CYBER SOLUTIONS - COMPLIANCE SERVICES

Federal Information Security Management Act (FISMA) Assessment

SparkC's Federal Information Security Management Act (FISMA) Assessment provides knowledgeable and experienced consultants to assist federal agencies to improve their security posture and become compliant with FISMA.

Are you in compliance?

Today's complex information systems and networks are enormously beneficial for most users, but they do come with certain inherent risks. That's why proper information security is so vital to a federal agency's ability to fend off cyber criminals and protect sensitive national security information.

Federal agencies are an alluring target for hackers because these agencies transmit, process, and store vital, strategic, and confidential information that could be used for personal gain or to harm national interests. As a result of these threats, the Federal Information Security Management Act (FISMA) was created in 2002 to govern the management of information security among federal agencies. The Act requires federal agencies to secure government information and assets against natural and man-made threats.

Specific FISMA requirements are detailed in NIST Special Publication 800-37 (or NIST SP 800-37), NIST SP 800-53, and the Federal Information Processing Standards (FIPS) publications 199 and 200.

It is critical that agencies conduct a FISMA assessment to determine the risks to federal information systems and become compliant with this regulation.

SparkC provides knowledgeable and experienced consultants to assist federal agencies to improve their security posture and become compliant with FISMA.

How SparkC will ensure compliance

Our FISMA assessment service helps federal agencies to:

+ Catergorize the information to be protecetd
+ Select minimum baseline controls
+ Refine controls using a risk assessment procedures
+ Document the controls in the system security plan
+ Implement security controls in appropriate information systems
+ Assess the effectiveness of the security controls once they have been implemented
+ Determine agency-level risks to the mission or business case
+ Monitor the security controls on the continuous basis