rooted in entities disassociating compliance from security and/or developing organizational silos. Below is a detailed explanation of each of the four themes and recommendations on how to prevent their occurrence.

THEME 1: DEVELOPMENT OF ORGANIZATIONAL SILOS

ORGANIZATIONAL SILOS: Lack of internal coordination and uniformity between business units, departments, or layers from the top down.

Observations

Multiple entities have experienced CIP compliance deficiencies as a result of a lack of internal coordination and uniformity that can be characterized as organizational silos. These silos occur when entities fail to coordinate and/or consolidate compliance efforts across all business units or departments and between layers from the top down. Differing compliance programs within a single entity can lead to internal confusion, contradictions between processes, lack of ownership of projects or tasks, and other issues. Importantly, silos may reduce security if the relevant groups are not closely communicating and coordinating with one another. A failure to communicate may cause gaps in areas such as access control, incident response, recovery planning, and change management.

Silos can occur **vertically** (such as between business units) or **horizontally** (between layers from the top down), or both.

Vertical silos occur when an entity does not coordinate across businesses, business units, departments, or groups. This lack of uniformity and coordination can be especially problematic because many of the CIP Reliability Standards cross multiple business units or departments. For example, Human Resources ("HR") is usually one of the first departments, or the only department, to know when an individual's employment commences or terminates. The combination of this fact with inconsistent processes (or lack of processes) across HR and other business units routinely leads to an inability to successfully implement CIP-004 because the lack of coordination can result in unintentionally and improperly authorizing, or failing to revoke the authorization of, an individual's access to critical cyber assets.

SILOS

Key Concepts

Vertical Silos

(Between Business Units or Departments)

Horizontal Silos

(Between Layers from the Top Down)

Bureaucratic Paralysis

occurs as a result of too many unnecessary layers of review.

Some entities see vertical silos develop because of corporate restructuring, either due to mergers, acquisitions, or other actions. In the case of mergers or acquisitions, silos arise when entities fail to integrate and instead continue to operate as two separate companies, even if on paper they have a single compliance program.

Regarding **horizontal** silos, these can arise between layers from the top down. These silos have occurred at some larger entities where they had overarching policies on compliance or an overarching compliance program and then implemented individual compliance programs for the business units. The issue arises when these individual programs are not coordinated with, and sometimes contradict, the overarching compliance policies or program. As a result, the subject matter experts within individual business units had difficulty trying to reconcile which process to follow during implementation. This compliance program splintering tends to occur when upper management institutes processes in the overarching program that are not practical when applied to the operational needs of the individual business units.

Additionally, middle management can either be the key to an entity's success or hinder an entity's ability to implement an effective compliance program. The Regions have observed issues with middle management occur in two different ways. First, the right message regarding a policy on security and compliance may be sent from the top down to middle management, but that message can stop at middle management if they do not agree with the message. On the other hand, top management may not have an accurate picture of the state of security and compliance if middle management is not raising concerns up the chain. In this scenario, middle management may be reporting that its security and compliance program is running more smoothly or successfully than it is in reality. Top management cannot set the right tone if they have an inaccurate understanding of the state of the program.

One byproduct of horizontal silos can be bureaucratic paralysis. This has occurred where there are multiple layers of review, which can result in tasks getting lost in the review process and taking too long to complete. At one entity, proposed fixes to simple problems had to go through many layers of review before the entity was permitted to resolve them or submit the self-report to the Region. As a result, the process changes that needed to occur were delayed. Over time, employees stopped identifying or reporting issues, at least in part because they could not see the immediate impact of identifying or reporting issues. Consequently, this negatively impacted preventive and corrective controls.

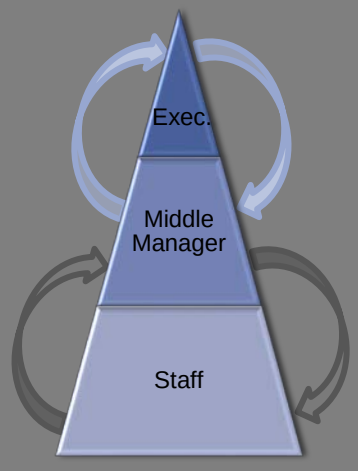
Suggestions to Address Organizational Silos

To avoid inconsistencies, entities should focus on coordinating compliance programs throughout the entity, including between departments, business units, and different levels of management. One way to coordinate compliance programs is to identify process owners that have the authority, ability, and responsibility to reach across business units to coordinate with other business units. Also, using cross-functional teams where possible can help fill knowledge gaps and ensure coordination and consistency between silos.

Breaking Down Vertical Silos

- ➔ **Communication**
- ➔ **Cross-Functional Teams**
- ➔ **Coordination**
- ➔ **Process Owners**
- ➔ **Collaboration**
- ➔ **Structured Plan**

Common Communication Channels



Regarding **vertical** silos created from corporate restructuring, we have seen entities navigate this successfully with careful planning and thoughtful execution. One entity's strategy for integrating an acquired company into the existing company included four steps – acclimate, plan, structure, and people.

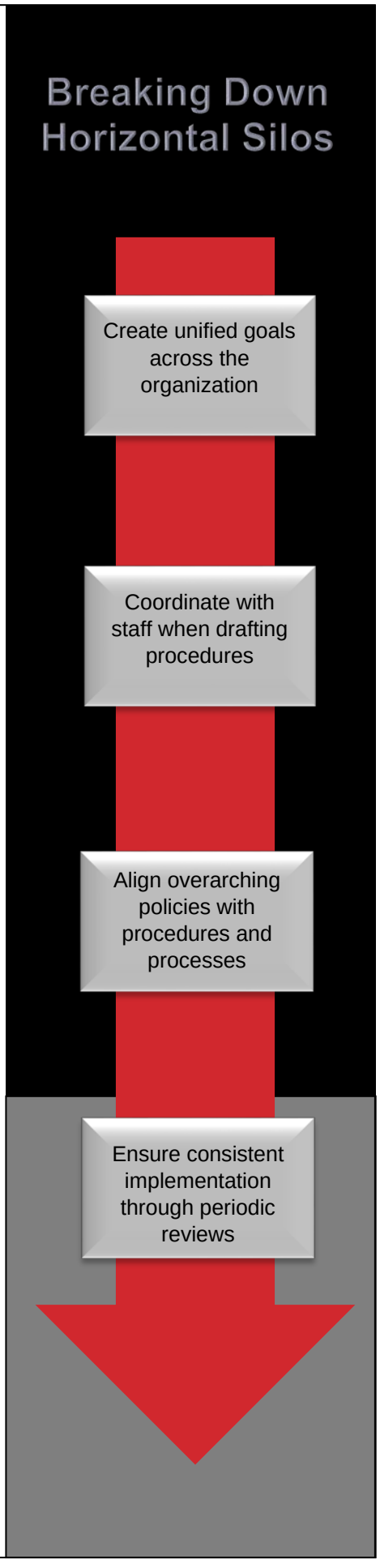
First, the entity spent time bringing key compliance personnel and subject matter experts from both companies together to learn about the existing structure, culture, and general state of each entity's compliance program. The initial sessions also identified risks and challenges to the integration. This acclimation step helped both entities collect the information and form the relationships necessary to develop a strong integration plan. The second step was to develop that detailed plan, which assigned responsibilities and milestones to merge compliance processes and procedures. A lot of this work was done before any restructuring actually took place so that on day one of the restructuring, the entities could begin making changes necessary for successful integration. Third, the entity developed a unified compliance structure to help it get buy-in starting at the top. This structure included instituting a combined NERC Steering Committee with senior management from both companies. Fourth, the entity approached the integration as a partnership or collaboration rather than an ownership takeover. This approach included simple things such as using the term "we" instead of "them" and taking the time to explain and understand why each entity did things certain ways rather than demanding they be done a certain way. The entity also had an open mind regarding using best practices from the acquired company's compliance program and integrating those into its existing compliance program; the entity did in fact adopt some of the acquired company's practices.

To sustain the integration process, entities need to be aware of institutional burnout where people might be taking on too much work. Integration can be a long process, so being aware of how hard people are working and where entities can assist (with resources or work management) can help ensure the acquired entity remains a participant in the process instead of retreating from the process.

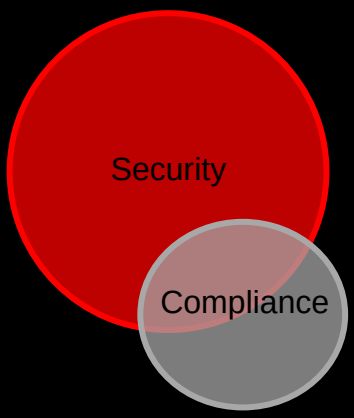
Vertical silos may also be a source of inconsistent adoption of new or revised Reliability Standards. For example, CIP-013-1, Supply Chain Risk Management, will bring new departments into contact with the CIP Standards. Entity management must decide who builds the compliance program and compliance documents for these departments. When addressing new or revised Standards, entity management should ensure that a consistent approach is followed so that there are no gaps in security or compliance.

Regarding **horizontal** silos, when developing procedures, management should work with those who implement the procedures to ensure that the procedures are practical. If a compliance program is creating hurdles and is disconnected from practical reality (as opposed to being efficient and considerate of the obligations of the stakeholders), it is likely that compliance program splintering may occur, which leads to compliance inconsistencies and, ultimately, jeopardizes the secure operation of the system.

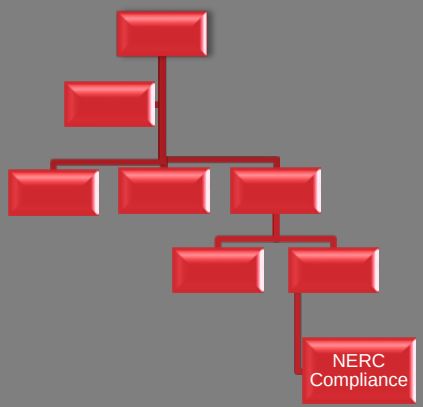
To assist in ensuring consistency across the entity (vertically and horizontally), an entity's CIP Senior Manager should have a deep understanding of the entire CIP compliance program and the organization of the business and should be able to identify any silos that exist. The CIP Senior Manager should then assess



DISASSOCIATION
Key Concept



An **indicator of disassociation** may be the compliance department's location in the organization chart (tucked away within a single business unit or as a function of the Information Technology department).



the silos to ensure that they are appropriate for the entity's situation. For example, the Energy Management System department, IT, and the physical security group might have separate compliance programs due to being three different business units within the entity. Having three separate programs for these areas may or may not be appropriate, but if they are appropriate, the entity must ensure that the compliance processes and procedures are coordinated and well documented. Entities need to avoid situations where individuals or individual business units only consider their own responsibilities rather than the larger picture and how the business units must work together towards security and compliance.

Additionally, it is also important to remember that senior management is where the messages starts, not ends. Senior management must ensure its direction and message is carried down through middle management to the staff. To do this, senior management can get involved in compliance matters by: (a) holding periodic meetings with the individuals responsible for executing the compliance programs to stay apprised on current issues and monitor general compliance activities; (b) approving the compliance program and significant changes to procedures; (c) reviewing and approving all or a sample of self-reports, mitigation plans, self-certifications, and other compliance documentation; and (d) participating in or reviewing internal assessments or audit reports.

THEME 2: DISASSOCIATION BETWEEN COMPLIANCE AND SECURITY

DISASSOCIATION: Treating security and compliance as completely separate functions that serve separate purposes, resulting in a diminished value or emphasis on compliance.

Observations

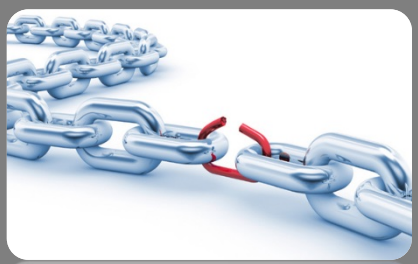
Issues often result from an entity disassociating compliance from security (and by extension, reliability), which results in diminished value or emphasis on compliance. Some entities may at times view CIP compliance as merely a "paper" exercise rather than viewing it as a baseline level of what an entity needs to do to maintain security, or, even better, as a natural byproduct of implementing an entity's procedures to ensure the secure operation of its system.

The Regions have observed situations where entities' NERC Compliance departments, which were responsible for compliance for the entire enterprise, were tucked away within a single business unit. On paper, the compliance departments had the responsibility to ensure compliance throughout the organization, but in practice, the groups were not empowered or given resources to drive a consistent enterprise-wide compliance program. As a result, NERC compliance was not a priority among other business units, but rather, each business unit made its own operations a priority. Consequently, certain aspects of compliance went unaddressed due to gaps in processes.

Addressing Disassociation

Verify that no security gaps exist.

1. ***Ensure procedures, policies, and programs*** *align with security features.*
2. ***Implement physical protections*** *for staff, facilities, and equipment.*
3. ***Verify electronic perimeters*** *(such as firewalls, DMZ's, and IDS systems) are configured and operating as intended.*
4. ***Identify and verify ports and services*** *and that network devices are communicating.*
5. ***Ensure antivirus, monitoring, and change controls*** *are operational.*
6. ***Verify only necessary applications*** *are installed, patched, and up-to-date.*
7. ***Ensure storage locations and access provisioning*** *are implemented as intended.*



The Regions have also identified problems where compliance and operations are concentrated in the same management or within one department, which becomes an issue if the manager has competing concerns (day-to-day operations versus compliance). For example, some entities charge IT with CIP compliance, but IT's primary responsibility is managing the entity's information systems, and thus compliance may take a back seat to IT's operational duties.

One area that tends to be deficient when compliance and security are not working together is patching, as it sometimes gets overlooked for the perimeter security solutions such as firewalls and intrusion detection. No single security solution can secure a network from all types of attacks—some solutions prevent unauthorized access (e.g., firewalls and intrusion prevention) and other solutions fix internal network weaknesses (e.g., vulnerability assessments). The Reliability Standards help ensure that all security solutions are working together and complement each other to reduce the possibility of successful attacks. Figure 2 illustrates the multiple layers of security controls that entities should have in place to protect critical information pursuant to the CIP Reliability Standards.

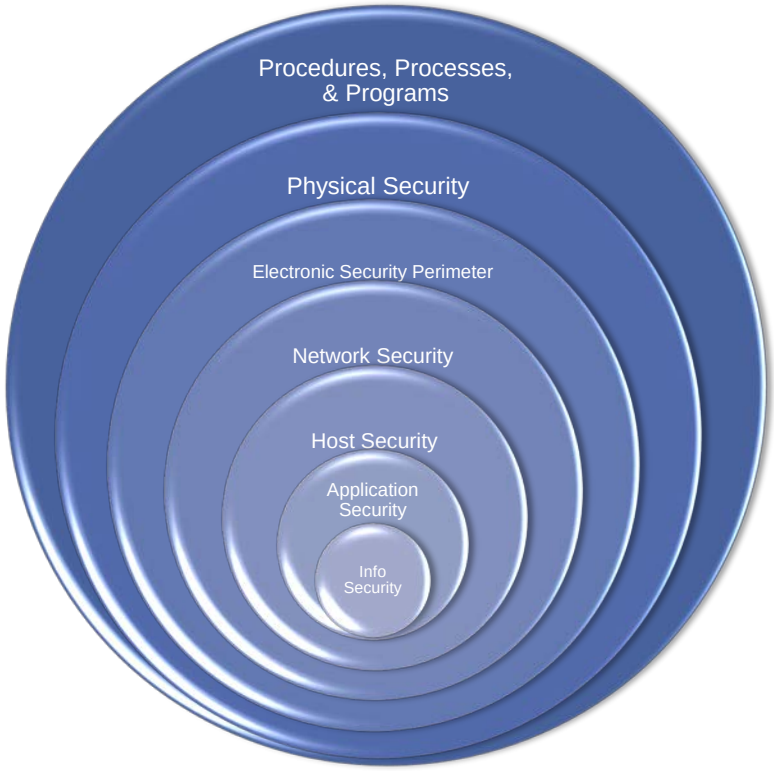


Figure 2: Layered security controls present with defense-in-depth strategies.

Suggestions to Address Disassociation between Compliance and Security

Compliance efforts should be driven from the top down through adequate resources, direction, communication, and structure.

To that end, if an entity's NERC compliance department is separate from other business units, it should have the authority to implement practices and procedures to ensure a consistent compliance program throughout the company. Alternatively, if an entity's corporate culture is such that compliance is made a priority, it may not matter how much actual authority it has. For example, a Region has observed an extremely successful compliance program despite the entity housing the compliance department in a separate business unit without much, or any, actual authority over other business units. The program works well because senior management has conveyed the message throughout the entity that compliance with the Reliability Standards is valued and necessary to ensure secure operations, thus enabling the compliance department to coordinate compliance efforts and ensure all business units make compliance a priority.

The CIP Senior Manager should be a key resource in these efforts. The CIP Senior Manager must have the responsibility and authority to lead and manage both the implementation of CIP compliance and the ongoing adherence to the CIP Standards.

Another strategy to ensure the entity strives to achieve reliable operations, which are also compliant, is to write procedures and processes that go above and beyond what is required for CIP compliance. These processes and procedures allow and encourage the entity and its employees to focus on reliable operations rather than focusing merely on what is necessary to meet the CIP Reliability Standards.

THEME 3: LACK OF AWARENESS

LACK OF AWARENESS: Not understanding how an entity's systems work or how its compliance department is functioning and performing.

Observations

An entity's lack of awareness of how its systems work or how its compliance department is functioning can result in significant CIP compliance deficiencies. The reasons for the lack of awareness can vary, but the Regions have recently observed four causes recur more often than others: (a) lack of vigilance; (b) insufficient expertise; (c) lack of engagement with the regulator; and (d) inadequate root cause analysis.

First, entities must stay vigilant in ensuring security and compliance. Entities that are considered top performers regarding security practices and compliance programs can sometimes fall victim to this theme. These entities can get too comfortable knowing they have a good compliance history and top security practices. But, assuming that the status quo will remain in place can be misguided, especially in an industry where the technology, threats, and rules are constantly evolving.

AWARENESS *Key Concepts*

Causes of Lack of Awareness

1. **Lack of Vigilance**
2. **Insufficient Expertise**
3. **Lack of Engagement with the Regulator**
4. **Inadequate Root Cause Analysis**

Helpful Resource

In 2017, FERC Staff released a summary report, Lessons Learned from Commission-Led CIP Version 5 Reliability Audits, which provides information and recommendations to assist with assessing risk, compliance, and overall cyber security.

As an example, one entity was advanced in terms of security practices, had a strong culture of compliance, and had a compliance history that indicated the entity could successfully identify, assess, and correct noncompliance. The entity assumed its program was working as intended in certain business areas, but failed to verify this assumption, and as a result, its patch management program in those areas suffered. The individual charged with managing the program was not keeping up with the procedures, and the entity failed to have quality checks in place to identify this deficiency.

Second, insufficient expertise can lead to deficiency in entities' CIP programs. For example, one entity tasked its compliance personnel, who were not technical subject matter experts, with doing some of the technical tasks required by the CIP Standards. This caused issues such as errors in identifying the Electronic Security Perimeter, including access points, which resulted in deficient security controls on the assets within the Electronic Security Perimeter. The compliance personnel did not have sufficient technical expertise to know they had a significant CIP compliance issue.

Third, the level of engagement an entity has with the Regions can impact the entity's ability to identify and correct deficiencies. The Regions take a proactive approach to security and compliance through external outreach and individual engagements and interactions with entities. However, an entity that is disconnected from this outreach or disinclined to raise questions or issues with its respective Region(s) may be less aware of some of its deficiencies. The entity's attitude might be that it will work with the regulator to the extent required. But, the Regions have found that entities are generally more successful when they are actively engaged because it allows the Regions to share with the entity best practices and trends that the Regions are seeing across the industry.

Lastly, an entity's lack of awareness may be caused by the entity not digging deep enough into known violations to understand the true root cause(s) in order to prevent recurrence. As illustrated in Figure 3, there are often multiple root causes, but these are not always as obvious.

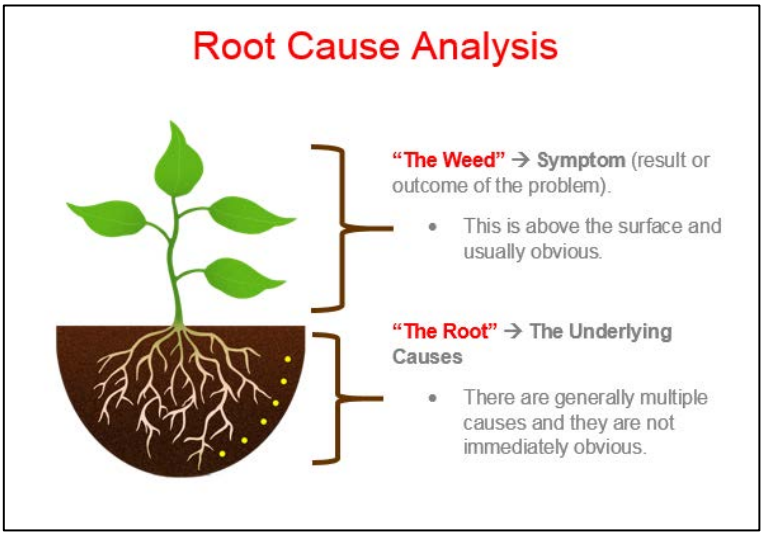


Figure 3: Root cause analysis basics.

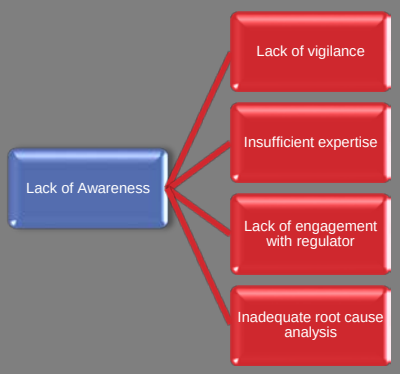
Where is your blind spot?

An entity should understand why it lacks awareness before trying to resolve its issues.

As Donald Rumsfeld explained:

> [T]here are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns -- the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones.

Entities should focus on the "known unknowns" and the "unknown unknowns" to understand where it is weak in its security posture.



Often, entities submit Mitigation Plans that identify the root cause as human error and then focus mitigation on re-training the individuals who made the errors. But, when we dig a little deeper, there is typically also room for improvement with respect to preventative controls. For example, an entity had a recurring issue with applying patches several weeks or months late. Because of the repeat nature of the issue, the Region took a closer look at the entity's procedure and determined it was lacking certain controls to ensure the individuals responsible for implementing the patches were meeting relevant deadlines. The entity then added a step to its process to have a small group of individuals (some of whom were not responsible for actually implementing the patches) meet on a monthly basis to track the implementation of mitigation plans to help ensure the entity met implementation deadlines. These types of verification controls can help avoid human errors, especially where entities experience recurring issues.

Suggestions to Address Lack of Awareness

While the root cause of the entity's lack of awareness may vary, the lesson for entities is that they should invest the time or financial resources necessary to fully understand their systems and programs and where their systems and programs may be weak. This is a continuous process, especially because an entity may be strong in a certain area, but then start falling behind due to changes in threats, technology, rules, and people or as a result of becoming comfortable with the status quo.

To understand where an entity is weak, entities should focus on quality management, which includes objective evaluations of the quality of the organization's reliability activities. These evaluations could be done internally by groups not performing the relevant tasks, or by third parties, or both. They could be periodic, such as annual third party audits, or could be embedded into existing procedures. For example, an entity could add an independent check within its access provisioning procedure where an individual (who is outside of the access process) could verify that the access is being provisioned as intended before the procedure is complete. Additionally, entities should use cross-functional teams where appropriate to help ensure consistency across the different groups in implementing the compliance program.

Another way to identify potential weaknesses is to perform benchmarking activities. Several entities have recently spent significant time benchmarking their security practices and compliance programs against each other and, as a result, were able to learn from each other and identify ways to improve their overall security postures. Entities can participate and engage in forums provided by the Regions for sharing best practices and benchmarking, such as seminars, outreach, and technical committees.

Lastly, if an entity does not have necessary expertise, then strong capabilities and performance in workforce management practices can assist the entity in ensuring it hires and trains the appropriate personnel to fit its needs. Workforce management includes establishing baseline competencies necessary to run a secure and reliable operation, taking an inventory of current skills, identifying gaps, and addressing the deficiencies by hiring appropriate personnel or providing training to current employees.

Ensuring Awareness

Quality Management **focuses on objective evaluations of the quality of an organization's activities to ensure the integrity of the activities.**

Quality Management plans should include:

- ✓ **Independent checks**
- ✓ **Staff participation**
- ✓ **Mechanisms for raising quality**

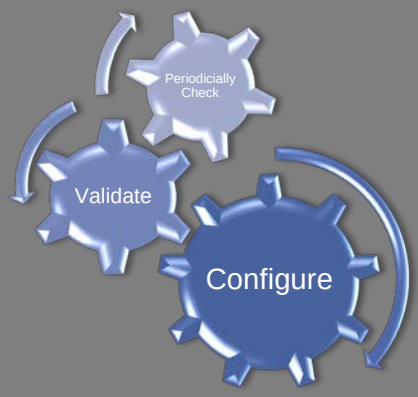
Helpful Resource

NERC's Cause Code Assignment Process: An Event Investigation and Data Analysis Tool, available here, provides a systematic approach to assigning cause codes after a bulk power system event.

TOOLS
Key Concepts

Automation Risks?

- ✓ **Follow documented process to configure.**
- ✓ **Validate configuration.**
- ✓ **Conduct periodic checks to ensure automation is functioning as intended.**



THEME 4: INADEQUATE TOOLS OR INEFFECTIVE USE OF TOOLS

INADEQUATE TOOLS OR INEFFECTIVE USE OF TOOLS: Not using tools that are necessary given an entity's environment, improper configuration of tools, and overreliance on automated tools.

Observations

As CIP programs mature, entities tend to increase their use of automated tools to assist with security and compliance. This is encouraged, especially for larger entities that manage thousands of assets and people. However, when implementing automated tools, entities should be careful not to over rely on the automated tools, and should implement manual controls to confirm that the tools are working as intended.

More recently, the Regions have observed some entities that, after implementing new tools, failed to verify that the tools were properly configured. In one case, an entity implemented a tool to create and track baselines, but failed to verify that the tool captured all of the entity's assets when creating the baselines. As a result, the tool failed to capture several assets and thus the entity was unable to track unauthorized changes to the baselines. Entities need to properly configure or "tune" these tools and then perform verification and validation exercises to ensure that they work as intended in the entity's environment.

Suggestions to Address Inadequate Tools or Ineffective Use of Tools

Automated tools can be extremely valuable in security and compliance. In the CIP world, such tools as log management, intrusion detection, and configuration management, although initially expensive, can save thousands of hours of manual effort and can help detect deficiencies or security breaches that manual processes cannot detect. However, it is a mistake to think that it is possible to purchase a tool and install it with no additional work. Such tools must be configured for the intended job, with input from end users, and this configuration is almost never simple. Additionally, entities must continuously update and maintain their tools.

Examples that the Regions have seen in the field include automated system configuration tools that assume all applications install themselves in the same way, and patch management systems that, by default, do not look in all applicable locations for patches.

CONCLUSION

Effective security and CIP compliance programs that are properly executed require an appropriate amount of technical expertise, senior management involvement, and a sense of ownership on the part of employees responsible for executing procedures. Once an entity develops coordinated, effective security and compliance programs, with input from senior management and others responsible for executing the programs, the entity needs to consistently execute this coordinated compliance program throughout the entity. And, to help ensure entities are always improving, or at the very least not falling behind, entities should create structured approaches to improvement that include regular meetings to discuss implementation and challenges of their programs. In addition, entities should continuously evaluate implementation of the program.

If any of these pieces are missing, an entity may encounter significant struggles in mitigating against the risks behind the CIP Reliability Standards.