Control Compliance Suite - NERC and FERC Regulation

The North American Electric Reliability Corporation (NERC) is a non-profit organization which oversees eight regional reliability entities and encompasses all of the interconnected power systems of the United States and Canada. NERC has created a number of standards including those focused on the protection against cyber attacks. The most widely recognized of these is NERC 1300 which calls out Critical Infrastructure Protection (CIP) standards CIP-002-1 through CIP-009-1.

These NERC specified network security administration and best practice guidelines were made legal regulation by the Federal Energy Regulatory Commission (FERC) as of January 18, 2008 via 18 CFR Part 40.

http://www.ferc.gov/whats-new/comm-meet/2008/011708/E-2.pdf

History of NERC Standards

While these complexities pose challenges to enhancing security in the electric power industry, the need for security has never been more acute. The need to maintain or enhance power system reliability and availability drives increased security. Stated another way, security is a business enabler for reliability and availability in the new interconnected environment.

And today, the need for security is now formalized as a regulatory requirement. NERC has approved wide-ranging cyber-security guidelines ("NERC CIP") to replace narrower, temporary precautions adopted in 2003 as the NERC Cyber Security Standard 1200 (and renamed the NERC Cyber Security Standard 1300 in 2004). NERC CIP is the first set of comprehensive requirements to protect electric utility assets from cyber security attack. Compliance will be enforced by Energy Reliability Organization (ERO). NERC was designated as the ERO in July, 2006. Refer to www.nerc.com for more information.

Most electric power utilities have already achieved compliance with NERC Standard 1200 and are currently planning compliance with NERC CIP. NERC CIP covers the same areas covered by the NERC 1200 Standard, but with some important differences. Major changes from NERC 1200 to NERC 1300 CIP include power generation is now being covered; new security areas now covered such as disaster recovery, patch management, and different types of policy compliance, enforcement, and practices.

NERC CIP Standards

NERC CIP identifies the minimum requirements to implement and maintain a cyber security program and to protect cyber assets critical to reliable bulk electric system operation. It is divided into the following eight separate reliability standards:

- CIP-002: Critical Cyber Asset Identification
- CIP-003: Security Management Controls
- CIP-004: Personnel and Training
- CIP-005: Electronic Security Perimeter(s)
- CIP-006: Physical Security
- CIP-007: Systems Security Management
- CIP-008: Incident Reporting and Response Planning
- CIP-009: Recovery Plans for Critical Cyber Assets

CIP 002—Critical Cyber Assets Identification

Critical Asset Identification Method: A risk assessment methodology should be used to Identify all critical assets. The risk assessment should include the following activities:

- **Operational Risk Assessment:** In this step, critical operational assets are identified and underlying information technology is cataloged. Once completed, a qualitative risk analysis is performed to identify possible threats and vulnerabilities. The risk analysis should also take into account possible threats that could be mitigated or exacerbated by interconnectivity with other parties. Identified threats should include a threat description, the probability of the threat causing a problem, and the impact of that problem.
- **Network Vulnerability Assessment:** A network vulnerability assessment should be performed to accurately depict the current security posture of cyber assets associated with critical infrastructure.
- **Policy Review:** All associated policy documentation should be reviewed to assess its overall effectiveness in policy and practice.
- **Gap Analysis:** Based on information gathered during the network vulnerability assessment and policy review, a gap analysis should be performed to evaluate current practices in accordance with policies and CIP requirements.
- **Security Awareness Review:** A general review of executive and operational security awareness should be performed. General security practices and the strategic importance of security should be evaluated.

CIP 003—Security Management Controls

Security Policy: The responsible entity should have a security policy in place, explicitly stating executive management's commitment to security. The security policy should describe the framework for implementing and managing security controls, including the security principals, standards, and regulatory requirements to which the responsible entity is subject. The security policy should describe where in the organization responsibility for security resides.

CIP 004—Personnel and Training

Awareness: A security awareness program that describes and communicates the security policy and all relevant procedures and standards should be provided for all employees.

Training: all employees, whose role has a security component, including users with access rights to classified information or system administrators responsible for the management of critical cyber assets, should receive security training.

Personnel Risk Assessment: Background checks should be conducted on all candidates for roles with access to classified information or access to critical cyber assets.

Access: The responsible entity should maintain records of all access rights for all employees or contractors with access to classified information or to critical cyber assets. Access rights should be reviewed on a quarterly basis. An individual's access rights should also be reviewed upon any change in position or responsibility (including promotions within the department).

CIP 005—Electronic Security Perimeter

Defined Electronic Security Perimeter: The electronic security perimeter should be well delineated and thoroughly documented. Any access through the perimeter should go through a limited number of well-controlled points that only allow the minimum number of ports and services, and are configured for default deny.

Electronic Access Controls: Two-factor authentication should be used for any access through the electronic security perimeter. Authentication should be centralized for all access points. Where two-factor authentication is not feasible, access through the perimeter should also be limited to known hosts.

Wireless Security: All wireless traffic should be encrypted using 128-bit or better encryption. Systems using 802.11 wireless should be tuned to the minimum strength required, not broadcast SSID, and use WPA2 encryption with AES.

Protocol Security: All traffic traversing the electronic security perimeter should be encrypted using 128-bit or better encryption.

Vulnerability Assessment: A vulnerability assessment should be performed quarterly on the electronic security perimeter. These assessments should identify all devices on the perimeter, the ports and services allowed through the devices, and any devices that are visible through the perimeter.

Monitoring Electronic Access: All traffic traversing the electronic security perimeter should be logged. All logging performed by devices on the electronic security perimeter should be stored on a centralized log server. These logs should be reviewed monthly and retained for at least 90 days.

Documentation Review and Maintenance: All systems in the electronic security perimeter should be thoroughly documented, and the relationships between systems should also be documented. All changes should be thoroughly reviewed and implemented according to a documented procedure, and those changes should be immediately reflected in the documentation.

CIP 006—Physical Security

Physical Security Plan: The physical security plan should outline the physical perimeter and controls around all critical assets and critical cyber assets. It should address potential vulnerabilities and contain plans to respond to or mitigate potential risks.

Documentation Review: Physical security documentation should be reviewed quarterly to ensure that it reflects the current environment and controls that are in place in the environment.

Physical Access Controls: Electronic locks with a centralized authentication system supporting two-factor authentication should be used wherever possible. If this is not possible, strong key control procedures should be used to prevent loss, theft, or unauthorized duplication of keys. All critical cyber assets should be located in secure facilities, with restricted access.

Identification: All employees and visitors should be required to wear photo identification badges that are clearly visible above the waist at all times.

Logging Physical Access: All attempted and successful access to areas containing critical assets or critical cyber assets should be logged electronically to a centralized logging server.

Monitoring Physical Access: All potential entry points to the physical security perimeter should be monitored electronically. Dedicated staff should monitor video in real-time.

Access Log Retention: Access logs should be reviewed monthly for unauthorized access and retained for at least 90 days. Video should be retained for at least 90 days.

Maintenance and Testing: All physical security controls should be tested quarterly to ensure effectiveness.

CIP 007—System Security Management

Non-critical Cyber Asset Inventory: All devices within the electronic security perimeter should be defined and cataloged. This catalogue should list the details of every asset, including the type of asset, location, manufacturer, model number, serial number, version, date installed, network address, hardware address, and date of last inspection or maintenance.

Test Procedures: Any changes to the production environment must be documented, approved by authorized authority, tested in a non-production simulation of the running environment, and then applied to the production network during a scheduled window, with a rollback procedure.

Ports and Services: A best practice is to ensure that only those ports and services necessary to provide essential functionality should be enabled on all cyber assets.

Security Patch Management: When patches are released by device manufacturers, they should first be evaluated for criticality based on the severity of the potential exploits they address.

Malicious Software Prevention: All systems that support anti-virus software should have antivirus software installed. The client software should be configured to update definitions at least every 24 hours from a secure, centralized server controlled by the covered entity.

Security Status Monitoring: All systems should log to a centralized log host, and those logs should be reviewed monthly and retained for at least 90 days.

Disposal and Redeployment: All decommissioned systems should be destroyed and not re-used. If systems must be re-purposed, all hard drives should be overwritten with random data seven times, and all BIOS settings should be reset to the default before being released.

Cyber Vulnerability Assessment: A vulnerability assessment should be performed quarterly against all devices within the electronic security perimeter. These assessments should identify all devices on the network, the ports and services running on the devices, and any applications running on the devices.

Documentation Review and Maintenance: All non-critical cyber assets should be documented, and the relationships between systems should also be documented.

CIP 008—Incident Response

Incident Response Plan: The responsible entity should implement an incident response plan that explicitly states the authority under which the plan operates the constituency for the plan, and the services that the plan will offer that constituency. Also, the jurisdiction of the incident response team should be defined together with any dependencies on other internal or external organizations.

Incident Response Documentation: The incident response team should maintain records of all incidents or suspicious events, including original evidence such as system or host logs, video or physical access records. Also, all records of investigation of, or response to, an incident or event should be maintained. Report all incidents to ES ISAC. For more information, refer to http://www.esisac.com.

CIP 009—Disaster Recovery

Recovery Plans: Recovery plan must define action triggers, acceptable downtime service level, and acceptable data loss. The recovery plan should include critical vendors as part of the planning process and a risk assessment.

Exercises: Define, perform exercises, and evaluate results based on probable disaster scenarios.

Change Control: Document changes to critical assets, recovery plans, and test procedures.
Changes must be must be kept current with regular updates.

Backup and Restore: Recovery of critical assets must be ensured with applications to acceptable patch level, data to acceptable interval, and network/operating system configurations to the last known state. Additionally, authentication mechanisms must have the capability of being restored to the last known state.

Testing of Backup Media: Backup media must be verified to a level that ensures that the data catalog is not corrupt and that can be restored to an acceptable level. Media must be available within an acceptable time period and re-usable media must be within its life cycle.

How Symantec Control Compliance Suite Addresses These Requirements

Automation of Technical and Procedural Evidence Gathering

Symantec delivers the most comprehensive solution to automate the process of compliance. Businesses everywhere are attempting to cost effectively comply with mandates like those called out by FERC regulation. But achieving good governance and successfully addressing this problem means having a comprehensive view; one that spans across the need to understand regulatory requirements to performing technical assessments. Control Compliance Suite (CCS) and Policy Manager (PM) provide this holistic approach.

With Symantec Control Compliance Suite and Policy Manger organizations can easily formalize and automate the tasks that are typically weak links in compliance: assessment, remediation, approval workflow, exception management, and consolidated reporting. CCS/PM helps organizations tackle those difficult problems, while also easing the task of defining and managing policies, mapping policies to controls, publishing policies to end users, and collecting/archiving evidence of compliance.

Managing NERC/FERC CIP Controls with Control Compliance Suite

Symantec's Control Compliance Suite can assist organizations in complying with all of the NERC/FERC CIP CIP-002-1 through CIP-009-1 requirements.

Control Compliance Suite works through a process of scheduled agent-less reporting. Detected issues or non-compliant situations are handled through change controlled remediation to provide end to end management. Our development and research teams are consistently updating CCS content to ensure our customers have the most up-to-date best practice control recommendation and guidance information.

Summary

The Control Compliance Suite meets the requirements of NERC/FERC compliance head on by providing a holistic and automated method to gather both procedural and technical control evidence. Most importantly, CCS provides a consolidated visualization of compliance to NERC/FERC regulation and other mandates and provides a means to quickly identify and remediate deficiencies before they come under auditor scrutiny.

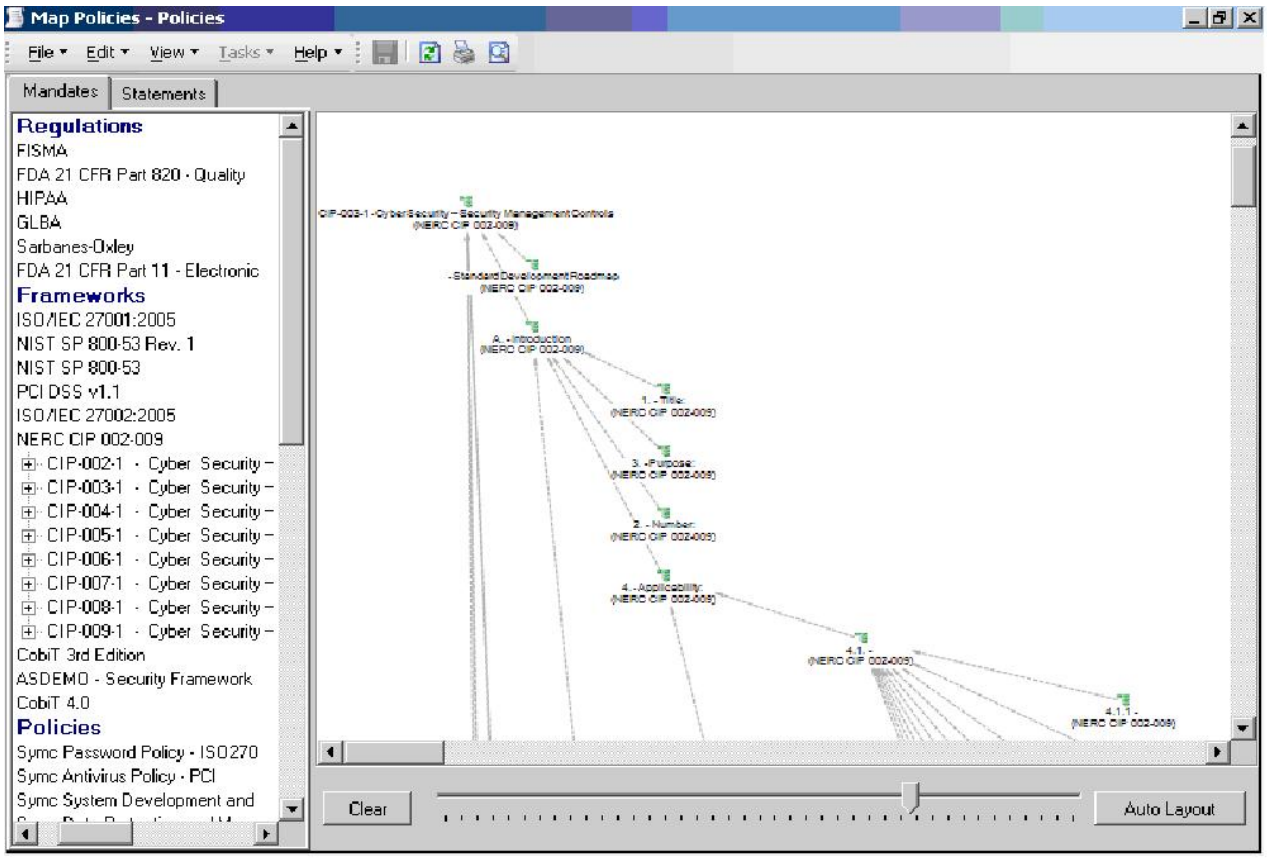

Figure 1: View Mappings of Regulation Requirements to Control Statements

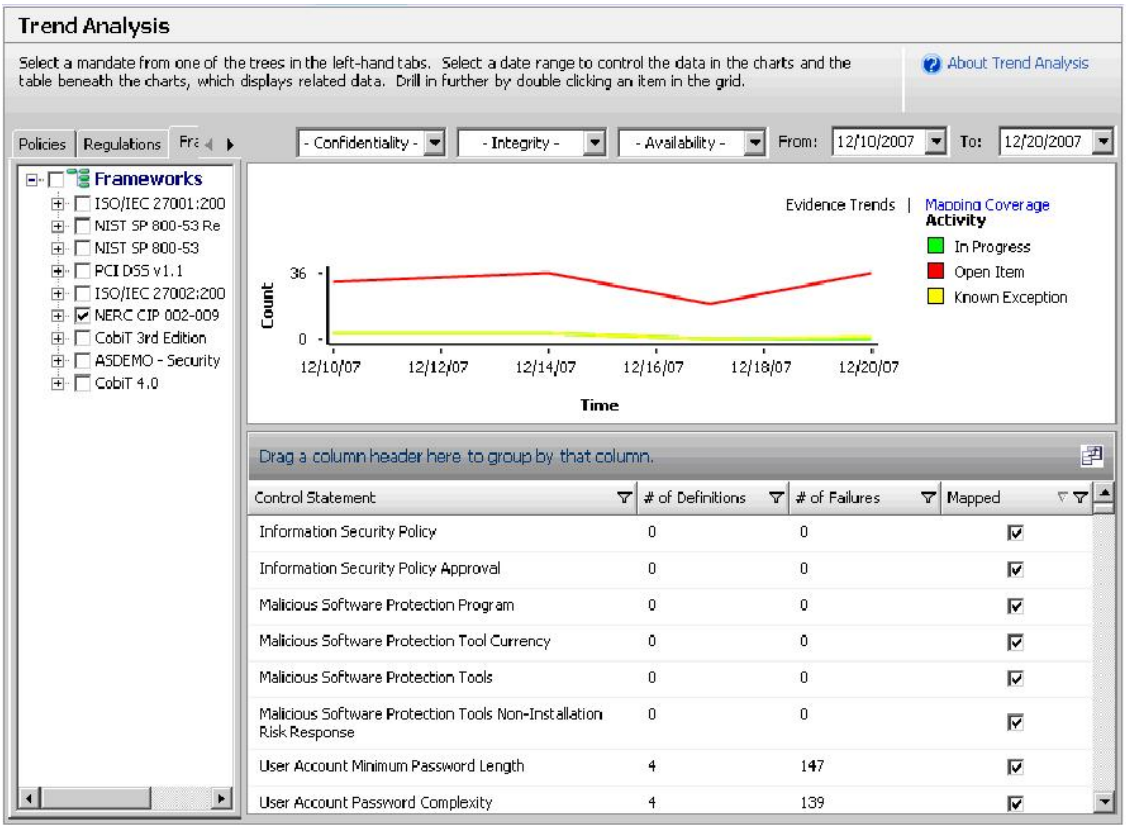

Figure 2: Track Control Statement Coverage to Manage Compliance Objectives

Contact Us Today

Call toll-free 1 (800) 745 6054

Visit Our Web Site

http://enterprise.symantec.com

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

10/08 14566044

Confidence in a connected world.

symantec.