



Information Assurance / Certification and Accreditation

MAR has experience with all aspects of Information Assurance, and we are dedicated to supplying our customers with quality and cost-effective security solutions in both classified and unclassified environments. Our talented IT team can swiftly and thoroughly assess a system's risks and requirements, and develop security-related documentation to obtain an Authority to Operate (ATO). We use and maintain an internal MAR Wiki site that stores our Knowledge Management system, allowing us to generate these documents quickly and ensure their consistency and accuracy. Our dynamic team of security experts is intimately familiar with the demands and specifications of Government regulations, and work closely with our customers to make certain that their systems are secure and in compliance with all regulatory standards..

We provide Certification and Accreditation (C&A) support, employing a value-added process that maximizes quality and minimizes complexity, reducing labor and time requirements for completing a certification package for each system.

MAR security specialists make use of effective data gathering tools (custom interview checklists, questionnaires, templates, etc.) followed by analysis for applicability across multiple systems, platforms, and locations. Data and analysis is documented and retained to provide reference for information re-use, re-certification, or audit/inspection.

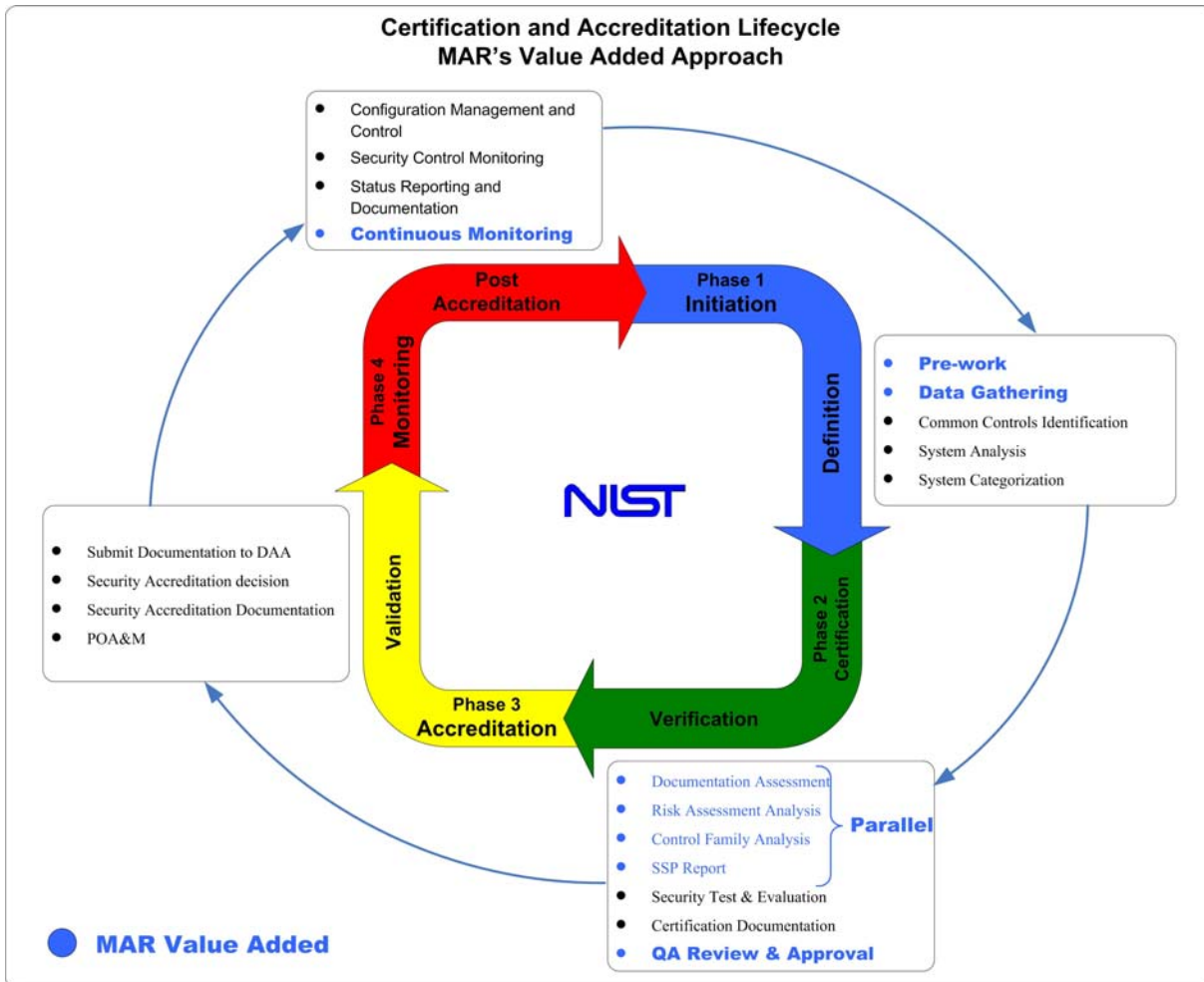


MAR C&A Wiki Site

Threat sources (human, environmental, and natural) and vulnerabilities are identified, and their impact and likelihood are assessed in order to gauge risk to the information system. Security control compliance analysis is assessed as well. Any threats identified during vulnerability testing are documented in the Risk Assessment. As Risk Assessment findings are completed, they are documented in the appropriate template. MAR's C&A process also ensures that observations entered into the Risk Assessment will include the level of detail needed to expedite the completion of a System Security Plan (SSP).

Security controls considered "Not in Place" or "Planned" are included in a Plan of Actions and Milestones (POA&M). Updates to the POA&M template is a continuous process throughout the Certification & Accreditation lifecycle.

For civilian agencies MAR security specialists design security control tests for the Security Control Assessment Plan based on NIST SP 800-53A guidance, tailored where applicable to the specific system or control being tested. MAR test designs will be analyzed for applicability across multiple systems, environments, and locations. In addition, custom test scripts and testing tools (such as DISA Gold Disk, Nessus, or CORE IMPACT) are also maintained and updated for reuse.



Continuous monitoring is important to the post-accreditation security of the information system. Our security control compliance analysis will ensure that policy and procedures are in place for: security monitoring and status reporting, risk analysis integrated with configuration management review; updates to documentation; and, re-certification. The re-certification level of effort can be greatly reduced through careful documentation and continuous monitoring processes.



Information Assurance / Certification and Accreditation

To provide additional visibility into our process, MAR utilizes Earned Value Management (EVM) tracking to capture metrics for each phase of C&A. Data gathered from our EVM metrics are used to continuously improve our internal processes and offer recommendations to our customers for improvements to their security programs.

Examples of our past performances include:

US Nuclear Regulatory Commission (NRC)



The NRC awarded MAR a contract to assist with the certification and accreditation (C&A) process under their Consolidated Information System Security Services program, which will integrate the current ISS program with the ISS Capital Planning and Investment Control (CPIC) to ensure fiscally responsible IT investment management. The scope of the contract covers twenty six functional areas including Program Management, Integrated Project Planning and EVM reporting to support the full range of information security services. We are collaborating closely with NRC system owners to provide centralized security support services to guarantee the system's compliance with FISMA, FEA, OMB M-04-04, NIST 800 Series, and other C&A requirements. Our capable technical staff is using proven, functional methods of production that are both expeditious and cost-saving to develop an Authority to Operate (ATO) package that includes Security Categorizations, Risk Assessments, ST&E Plans and Executions, and other security related documentation.

Office of the Director of National Intelligence (ODNI)



MAR's experts provide IT security/engineering support to the US Government Office of the Director of National Intelligence (ODNI). In the role of Information System Security Manager (ISSM), MAR is responsible for implementing and enforcing information security policy and guidance, building and managing the Information System Security Officer (ISSO) team, and working with the customer's Lead Certifier to determine the certification and accreditation (C&A) process. In support of this, our staff directs the development of security standard operating procedures and standard C&A body of evidence documentation, prioritizes systems for C&A, coordinates certification testing with the Lead Certifier, and submits C&A body of evidence to the DNI Designated Accrediting Authority (DAA).

MAR staff has also represented our customer on a senior government team in support of the DNI CIO's C&A revitalization effort, helping to develop a new C&A process for the US Government. Additionally, we helped develop the organization and process to be followed for all internal ODNI C&A activities. MAR personnel further represented our customer at DNI CIO ISSM and IA monthly meetings, IC Audit Working Group, and the C&A Roundtable at the Security Solutions 2006 Conference in Tampa, FL.