SYNOPSYS®

www.synopsys.com |

Your Trusted Partner for NERC CIP Compliance and Beyond

Maximize your investment in the Cyber Vulnerability Assessment (CVA)

Performing a CVA is an annual requirement for electric utilities that must comply with The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP). We empower utilities to address mandatory NERC CIP compliance requirements (annual CVA audit) plus build a foundation for a comprehensive end-to-end risk-based mitigation approach to cybersecurity.

We prepare your organization for NERC CIP audits

We help satisfy CIP audit requirements by conducting a CVA that specifically targets two NERC CIP standards: CIP-005 (Electronic Security Perimeter) and CIP-007 (Systems Security Management). We bring more than 20 years of experience in cybersecurity to help your organization execute a thorough CVA and remediate any issues that are discovered.

Devices sitting on the edge of your electronic security perimeter, including smart meters, collector units, or reclosers, are now interconnected devices that run sophisticated software. In large part, the Smart Grid gets its name from the sophisticated hardware and software distributed on the edges of your electronic perimeter collecting data, making decisions, and taking actions in real time. You need a partner that provides deep expertise in software, firmware, network, mobile, and physical security to comprehensively examine the controls protecting your critical assets.

Comprehensive and cost-effective approach to delivering CVAs

Every CVA consists of an end-to-end security evaluation, which includes:

- A review of your existing CIP documentation and the results of previous assessments
- Identification of Electronic Security Perimeter (ESP) access points through manual and automated methods
- A report with actionable remediation guidance to help fix any discovered vulnerabilities
- Assessment of default accounts, passwords, and network management controls
- A detailed port and service review on each identified access point
- Detailed documentation to support your CIP audit

Protecting the electronic security perimeter created by the Smart Grid requires an understanding of your utility's threat model and the critical assets protected by your electronic security perimeter. Traditional network security does not cover the security of the software components within all new Smart Grid technologies. Our vast experience in both network and software security can help your organization comprehensively evaluate your security posture. This examination involves evaluating risks across multiple layers, from software running on embedded devices to the physical security controls in place. Your people, process, and technology controls are systematically evaluated against the risks they face from your adversaries.

We believe an end-to-end security evaluation is necessary to protect your organization and ensure a successful NERC CIP audit.

Going beyond compliance with a cyber-risk management program

Your customers expect you to keep the lights on and your investors expect you to increase shareholder value. Not paying due attention to security hinders your ability to achieve these business imperatives. While Smart Grid enables you to achieve reliability and cost efficiency, it also opens your organization to cyber-based risks that necessitates a systematic approach to security risk management composed of three phases:

1. **Gap Analysis and Remediation Planning.** Understand the current state of your cybersecurity program across people, process, and technology dimensions, and identify where gaps exist against defined best practices. This phase provides your organization with a custom remediation plan that is based on your company's unique risk profile.
2. **Remediation Plan Execution.** Mitigate your people, process, and technology risks by executing the remediation plan customized for your company. For example, this may include conducting security awareness training, performing vulnerability assessments, or addressing third-party security risks. This phase results in either the establishment of a cyber-security program, or fine tuning of an existing program based on the remediation plan.
3. **Ongoing Program Execution.** Continually execute and enhance your cybersecurity program activities to maintain a security posture at a level where your organization's risks are within defined tolerance levels. This will involve continuing some of the activities started during Remediation Plan Execution phase (e.g., vulnerability assessments) and will also include an ongoing program to manage cyber risks related to third-party products and services. This phase enables proper risk management, as well as cost-effective compliance with existing and upcoming cyber-security regulations.

3 reasons to choose us as your CVA partner

Building a cyber-risk management program is a complex endeavor that requires an experienced partner to help you navigate the challenges and maximize the return on your security investment.

1. In partnership with NRECA, we created the Guide to Developing a Cybersecurity and Risk Mitigation Plan, consisting of tools, a risk mitigation checklist, and a step-by-step template to help utilities address cybersecurity risks holistically and systematically.
2. Our practical and actionable approach to cyber-security risk management has been downloaded thousands of times and is currently in use by dozens of utilities across the world after having been widely praised by DOE.
3. We were also a contributor to the creation of DOE's Electric Subsector Cybersecurity Capability Maturity Model (ES-C2M2).

Contact us to start a dialogue about helping your organization meet current NERC CIP compliance requirements, stay ahead of emerging requirements, and implement the right security risk management approach for your organization.

To learn more about how we can help you conduct your CVA,
contact us at software-integrity-sales@synopsys.com or +1 800.873.8193.

The Synopsys Difference

Synopsys offers the most comprehensive solution for integrating security and quality into your SDLC and supply chain. Whether you're well-versed in software security or just starting out, we provide the tools you need to ensure the integrity of the applications that power your business. Our holistic approach to software security combines best-in-breed products, industry-leading experts, and a broad portfolio of managed and professional services that work together to improve the accuracy of findings, speed up the delivery of results, and provide solutions for addressing unique application security challenges. We don't stop when the test is over. Our experts also provide remediation guidance, program design services, and training that empower you to build and maintain secure software.

For more information go to www.synopsys.com/software.

Synopsys Inc.
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: (800) 873-8193
International Sales: +1 (415) 321-5237
Email: software-integrity-sales@synopsys.com