NIST Cybersecurity Framework 10 Step Guide

Protecting client confidentiality, maintaining compliance, and building trust.

1 Identify Critical Assets

Catalog sensitive data: case files, client communications, etc.

→ **Know** what you have to protect it effectively

2 Assess Your Current Posture

Evaluate your existing cybersecurity practices using NIST CSF

→ **Reveal gaps** and prioritize improvements

3 Establish Security Policies

Create policies for passwords, device use, remote work, and data

→ **Empower** your team with clear expectations

4 Review Cyber Insurance Policy

CGP provides a free policy review to ensure your firm is fully covered

→ **Ensure Policy** aligns with firm's risks

5 Train Your Team

Educate attorneys and staff on phishing, safe browsing, and client data handling.

→ **People are your first line of defense**

6 Gather Client Requirements

Understand the security requirements of your clients as each may have different needs

→ **Aligns** the firm with client compliance needs

7 Implement Safeguards

Deploy MFA, firewalls, 24x7 endpoint protection, etc.

→ **Build strong,** layered defenses

8 Practice with tabletop exercises

Simulate a cybersecurity incident in a no-risk environment to test your firm's response

→ Schedule **yearly** to review and improve your plan

9 Create an Incident Response Plan

Outline how your firm will respond if there is a security incident

→ Speed and transparency matter

10 Back Up & Recover

Regularly back up data and test restore procedures

→ **Prepare for worst case scenarios with minimal downtime**

512-649-2424

help@clear-guidance.com

www.clear-guidance.com

ALA VIP℠ Value in Partnership

CLEAR GUIDANCE PARTNERS
STRATEGY + TECHNOLOGY