



Information Assurance Security Through the Entire System Life Cycle

a.i. solutions

Managing a federal information security program requires a common-sense, comprehensive, impact based approach that balances risk against the mission/business need.

At **a.i. solutions**, we empower Information Security Officials and Information System Owners with strategies to implement “**near real continuous monitoring**” to support the dynamic federal environment. Our solutions focus on putting decision maker’s limited security dollars to strategies that provide true protections to federal information systems while meeting compliance requirements.



The value of the National Institute of Standards & Technology (NIST) **Risk Management Framework** can only be realized with a program that includes a continuous monitoring, security lifecycle approach. Our continuous monitoring implementations provide our customers with standardized, repeatable security impact assessments and processes. This provides the necessary metrics and organizational risk understanding needed to make value based security decisions to enable an agency to fulfill its mission. We use an **impact based approach** that starts with an understanding of the clients risk profile and business processes. This permits a tailoring of security controls based on impact that radically lowers the cost of security while improving effectiveness.

The a.i. solutions Approach

Our company has **notably low employee turnover**, allowing for long-term continuity between our team and agency managers. We value trust with our customers, and forge partnerships that are vital for effective Information Assurance programs.

Our employees are **fully versed in all federal mandates** for information assurance, including the Federal Information Security Management Act (FISMA), and the requirements of the National Institute of Standards & Technology (NIST).

At **a.i. solutions**, we take a “**common sense approach**” and have a value-added service mentality that saves customers money by solving problems in a smarter way.

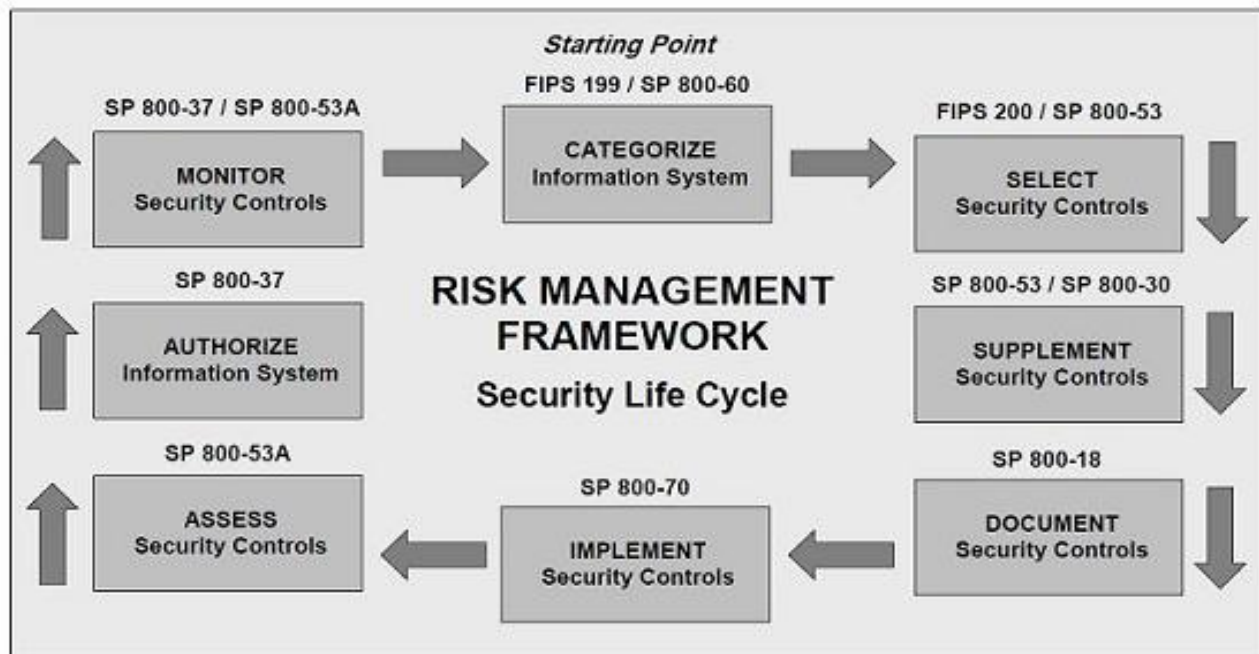
Our Information Assurance services:

- FISMA Compliance
- Security Operations
- Vulnerability Management
- Application Security Lifecycle Solutions
- Intrusion Detection and Prevention
- Forensics
- Incident Response and Recovery
- Network Security
- Security Architecture
- Risk Management
- Security Impact Assessments
- Risk Consulting Solutions
- Privacy Act Compliance
- Security Authorization (C&A)
- Business Impact Analysis
- Business Continuity
- Disaster Recovery
- Contingency Planning
- Contingency Testing, Training, and Exercising (TT&E)



a.i. solutions

Information Assurance Security Through the Entire System Life Cycle



Every agency is different, and while developing an **Information Assurance program**, we work to understand the agency mission, customer’s objectives and risk profile in order to create a customized program strategy.

The Security Lifecycle Approach is more than just a buzzword at **a.i. solutions**. Staff involvement with system development, throughout the lifecycle, ensures a **“baked in rather than bolted on”** security approach. Our team enhances the security posture by participating in the software/system development lifecycle with requirement definitions, code/design reviews, system architecture reviews and support of milestone reviews.

Key Customers:

- **NASA Headquarters**
 - NASA Headquarters Information Technology and Communications Division
 - Facilities and Administrative Support Division
- **NASA Agency**
 - NASA Office of the Chief Information Office
 - NASA Office of the Inspector General
 - NASA Office of Protective Services
 - Aeronautics Research Mission Directorate
 - Space Operations Mission Directorate
- **NASA Centers**
 - NASA Goddard Space Flight Center
 - NASA Kennedy Space Center
 - Jet Propulsion Laboratory

For more information, contact:

Jeff Nicholson, Information Assurance Manager
Mission Assurance Division
jeff.nicholson@ai-solutions.com