EITS
Enterprise IT Security

Security Assessment and Enablement

At a high level, security assessment is about identifying, prioritizing, and managing risk for your organization

SOLUTION BRIEF

Although a framework and standards are key in this process, we believe each customer requires a tailor-fit based on where they are in the Cyber Security Maturity Model and considering their priorities. EITS aligns our security assessors based on experience in industries and/or specific compliance requirements customers may have; for example, the needs of manufacturing customers can differ from those of healthcare or financial organizations. Our team brings a combination of experience identifying and quantifying risk in addition to managing risk and solving security challenges from a customer's perspective.

KEY BENEFITS

- Understand current security controls and supporting processes
- Identify weaknesses that can be exploited
- Compliance Assessment
- Enable the right security investments

Security begins with RISK Management

The goal is to provide you with an understanding your current security control, supporting processes, and potential areas for improvement. Data results are used to enable the right security investments on a go-forward basis. Though we utilize a three-step assessment process (identify, prioritize, and manage), each step is structured and methodical.

Identify

Using the NIST CSF (Cybersecurity framework) as a foundation, we develop an understanding of risk to systems, people, assets, and data.

1. Inventory
Physical and software assets to establish a foundation for asset management.

2. Assess Business
Identification of business environment(s), role(s) in supply chain, and critical infrastructure.

3. Policy
Identify existing or required policies to define governance program, legal and regulatory requirements, and potential cyber security gaps.

4. Vulnerabilities
Exposures to internal / external resources that can be exploited by an adversary; risk response activities are also a basis for risk assessment.

- This goes beyond vulnerabilities on internal physical or software assets and into identification of potential flaws in a customer's existing security controls/ architecture.

Prioritize

Often, organizations will be faced with cyber risks far beyond what can be solved in weeks, months, or even years. The ability to prioritize what can realistically be done, and push lower priorities out, is critical to a successful security program.

An example of outcomes includes:

- Stakeholder matrix
- Gap analysis/ roadmap
- Threat inventory:
  - Categorize
  - Probability scale
  - Impact assessment
  - Financial impact

Security Criticality Rating

A structured way to assess the security criticality of software and supporting physical infrastructure based on the sensitivity of data and criticality to the business.

Manage

Using a risk management strategy, we collaborate with customers to establish risk tolerance and a risk register process, which are then used to prioritize and manage risks.

Supply Chain Risk Management Strategy

Priorities, constraints, risk tolerances, and assumptions used to support risk decisions associated.

Leveraging the right assessor / technical resource is critical to a successful security assessment. EITS aligns our assessors based on experience in industries and/or specific compliance requirements customers may have; for example, the needs of manufacturing customers can greatly differ from those of healthcare or financial organizations. Our team brings a combination of experience identifying and quantifying risk in addition to managing risk and solving security challenges from a customer's perspective.

EITS
Enterprise IT Security

EITS helps businesses, education and government agencies build and manage secure IT environments for a changing world. We secure what matters most: their business, their IT environment, their intellectual property and their reputation. Our holistic approach addresses the Architectural, Operational and Organizational facets of Information Security applying a proven architecture blueprint for scalable, agile, manageable IT environments, hardened to DOD-level security standards. Agencies and businesses who have suffered severe data breaches have tapped EITS to remediate their issues, and to dramatically lower the risk of future events. We are driven by our culture of Excellence and Substance: We Always Make Mission.

VOICE: (704) 900-8042 EMAIL: info@eits.com WEB: www.eits.com MAILING ADDRESS: 525 North Tryon St. Suite 1600, Charlotte, NC 28202