Top 10 Compliance Issues for Implementing Security Programs

This White Paper articulates the top ten issues that we have encountered in the design and implementation of comprehensive Security Programs. Security Programs, in this context, are defined as policies, procedures, processes, evidentiary documentation and cyber and physical security vulnerability assessments.

While the issues delineated in this document are based on our experience in the implementation of the North American Electric Reliability Corporation's [1] (NERC) CIP Reliability Standard, we believe it is applicable to other standards such as the NIST guidelines and the Nuclear Regulatory Commission (NRC) Regulatory Guide 5.71. The CIP Reliability Standard is the most comprehensive and pervasive standard among all of the 100+ NERC standards in force today.

As background, NERC was designated as this "electricity reliability organization" (ERO2[2]) by FERC on July 20, 2006. The standard, which addresses asset identification, security management controls, personnel risk assessment and training, cyber and physical perimeter security, systems security management, and incident reporting and recovery, was developed to ensure all relevant electric utility entities identify and protect Critical Cyber Assets [3]that control or could impact the reliability of the Bulk Electric System (BES)[4]. The path towards ensuring a compliant Security Program has been appropriately designed and can be sustained is proving to be a challenge. This White Paper provides insight to the top ten issues that frequently surface during the course of implementing the requisite policies, processes, and evidentiary documentation requirements. The top ten issues are illustrated in Figure 1 and discussed in the paragraphs that follow.

[1] NERC is an international, independent, self-regulatory, not-for-profit organization, whose mission is to ensure the reliability of the bulk power system in North America.
[2] ERO refers to NERC's role. It is a generic name given by U.S. Congress to the independent entity that would be given the authority to develop and enforce mandatory standards for the reliable operation and planning of the bulk power system throughout North America, as called for in the U.S. Energy Policy Act of 2005.
[3] Critical Cyber Assets are essential to the reliable operation of Critical Assets and meet CIP 002, Requirement R3. Critical Assets are those facilities, systems, and equipment which, if destroyed, compromised, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the BES.
[4] The BES is defined as the electrical generation resources, transmission lines, interconnections with neighboring systems, and associated equipment, generally operated at voltages of 100 kV or higher. Radial transmission facilities serving only load with one transmission source are generally not included. The Bulk Power System, as defined in the Energy Policy Act of 2005, is generally defined as the same although different interpretations are present among regulators and industry.

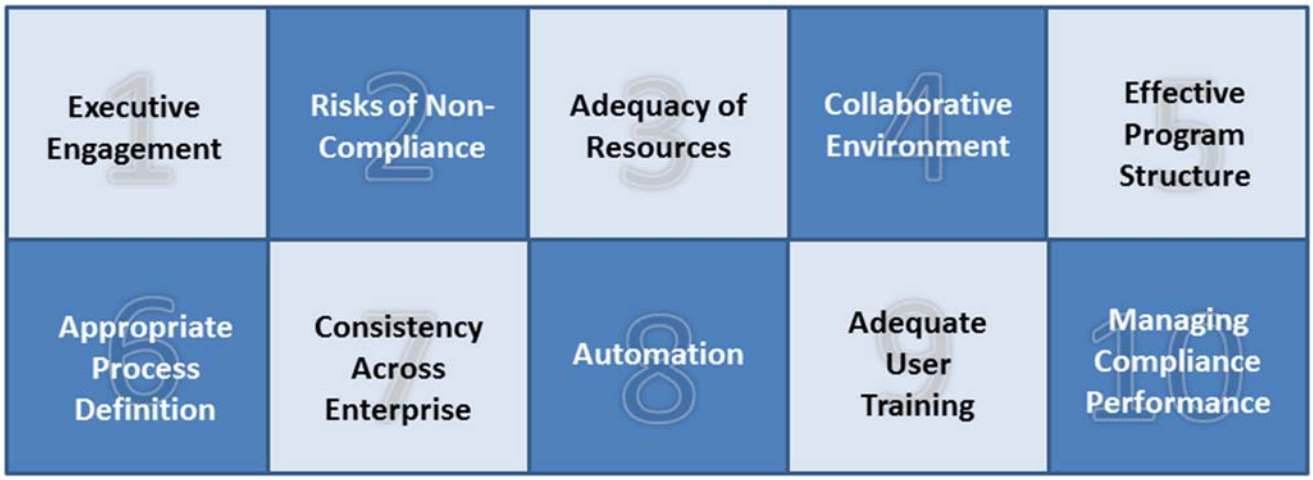

Figure 1: Top 10 Compliance Issues for Implementing Security Programs

1. Executive Engagement

One of the most strategic issues that can impact the design and implementation of a comprehensive Security Program is the need for executive engagement at the top of the organization. The need for this participation is based upon:

- The resultant policies, processes, and documentation required to implement a compliant Security Program impact multiple organizations.
- Direction and support need to come from a position that has the authority to provide an appropriate governance structure in order to ensure adequate participation and a collaborative environment resides within the requisite organizations.
- Considerable funding is required to design, implement, and sustain the compliant Security Program; appropriate budgeting at the executive level addressing the necessary vision across the corporation involving multiple organizations is needed to support the multi-faceted program.

In today's environment, a number of competing strategic issues are continually being assessed at the corporate level. These issues include, but not limited to, decreasing revenues during the current economic turmoil, smart grid initiatives, "green" related environmental issues, availability of capital, acquisition and resurgence of nuclear energy, aging work force, generation resources, transmission requirements, and the general reliability of the electric grid. With these issues on the forefront, the attention needed to mitigate the risk of non-compliance with the requisite security standards is often lost in the shuffle. In order to ensure compliance is sustained, an executive oversight committee (where issues can be surfaced) coupled with a cross functional team to support resolution of issues and maturing of the Security Program is a valuable and tactical management approach.

2. Risks of Non-Compliance

Non-compliance can result from a number of events culminating in substantial financial and social impact on the corporate entity. From an enforcement perspective, based on their audit findings of violations of the requirements of the standard, in terms of the NERC CIP Reliability Standard, the Regional Entities [5] shall, in accordance with published guidelines, determine and levy monetary penalties and non-monetary sanctions

[5] NERC shall have oversight of the application of the guidelines to ensure consistency.

and remedial actions[6]. Assessed penalties will be based on the Violation Risk Factors[7], Violation Severity Levels[8], repetitive violations, ability to pay, intentional violation, concealment of violation, self-disclosure and voluntary corrective action, and other extenuating circumstances.

Based on the maximum limitation penalties of up to $1 million per day per event, monetary penalties can be very significant. NERC is not constrained from assessing the same penalty amount for multiple violations that occur on the same day. Many of the proposed Violation Severity Levels have been designed such that significantly lower penalties will be assessed for those violations that are small in number or brought into compliance in a short period of time. Companies can reduce the amount of potential penalties by ensuring that non-compliance is identified, minimized, and resolved as soon as possible.

Non-monetary penalties can also be levied with respect to limitations in activities, functions, operations, and other appropriate sanctions. Sanctions may also impact the corporate posture with negative press. The worst nightmare is being on the front page in a story that illuminates a significant violation or event that caused an outage of the bulk electric system. In any event, there are significant non-monetary penalties that need to be evaluated in assessing the risks associated with non-compliance at any level.

As a result, the need for a formal risk management program is surfacing in many entities that have not developed the same. The directions being pursued by the regulatory authorities in this regard indicate that managing risks will be high on the agenda. Integrating risk mitigating provisions into the operations and underlying compliant Security Programs from a corporate perspective is a Critical Success Factor and vital business practice.

3. Adequacy of Resources

The resources (staff and funding) required to design, implement and sustain a compliant Security Program is quite significant and represents an important and visible budget item. Efforts to design a compliant Security Program have typically required between 2,000 to 10,000 man hours exclusive of user training, personnel risk assessments, and expenditures required for cyber and physical security infrastructure upgrades.

Ongoing sustainment will increase head count between one and five full time equivalents depending upon the type and number of infrastructures (generation facilities, substations, control centers) containing the Critical Cyber Assets (CCAs) or Critical Digital Assets (CDAs) as applicable to the underlying standard, the complexity of organizations involved in managing these assets, the number of staff having cyber and physical access to CCAs or CDAs, and the Information Protection program ingredients.

The recognition that the underlying Security Program requires significant resources to sustain the operations of the Security Program, especially in the first few years of operation, is one of the most significant miscalculations. For example, the effort alone to maintain configuration management through effective change control (including pre-testing, post-testing, approvals, documentation updates, etc.) for the requisite CCAs and CDAs, Electronic Security Perimeters, and Physical Security Perimeters can be quite daunting. Personnel risk assessment issues, especially at the initiation of the program, can also present a challenge to existing staff.

---

[6] Remedial Actions are directives that may be issued to a bulk power system entity to resolve an alleged violation that must be corrected to promptly reduce the reliability threat.

[7] Violation Risk Factors (VRFs) are assigned to each requirement of the standard and compare the expected or potential impact of a violation to the reliability of the bulk electric system. VRFs values include Low, Medium, and High.

[8] Violation Severity Levels (VSLs) are defined measures of the degree to which a violator violated a requirement of the reliability standard. VSLs values include Lower, Moderate, High, and Sever.

Ongoing sustainment staffing can ultimately be reduced through automation as described in the paragraphs that follow.

4. Collaborative Environment

The typical comprehensive security standard requires that organizations heretofore not operationally tightly coupled, or that do not communicate frequently, to collaborate in the design, implementation and sustainment of the compliant Security Program. Specifically the corporate information technology organization, or business IT, typically does not get involved in operations of the transmission or generation facilities. Likewise, the human resources department is not always linked in with access control processes. Substation engineering and transmission grid operations are also frequently located in separate departments. Generation operations are almost always separated. Finally, organizations addressing physical security and cyber security organizations are typically separated.

These organizational characteristics presents challenges to the design, implementation and sustainment of a compliant Security Program as a significant portion of the underlying compliant Security Program processes require smooth hand-offs across organizational boundaries. With this recognition, the governance issues raised earlier in this document become quite apparent. Ultimately, the need for a collaborative operations environment coupled with an appropriate governance structure is paramount in providing an environment for efficient and effective policies, processes, and plans to be sustained across the organization.

5. Effective Program Structure

The provisions that encompass most security standards were designed by multiple groups of engineers, information technology specialists, and physical security managers. Unfortunately, the resultant standard [9]is not necessarily organized in a logical and functional manner. It has proven to be very difficult and ineffective to take a Standard-by-Standard, Requirement-by- Requirement, approach to design, implement, and manage the sustainment of the compliant Security Program. For example, in the CIP Reliability Standard access control is addressed in four separate topical areas of the standard. As a result, utilizing the structure of the standard to govern the design, implementation, and sustainment activities adds considerable risk and complexity to the sustainment endeavor.

In order to simplify the design and implementation tasks and manage the sustainment of the compliant Security Program in an effective manner, a functional framework is considerably more appropriate. Functions define “what” needs to be done, processes (procedures) define “how” the work is to be performed, and “organizations” (the governance structure) defines who has responsibilities for performing the work. Functions are usually more static, processes typically cross functional boundaries, and organizations are frequently quite dynamic. Therefore, functional definitions provide a good “business model” foundation from which to assess, design, and implement new or enhanced programs.

Fifteen (15) different functional program areas[10], as illustrated in Figure 2, have been designed as relevant to the design and implementation of a responsive and comprehensive NERC CIP Reliability Standard compliant Security Program. This functional program business model provides the framework for an organized and logical approach to continually identify gaps, and subsequently develop the required policies, procedures, documentation, and training and security awareness program ingredients. In addition, any identified technical requirements, including supporting software tools such as document control systems, identity management

[9] The more recent NRC standard and NIST guidelines are more aligned with the functional framework concept.

[10] See The Challenge of Implementing NERC’s Cyber Standard, Public Utilities Fortnightly, September, 2006.

strategies, and network management tools, can be effectively developed in a controlled and consistent manner through this framework. Lastly, allocations of responsibilities within the organization can logically be assigned through a functional approach for sustainment of the Security Program.

Figure 2: CIP Reliability Standard Functions

It is important to note that visibility from a Standard-by-Standard / Requirement-by- Requirement dimension needs to be retained from an "audit" perspective. Auditors will need to understand and validate how each Standard and Requirement is being supported, e.g., what policy and process is being followed, and what evidentiary documentation is being generated to meet each of the underlying requirements of the standard.

Accordingly, the ingredients of the compliant Security Program need to be mapped (using a defined matrix) to the Standard / Requirement that they support. In conclusion, a multi-dimensional view is necessary to manage and provide ongoing audit support for the compliant Security Program.

6. Appropriate Process Definition

Today most standards define the need for "processes" throughout the requirements. Processes, in this context are frequently misunderstood as to what needs to be included in a process. First, there are two types of processes that need to be incorporated within a compliant Security Program as follows:

- Dynamic processes; and
- Structured processes.

Dynamic Processes are individually defined and assigned processes initiated to address an issue, gap, or commitment. Dynamic processes are typically uniquely defined "on the fly" and consist of one or two tasks assigned to specific individuals within the organization. The status of these processes are usually monitored until closed out or completed.

Structured Processes are pre-designed, more complex, processes typically consisting of multiple tasks and frequently involving multiple organizations. Structured processes need to be performed in a consistent manner and include appropriate internal control provisions. Structured processes are:

- Triggered by multiple Events, or the results of other Processes;
- Assigned by Roles rather than individuals;
- Contain a defined "Beginning" and an "End";
- "Self-documenting" e.g., generate evidentiary documentation each time they are performed;

- Define the "who, when, where, why, and how" the Policies (which defines the "what") will be implemented:
  - "Who" defines the roles and responsibilities;
  - "When" defines the timing of the Process (Event / Time Driven);
  - "Where" defines the location as applicable;
  - "Why" is to define the purpose of the process;
  - "How" defines the sequence and description of the Activities and Tasks.

Both types of processes are required to sustain a compliant Security Program. Dynamic processes can best be supported through the use of automated commitment management or tracking systems appropriately integrated with existing internal E-Mail and document management systems.

Structured processes are frequently designed to leverage existing procedures [11]using "pointers" or "references" to guide users through multi-task processes. This approach can leverage existing procedures and reduce the expenses associated with designing the required compliant Security Programs ingredients. However, as a result, these types of structured processes are frequently not "self-contained[12]" and difficult to use while not retaining the key characteristics noted above. These characteristics impact the complexity of the

Security Program and the ability to incorporate provisions for internal controls, ensure self-documentation, identify appropriate process linkages, and incorporate appropriate performance measures. Recognizing that Critical Cyber Assets or Critical Digital Assets [13] typically represent a small portion of the total number of cyber assets in the entity, at the risk and costs of duplicating processes, it is highly recommended that, as a general rule, self-contained processed be employed in the design of the compliant Security Program.

7. Consistency Across Enterprise

It is recognized that different types of infrastructures (generation plants, substations, transmission grid control centers) and organizations (divisions) operate differently. For example, generation facilities have scheduled maintenance outages at which time a variety of changes and upgrades can be made while transmission grid control centers are 7 x 24 operations. In other situations, different labor laws may impact the personnel risk assessment related processes in different divisions of the enterprise. Accordingly, there is usually a desire to customize the policies, processes, and documentation for each type of infrastructure. While there are certain processes that certainly need customization as such, the complexity of the compliant Security Program can become unmanageable if customization is allowed to flourish beyond reason. This is especially true if provisions for automation are contemplated in the future.

Therefore, in order to retain consistency and provide a means to effectively manage the complaint Security Program from a corporate perspective, customization should be minimized or employed in situations where the involvement of multiple organizations is minimal.

---

[11] The terms "Procedures" and "Processes" are frequently used interchangeably. In the context used herein, "Procedures", which can be written in responsibility – action or narrative formats, are text-based description of "Processes", the latter of which are visual depictions (flow charts) of the sequence of tasks using "swim lane" illustrations for responsibilities. In either case, appropriate evidentiary documents should be generated each time the process or procedure is executed.

[12] Not all processes need to be self contained. For example, the more stringent cyber access control requirements of the CIP Reliability Standard can effectively be integrated with the existing access control procedures. This approach is quite appropriate for this function. Alternatively, existing processes can be enhanced to incorporate the requirements of the CIP Reliability Standard. Existing incident response and disaster recovery procedures may also be effectively utilized.

[13] Or cyber assets that need to be protected.

8. Automation

It is acknowledged that most security programs are complex and contain a pervasive set of requirements necessitating the design, implementation and sustainment of a compliant Security Program that touches most departments / organizations within an organizational entity. In addition, non-compliance with the program has significant ramifications that heretofore have not been a component of the risk management agenda.

Once a compliant Security Program has been designed and successfully implemented, maintaining an efficient and effective sustainment becomes the objective of the day. Automation of many of the processes, both dynamic and structured processes as discussed earlier, and evidentiary documentation tasks obviously increases the efficiencies and can result in hard dollar savings (personnel costs).

A means to track gaps between changes in the NERC Reliability Standards and the compliant Security Program is also of great benefit to prevent future out of compliance conditions from occurring. However, many of the benefits for automation are not so obvious. For example, automation can:

- Mitigate consequences of missing deadlines and commitments;
- Minimize level of effort and costs to sustain Security Program;
- Ensure responsibilities for following through with process commitments, decisions, documents, and reports are completed;
- Ensure that process triggers will be executed (scheduled events and results linked from other processes);
- Improve timeliness and accuracy of compliance performance metrics and executive dashboards;
- Alert staff to upcoming events and requirements;
- Leverage information contained in existing systems;
- Ensure processes, tasks, and results are appropriately documented;
- Facilitate external audit readiness;
- Provide a basis for identifying gaps;
- Ensure compliance dates are maintained;
- Generate audit trails; and
- Ensure Security Program is consistently optimized and standardized across organizations and company.

The overall benefits for automating the basic functions of a compliant Security Program, provides a quick hard dollar payback amplified by the intangible benefits of ensuring compliance is maintained. There are a number of software solutions available in the marketplace, each with their advantages and disadvantages, which can be configured to provide an integrated solution while leveraging existing systems.

9. Adequate User Training

User training is for those individuals in the organization who will become involved in the execution of the policies, processes and procedures and generate relevant documentation. It is an essential component of the compliance Security Program that is frequently overlooked. The training includes review of the process responsibilities, defined processes and procedures, triggers for the processes, and how to generate the required evidentiary documentation and what to do with the results. User training, in this context, excludes the annual training required by many standards for those staff that have access to the requisite cyber assets being protected. The latter is a prepackaged training curriculum that can be fulfilled in a short period of time. In summary, this initial training component of the compliant Security Program is often overlooked and underestimated in terms of the time and resources required to continuously carry out the requirements of the

program. Estimates for large organizations have ranged up to 1,600 man days of user time for the initial training and familiarization with the processes and documentation requirements (also called role-based training). Subsequent training will be required as the program requirements evolve and issues, gaps, and commitments are addressed and fulfilled.

10. Managing Compliance Performance

Self-certification is a typical milestone that signifies the completion of compliant Security Program design, build, and implementation phases and the start of the operations management. Usually, only a portion of the standard requires specific controls. Measures in the standard in most cases refer to documentation of the associated requirement and are not measures of a compliance process or procedure performance. As a result, most entities in a time and resource constrained environment have not included focused design steps to ensure that controls, metrics, and performance risk assessments are addressed for all procedures. Few have had the luxury of analyzing newly developed security procedures for performance variations (i.e., non-compliance events). Additionally, most independent assessments and audits of compliance readiness target the identification of evidentiary documentation required for compliance, and not risk of non-compliance performance.

If the CMI SEI Capability Maturity Model [14]concept is applied to compliant Security Programs at most entities, one could generalize that most have moved from the Initial (Ad Hoc) and Repeatable maturity levels to the Defined level. A key success factor in compliance efficiency lies in the ability to embed compliance processes into existing operations. The more integrated the processes required by the standard are, the more effective the operations personnel will be in the execution of the additional requirements. With the procedures documented and personnel process knowledgeable as a result of implementation training, the procedures are then institutionalized as the “security-focused” way of doing cyber and physical security. Progression to the Managed level requires process metrics and a management focus on reducing procedure variations.

It takes a combined top-down and bottom-up approach to identify and design an effective metrics program to support ongoing compliance program management. Key performance indicators should be developed and linked to corporate objectives that include compliance objectives. Metrics should be identified and defined for supporting security-based processes using the SMART (specific, measureable, actionable, relevant, and timely) approach. Where existing systems have been modified to accommodate security requirements, new metrics reports will be necessary.

For more information:
DYONYX, LP
solutions@dyonyx.com
1-855-749-6758

[14] Carnegie Mellon Institute Software Engineering Institute