SECURITY ASSESSMENTS

Your Business, Your Mission, Secured!

Identifying and Addressing Risk & Resiliency for your technologies, to meet your business objectives.

HIPAA COMPLIANT

Security Assessments

Cybersecurity assessments assist an organization to identify, assess, and evaluate risk in their current and future state business environments. These assessments help to validate whether an organization has implemented the appropriate cyber controls for the technologies used to meet business objectives.

- It is imperative organizations have a transparent understanding of its current security posture to maximize it's security dollars, protect critical assets, customer or business data, and maintain pace with business growth.
- Fidus will partner with your organization to simplify traditional security assessments and provide effective, actionable security recommendations. We do this by conducting a security assessment tailored to your business industry and the systems and data leveraged to achieve your business goals.
- We will be your partner, treating your company and its critical assets as our own, thereby maximizing your investment dollars and aligning to the security of your business objectives.

Types of Security Assessments

We leverage this control framework to provide continuous governance and support to security professionals, including CISOs, in assessing and reporting cyber security to organizational leadership.

Health Insurance Portability & Accountability Act (HIPAA)

- **HIPAA's main goals are: 1.** Protect the overall security and privacy of healthcare information, **2.** Increase the efficiency of the healthcare system, **3.** Establish disclosure standards and protect against fraud & theft. HIPAA requires covered entities or organizations to complete a risk assessment to maintain compliance with HIPAA safeguards and controls.
- Our HIPAA assessment framework & methodology simplifies the numerous security control reviews by providing clients with an understanding of current state compliance. We provide transparent recommendations for opportunity remediation and a strategic, prioritized security roadmap.

National Institute of Standards and Technology (NIST) & Cybersecurity Framework (CSF)

- **NIST CSF** is a set of cybersecurity best practices and security recommendations that help businesses understand cybersecurity risks, identify and manage potential opportunities to remediate, as well as, reduce overall risks to critical networks, systems and data.
  - **ISO 27000** series of cybersecurity standards to assist organizations protect their information assets. ISO 27001 is a global standard for efficient information management to prevent security breaches and ensure critical data is protected in the event of an incident or breach.
- **NIST SP 800-52** is a set of Security & Privacy controls for federal information systems and organizations to meet the requirements of the Federal Information Security Modernization Act (FISMA).
- **NIST SP 800-71** are recommendations that review and address key establishment techniques that leverage symmetric key cryptography algorithms to protect symmetric keying material.

HIPAA COMPLIANT