LYNX
TECHNOLOGY PARTNERS

CSF Quick Tip Checklist

This document is a quick reference guide for creating your IT risk program following some of the key elements of the NIST Cyber Security Framework.

Identify

The organization identifies its mission objectives, related systems and assets, regulatory requirements, and overall risk approach.

Create a Current Profile

Beginning with the Categories specified in the Framework Core, the organization develops a Current Profile that reflects its understanding of its current cyber security outcomes based on its implementation of the Identify Function.

Conduct a Risk Assessment

The organization analyzes the operational environment in order to discern the likelihood of a cyber security event, and the impact the event could have on the organization. It is important that critical infrastructure organizations seek to incorporate emergent risks and outside threat data to facilitate a robust understanding of the likelihood and impact of cyber security events.

Create a Target Profile

The organization creates a Target Profile that focuses on the assessment of the Framework Elements (e.g., Categories, Subcategories) describing the organization's desired cyber security outcomes.

Determine, Analyze, and Prioritize Gaps

The organization compares the Current Profile and the Target Profile to determine gaps, and then determines resources necessary to address the gaps. The organization creates a prioritized action plan that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile.

Implement Action Plan

The organization implements the steps defined in the action plan and monitors its current cyber security practices against the Target Profile.

Three Keys to Remember:

1

Risk is the context in which you apply your security program. It is the language that business will understand. The foundation of a risk program is based on the controls, which in turn are influenced by regulatory and statutory mandates.

2

Be careful with absolutes, as risk is about gray areas – probability x impact. Probability by it's nature is often qualitative; Impact can be quantitative, but at some point, you'll always have to make a best guess backed by the facts at hand. So don't be afraid to use both methods to communicate risk. But no matter how you calculate risk, keep it simple.

3

The CSF is just a framework – think of a house and the blueprint/framework that guides the structure of the house, but not the make-up. The walls can be stone, brick, wood, or compound materials – these elements can be customized to your needs. Similarly, the elements of the CSF will vary by each organization's specific need, and you will have to customize these to your use cases.

www.LynxGRC.com