Compliance and Controls

CTS leverages the expanded set of security and privacy controls and gives organizations greater flexibility and agility in defending their information systems. For example, overlays provide a structured approach to help organizations tailor security control baselines and develop specialized security plans that can be applied to specific missions, business functions, environments of operation, and technologies. This specialization approach is important (1) as the number of threat-driven controls and control enhancements increases and (2) organizations develop risk management strategies to address their specific protection needs within defined risk tolerances.

Our CTS Team helps you to implement effective risk management processes that identifies, mitigates, prioritizes, and monitors an ongoing basis, risks arising from its information and information systems. Our Team provides guidance on managing information security risk at three distinct tiers: ***organizational***, ***mission/business process***, and ***information system levels***. The security controls that our Team recommends should be employed as part of a well-defined risk management process that supports your organizational information security programs.

The ultimate objective is that you and your organization can conduct day-to-day operations while accomplishing your organization's stated missions and business functions with what the OMB Circular A-130 defines as adequate security, or security commensurate with risk resulting from an unauthorized access, use, disclosure, disruption, modification, or destruction of information.

A key benefit of our consulting services is to provide you and your organization a set of guidelines for enhancing or selecting and specifying security controls for your organization and information systems to meet the requirements of the FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems. This guideline applies to all components of an information system that process, store, or transmit federal information. The guidelines have been developed to achieve more secure information systems and effective risk management within the federal government.

In addition to the security controls, we provide a set of information security program management controls, a set of privacy controls, and establish a linkage and relationship between privacy and security controls for purposes of enforcing respective privacy and security requirements which may overlap in concept and in implementation within federal information systems, programs and organizations. Standardized privacy controls provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance to those requirements. Incorporate the same concepts used in managing information security risk, helps organization implement privacy controls in a more cost-effective, risked-based manner. (The guidelines are applicable to all federal information systems other than those systems designated as national security systems as defined in 44 USC Section 3542.)

For more Information Contact:

Cyber Threat Solutions, Inc. (CTS)
info@cyberthreatsolutions.com
Phone: 571-334-1092