qmulos

PRODUCT BRIEF

NERC CIP: Q-Compliance

REAL TIME RISK MANAGEMENT & CON-MON COMPLIANCE FOR CRITICAL CYBER ASSETS

Control Categories

- ✓ CIP-002-5.1a: BES Cyber System Categorization
- ✓ CIP-003-6: Security Management Controls
- ✓ CIP-004-6: Personnel & Training
- ✓ CIP-005-5: Electronic Security Perimeter(s)
- ✓ CIP-006-6: Physical Security of BES Cyber Systems
- ✓ CIP-007-6: System Security Management
- ✓ CIP-008-5:Incident Reporting and Response Planning
- ✓ CIP-009-6: Recovery Plans for BES Cyber Systems
- ✓ CIP-010-2: Configuration Change Management and Vulnerability Assessments
- ✓ CIP-011-2: Information Protection
- ✓ CIP-014-2: Physical Security

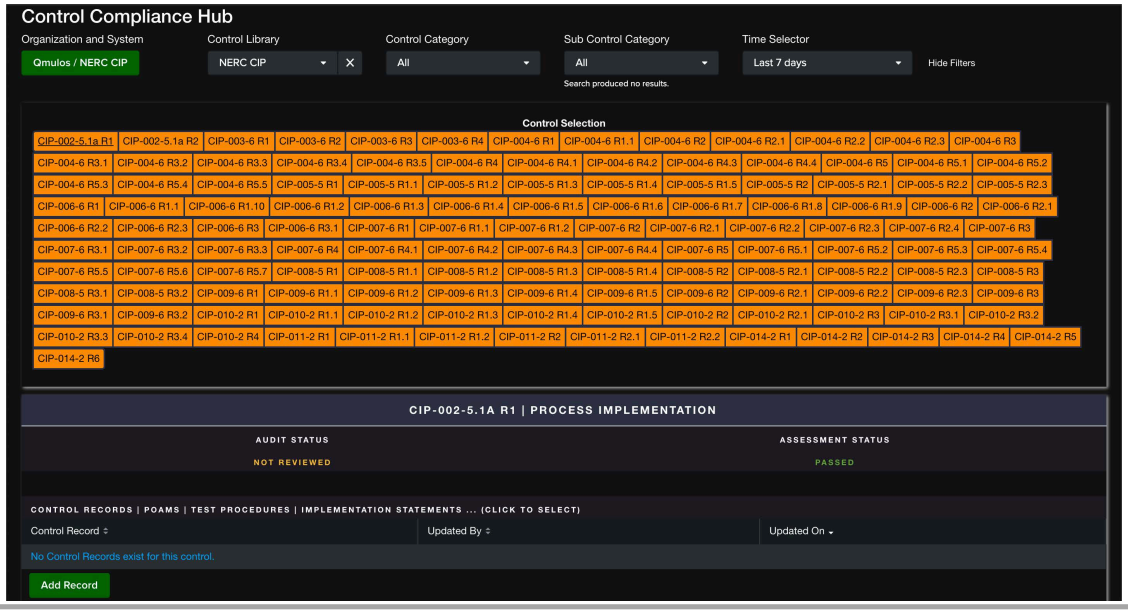
splunk> POWERED

The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) program is a set of standards to govern entities deemed critical to the bulk power system (BPS), to include reliability coordinators, balancing and interchange authorities, transmission and generation providers, owners, operators and users of any portion of said system, and are measured through risk assessments and audits on best practices and documented standards, compliance enforcement, and the procedures regarding distribution of critical information.

Maintaining and demonstrating compliance with NERC CIP is often implemented by manually collecting evidence of human activity, business processes, policies, and snapshots of limited technical data, such as quarterly or annual vulnerability scans and configurations. As a native Splunk powered solution, Q-Compliance solves this problem by applying a compliance lens to near real-time data being ingested across your enterprise and assessing it against the NERC CIP controls. Splunk is easily the best solution for ingesting data and providing visibility in near real-time. However, with such a powerful tool, sometimes data can get tricky and hard to contextualize; this is where Qmulos comes in.

Q-Compliance, is purpose-built to help you streamline and automate complex cybersecurity auditing and compliance requirements like NERC CIP, NIST 800-53, CMMC, HIPAA, and many others. By selecting the NERC CIP dashboard, the user can track how your organization and systems are scoring against each of the control categories, and where you need to improve. The dashboard provides the ability to quickly drill into specific domains to view compliance against the capabilities, practices and processes set forth, and drill into individual controls to see the specific systems, events, and assets that are non-compliant.

Q-Compliance also gives the user the ability to upload policy, procedure and file evidence as well as automatically log human activity—it keeps evidence needed for audits all in one place, making things more organized as well as efficient. Q-Compliance also aligns specific security controls with the NERC standards to use real-time log and event data from Splunk to help you automate the assessment and scoring of your organization's practices against NERC CIP. In addition, we have codified industry best practices into the workflow of the application that will help your organization institutionalize and optimize the processes that improve your cyber posture and protect critical cyber assets.



- Real time risk and compliance visibility, by control category or sub category
- A single pane of glass for all technical, human, or file (linked or uploaded) evidence and artifacts
- Workflows for time and event-based assessments

1560 Wilson Boulevard, Suite 900, Arlington, VA 22209 www.qmulos.com