Achieving Security Program Alignment with the NIST Cybersecurity Framework

INTRODUCTION

ScottMadden partnered with a large energy provider to align its security program with the NIST Cybersecurity Framework (CSF). The decision to align with the CSF was driven by a desire to develop a best-in-class security program and meet industry security expectations. The security program scope included the following:

- Information Technology (IT) and Operational Technology (OT) cybersecurity
- Physical security
- Personnel security

The CSF, the result of a 2013 Executive Order—"Improving Critical Infrastructure Cybersecurity"—is a voluntary set of standards, guidelines, and practices designed to help organizations manage security risks. While voluntary, alignment with the framework allows energy companies to demonstrate security program rigor toward meeting industry security expectations.

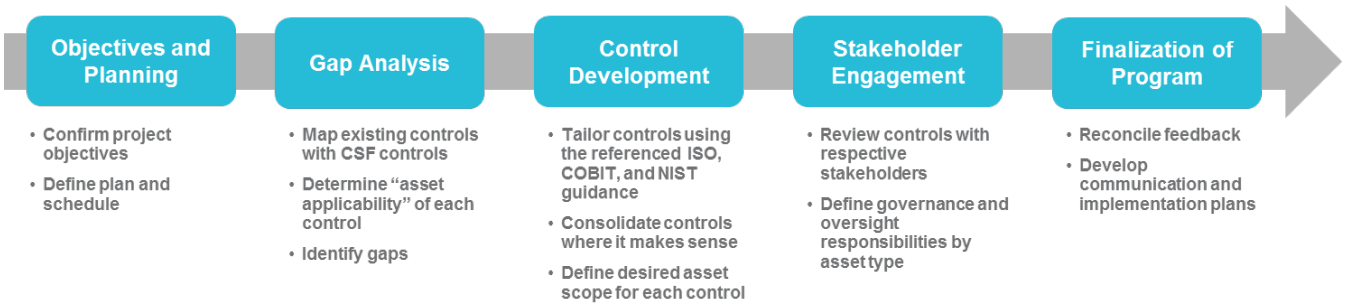
THE CHALLENGE

The CSF is comprehensive and references a number of existing cybersecurity standards, including ISO, other NIST standards, COBIT, and ISA. The client's existing security program was aligned exclusively to the ISO 27001 standard. Therefore, a number of controls were already in place, but there were gaps between CSF and current practice. These gaps were identified, and new controls were developed to close these gaps and create a complete program fully aligned with the CSF. While the CSF provides guidance, control language needed to be tailored to the organization to make it both practical and relevant.

Governance and oversight responsibilities for each control were defined to facilitate implementation of the revised security program. This required gaining buy-in from diverse stakeholders, each of whom had varying levels of experience with implementing security controls. Developing the right path for implementation of the revised program and communicating the benefits of the CSF were critical to overcoming objections and ensuring alignment with the desired future state cybersecurity framework.

HOW WE HELPED

ScottMadden used a collaborative approach to build consensus and ensure stakeholder engagement and alignment with the changes to the security program. Workshops and other activities allowed key personnel to provide significant input into the development of controls, establishment of governance, and development of implementation and communication plans. This approach was based on the five-step process depicted below.



Upon completion, the revised program included the following attributes:

- Controls tailored to the environment and fully aligned with the CSF
- Comprehensive applicability – IT, OT, and physical assets and personnel
- Integration with the corporate risk strategy and methodology
- Established and agreed-upon governance and oversight responsibilities for each control

ScottMadden organized the security program across core security functional areas to instill ownership and document accountability. The end result was a comprehensive and tailored program designed to enhance the understanding of security risks and the role of each employee in combatting those risks.

RESULTS

The following outcomes were delivered from this effort:

- A relevant, practical, and comprehensive set of risk-based controls tailored to the environment
- A consolidated security controls program inclusive of all important enterprise assets
- A program aligned with a leading edge industry framework that can be used to communicate security posture and drive ongoing improvements

ScottMadden's collaborative approach engaged stakeholders and cybersecurity experts from throughout the enterprise to develop a risk-driven, industry-aligned cybersecurity program.

Contact Us

ScottMadden, Inc.
3495 Piedmont Road
Building 10, Suite 805
Atlanta, GA 30305
www.scottmadden.com

Jon Kerner
Partner
678.702.8346
jkerner@scottmadden.com

Henry Bell
Director
678.702.8338
henrybell@scottmadden.com