enVista®
enabling enterprise commerce™

IT Security and Risk Assessments

enVista's tools and methods for assessing your IT environment are focused around a core set of procedures and products with a proven track record of accuracy and adaptability. Our security experts maintain industry certifications, take part in educational and information exchange forums, and routinely evaluate the tools and workflows used to maintain effectiveness.

Our security assessments are performed in stages including an initial questionnaire and consult, followed by technical scans and running assessment tools. Utilizing these inputs, enVista can then produce an appropriate assessment report based on your organization's required and recommended security posture. The report sections are reviewed with your company's management at a high level and internally by our team of security and infrastructure specialists. The results and outputs of the security assessment then become an integral component of the security roadmap and plan for our combined team.

Risk Assessment:

- enVista can perform the following IT risk assessments, among others:
  - **General IT** – We utilize industry-standard NIST guidelines.
  - **Cyber Security** – This assessment focuses on risk to your internal systems and public Internet presence for the organization. It includes detail on security, availability, and data integrity fundamentals.
  - **PCI DSS** – The PCI DSS standard assessment includes components from our General IT and Cyber Security assessments and also specific best practices and procedure review for organizations that process or maintain credit card data and transactions.
  - **HIPAA** – The HIPAA standard assessment adds a focus on patient data and personal information (ePHI) protection to our standard General and Cyber Security assessment criteria. We can adjust it specifically for businesses that are included under specific regulatory bodies such as the FDA or specific business models.
  - **Sarbanes-Oxley** – The Sarbanes-Oxley standard assessment is typically used for publicly-traded companies and has a focus on demonstrating security due care and diligence to those with a stake in the business.
  - **NIST Assessments** – The National Institute of Standards and Technology has produced a body of guidelines and processes for maintaining security posture and planning. The NIST guidelines can be used specifically to audit or assess organizations with State or Federal regulatory relationships or as tools for general risk management and security practices. NIST frameworks often work in parallel with Federal Information Management Security Act (FISMA) standards among others.