

A Phased Approach to NERC CIP 002-009 Compliance

Electric grid operations are highly interdependent — a failure in any single transmission can affect an entire region. What's more, the industry depends on the consistent and reliable availability of physical grid resources, integrated and scalable software and systems, and skilled knowledge workers. Volatility in sourcing, pricing, or quality of these market resources could have negative consequences for a utility company and its customers.

NERC CIP standards are designed to safeguard the industry and its customers against a variety of risks through vulnerability assessments, threat response strategies, disaster recovery planning, personnel screening and training, physical and cyber security controls, and other measures. Because of this complexity, those responsible for compliance should pursue a structured implementation methodology, which leads to a full understanding of all requirements, responsibilities and commitments — ensuring CIP compliance.

Phase 1: Assessment

The Assessment phase is the foundational and most important phase of a critical infrastructure protection program lifecycle: identifying assets critical to mission success and prescribing suitable security controls and other supporting security management infrastructure.

NERC CIP-002 diverges from NERC 1200 by requiring responsible entities to begin with a list identification of their Critical Assets (e.g., power plants, substations, and control centers). Those responsible for compliance need to establish their own "risk-based" criteria that correspond to their unique position in the grid, and Cyber Assets that support essential functions. The scope of a CIP compliance project is based on Critical Cyber Assets, and the list needs to be finalized before moving onto policies, information protection, training, network upgrades, physical security, security management infrastructure, backups, and recovery plans. See figure 1.

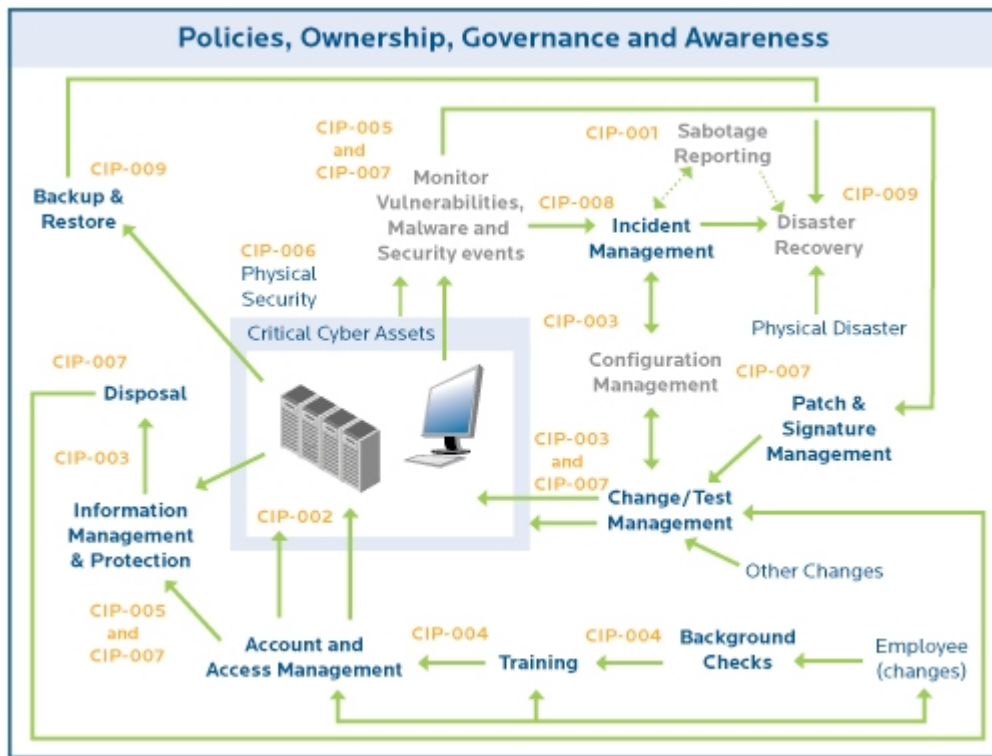


Figure 1: NERC CIP-002-009: Asset-Driven Program

Phase 2: Remediation

Here are suggested activities for the remediation phase of NERC CIP compliance.

Standard	Remediation Activities for Achieving NERC CIP Compliance
CIP-003: Security Management Controls	<ul style="list-style-type: none"> • Security Policy Assessments • Cyber Asset Security Baselines and Technical Standards • Information Protection and Handling • Security Management Strategy and Program Development • Deployment of Change Management Procedures
CIP-004: Personnel and Training	<ul style="list-style-type: none"> • Development of awareness solutions • Development of Training programs for visitors, contractors, employees, administrators and management • Access Controls for both Physical and Cyber Access
CIP-005: Electronic Security Perimeter(s)	<ul style="list-style-type: none"> • Network / ESP assessments • Network Architecture assessments • Wireless Architecture assessments • Identity and Access Management • Intrusion Detection Systems • Vulnerability & Risk Assessments • Firewall Management & Monitoring

	<ul style="list-style-type: none"> • Vulnerability Management • Installation of test and production infrastructure including cabinets, Secure Administration Gateway Environments (SAGE), firewalls, network infrastructure, secure dial-up etc.
CIP-006: Physical Security	<ul style="list-style-type: none"> • Physical Security Assessments • Physical Security Plans
CIP-007: Systems Security Management	<ul style="list-style-type: none"> • Security Testing Requirements • Security Control Test Procedures • Catalog, Analysis and Hardening of Ports & Services • Patch Tracking, Evaluation, Testing and Installation Program and Supporting Infrastructure • Antivirus Deployment Strategies • Manual and Automated Security Logging Programs and Infrastructure • Cyber Asset Retirement and Disposal Plan
CIP-008: Incident Reporting and Response Planning	<ul style="list-style-type: none"> • Incident Response Gap Analysis • Incident Response Plan Development • Incident Response Training • Incident Response Testing & Evaluation • IDS/IPS Management & Monitoring • Forensic & Incident Response
CIP-009: Recovery Plans for Critical Cyber Assets	<ul style="list-style-type: none"> • Business Impact Assessment • Selection and implementation of backup infrastructure • Development of Backup and Restoration procedures for data and assets • Disaster Recovery Plan Development • Disaster Recovery Plan Training • Disaster Recovery Plan Testing

Phase 3: Management

An effective CIP Compliance Management solution automates data collection, analysis, reporting, and compliance workflows, providing the following benefits:

- More accurate data in the compliance system (owing to less reliance on human data entry).
- Updates, correlation, and analysis are done by a tireless and accurate automated system.
- Lower risk of non-compliance penalties (owing to better data management, analysis and reporting)
- Personnel requirements reduced by more than one half (freeing the compliance team for analysis, management, and reporting, rather than data collection, data entry, clarification, correlation, and submission).
- With automatically orchestrated workflow and real-time information, companies can manage their compliance program continuously, rather than being deadline driven

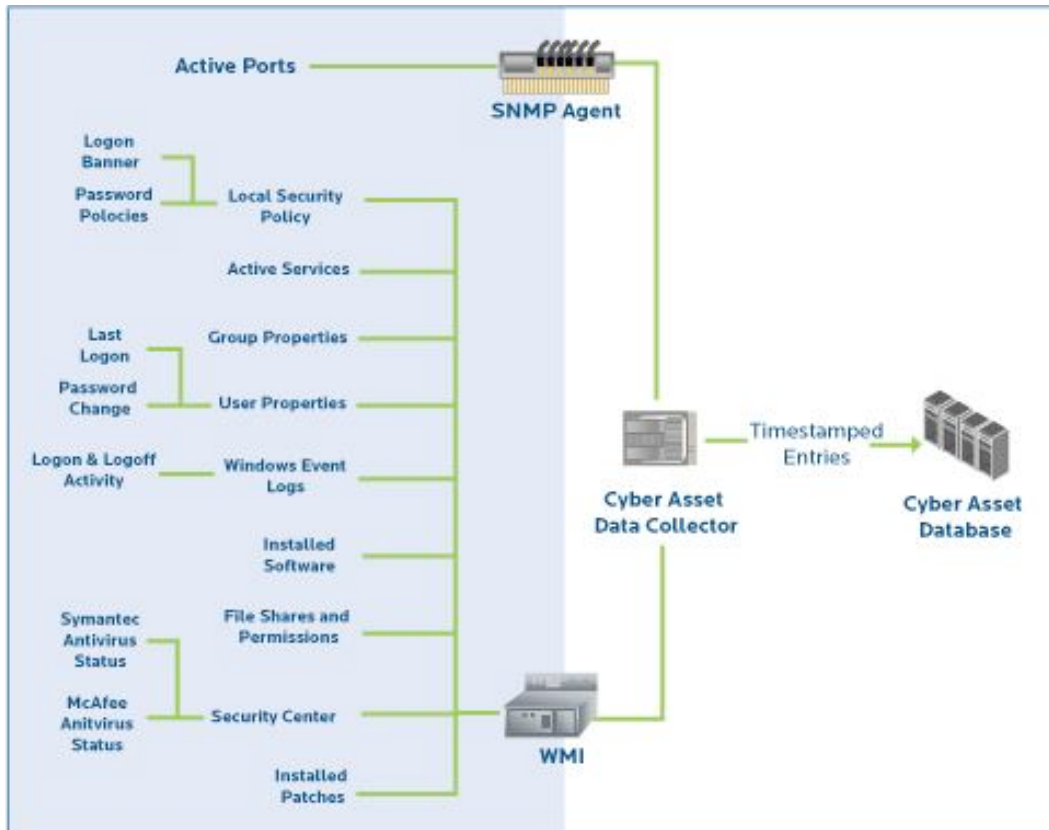


Figure 2: Automated NERC CIP Compliance Management – Sample Data Requirements

Phase 4: Compliance Assurance

By this phase, the company should have the following well-established:

- Policies and procedures
- Physical security controls
- Cyber security controls
- Cyber security perimeters
- Infrastructure

The biggest problem with sustaining compliance is regularly monitoring and tracking:

- Access to cyber assets
- Change detection
- Exception reporting
- Regular information collection, analysis and reporting.

Compliance management processes can be compared to the recurring business reconciliation activities each financial quarter or year end for reporting purposes. Today, Enterprise Resource Planning (ERP) solutions are routinely used to expedite and automate and businesses can get a snapshot of their financial health, on demand. This more accurate and more timely information supports more informed and more profitable business decisions.

When you apply this same type of automation to NERC CIP compliance, you can reap similar benefits. With a system automatically collecting information, analyzing it and reporting, and finally, orchestrating compliance-related business processes, you are never in the dark about your compliance status. For example, a system like this can seamlessly correlate training with cyber access, physical access, past cyber access logs and also physical access records to allow only access that is truly required. Also, it can ensure that personnel always have valid certification appropriate for their for their position description.

The Bottom Line

With a system that supports the convergence of multiple disparate data sources, such as cyber asset lists, training records, physical access rights and logs, cyber access rights and logs, patching status, change detection, security logs, and document status records – and when this system understands the relationships between these in the context of NERC CIP compliance and automates the workflow necessary to keep you compliant, you gain:

- Increased productivity.
- Fewer and better managed exceptions.
- Fewer self-reports.
- Improved reliability.
- Lower staffing costs.

Quote from text: "With a system automatically collecting information, analyzing it and reporting, and finally, orchestrating compliance-related business processes, you are never in the dark about your compliance status."