SEVNX

SECURITY FRAMEWORK ASSESSMENT

What is a Security Framework Assessment?

Security frameworks are comprised of a comprehensive set of established practices for managing cybersecurity. A Framework Assessment can help you understand how you stack up against those recommended practices. Some common frameworks include:

NIST CSF 2.0

defines six functions of cybersecurity controls as Govern, Identify, Protect, Detect, Respond, and Recover. NIST CSF 2.0 is becoming the most common framework being adopted.

ISO 27001

an international standard for managing information security. ISO 27001 has the benefit of a formal certification process.

NYDFS

Regulations such as NYDFS require covered entities to have a cybersecurity expert to oversee / implement the organization's cybersecurity program.

Other

common frameworks include the Payment Card Industry Data Security Standard (PCI DSS), HIPAA HITECH also known as the HIPAA Security Rule, and the Cybersecurity Maturity Model Certification (CMMC). These frameworks may be relevant depending upon your industry, your customers, how you do business, and the information you collect and process.

Could My Organization Benefit From a Security Framework Assessment?

Framework Assessments are beneficial to many organizations, including those without established Security Programs who don't know where to start and those with established programs who want an independent assessment to identify gaps in the people, process, and technology. Framework Assessments can be a productive exercise in strategic planning and budgeting for cybersecurity.

Why Use SEVN-X for Your Next Assessment?

Our mission at SEVN-X is to help our customers achieve better cybersecurity. Our Advisory Team brings broad security frameworks experience as well as assistance in implementing security programs following security frameworks.

info@sevnx.com

SEVNX

484.989.0911

ACHIEVE BETTER CYBERSECURITY