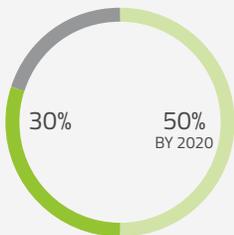


Benefits

- Align the organization with industry-recognized security best practices
- Leverage the knowledge of our experts as related to the CSF, NIST, FISMA, ISO, and other industry requirements
- Identify the shortcomings and resources needed to meet requirements
- Ensure infrastructure, staff, and security controls are robust, effective, and cost efficient
- Enhance reputation with executive management and clients that the organization is providing the best security possible



Gartner recently announced that 30% of all US organizations have adopted the Framework for measuring their security posture. Further, they believe that 50% of all organizations will adopt the Framework by 2020.

The NIST Cybersecurity Framework (CSF) provides a flexible, repeatable, and cost-effective risk-based approach to managing information security risk through analysis of five core functions; identify, protect, detect, respond, and recover. The NIST CSF Gap Analysis empowers organizations to develop and implement security standards and management practices, including the implementation and management of controls through an informed risk-based decision process.

Adoption of a risk-based security framework is a significant investment for any organization. Cylance Consulting's NIST CSF Gap Analysis assists organizations in **building an effective information security program**, which helps to **minimize exposure to risk**, and **ensure a clear strategy for handling incidents while maintaining a process for continual improvement and monitoring**.

Service Overview

The goal of Cylance Consulting's NIST CSF Gap Analysis is to evaluate the policies, standards, and procedures implemented by the organization and how they align with the five core functions; identify, protect, detect, respond, and recover. Cylance Consulting's experts work with your staff to identify positive practices in your program, as well as areas for improvement.

Elements of consideration include:

- Policy, Standards, and Procedures
- Program Management
- Human Resources and Organization
- Asset Management
- Physical and Environmental Considerations
- Communications and Operations
- Access Control
- Information Systems Management
- Response Plans and Management
- Regulatory Compliance

Deliverables

Cylance Consulting will furnish a comprehensive report detailing:

- Assessment findings and alignment to the NIST CSF
- Remediation strategies to achieve compliance with the NIST CSF and industry best practice
- Instructions for developing a roadmap for continuous improvement and monitoring

Understand the basic components of a solid security strategy. Contact Cylance Consulting or your technology provider to schedule yours today