CYBERSECURITY ASSESSMENT FOR NONPROFITS

Comprehensive cybersecurity assessments to safeguard your organization

Contact Armanino to discuss how we can help you with your cybersecurity concerns.

CONTACT US:

Jeremy Sucharski, CISA, CRISC
Partner
Governance, Risk and Compliance
925 790 2838
Jeremy.Sucharski@armaninoLLP.com

Ryan Prindiville
Practice Leader, Strategy & Transformation
925 790 2833
Ryan.Prindiville@armaninoLLP.com

Learn More
armaninollp.com/services/cybersecurity

Armanino's Cybersecurity Assessment Services help you combat the growing threat of cyberattack and safeguard your reputation, digital assets and donor and member data.

Our nonprofit experts provide a holistic review of your current environment, including your people, processes and technology. We evaluate your ecosystem, identify gaps versus your cybersecurity goals and objectives and help you develop a comprehensive and cost-effective cybersecurity plan that isn't just about an expensive technology solution.

Your Challenges

Cybersecurity breaches don't only affect large, for-profit corporations. Hackers are increasingly targeting nonprofit organizations, because they typically have older, more vulnerable systems and few or no proactive cybersecurity processes in place, making them easy prey. A study by Tech Impact and JPMorgan Chase found that almost 80% of nonprofits do not have adequate data backup and protection to safeguard sensitive donor data.

Faced with unknown threats, disparate systems and a weak security infrastructure, many nonprofit organizations don't know how to identify their risks and create an information security program. This puts their stakeholders at risk and leaves the organization completely unprepared if a breach occurs, which can do irreparable damage to their reputation. Our goal is to help you protect that reputation.

Process and Value

Our holistic assessments map your current state and help you define your cybersecurity goals. We focus on continuous improvement, not single-use checklists, to deliver value immediately and for the long-term health of your organization and your mission. With a proven methodology, our team helps you identify technical, organizational and administrative control deficiencies and strengthen your security processes. Depending on your needs, our review may include:

- Information risk management
- Threat and vulnerability assessment

- Security assessments, including NIST, ISO 27k, PCI readiness and COBIT
- Network security
- Operational security
- Privacy and data protection
- Employee awareness training
- Incident response planning

Assessment Types

Health Check: We review your technology environment against a framework (ISO, NIST) at a high level, to give you an understanding of your cyber-related risk exposure.

QuickStart: We perform a Health Check to assess your vulnerabilities, then we prioritize your risks and provide your management and operations teams with a step-by-step roadmap for implementing an information security program that achieves your cybersecurity goals.

Comprehensive: The Comprehensive Assessment includes everything the QuickStart Assessment offers and goes a step further. We map your IT environment to the appropriate framework (ISO, NIST) and help you implement your information security program, including controls for asset management, operations, access management and business continuity planning.

Upon completion of your assessment, we can work with you to help you manage your cybersecurity program on an ongoing basis.