



# Information and Security Assurance through Certification and Accreditation Initiatives

**Argosy Omnimedia, Inc.**

**Version 1.0**

07/26/2005

Document Number: A001701

Argosy Omnimedia, Inc  
6110 Executive Blvd., Suite 1065  
Rockville, MD 20852  
<http://www.argoc.com>

For more information contact:

Rob Montgomery  
301.816.9373 x17  
[rob.montgomery@argoc.com](mailto:rob.montgomery@argoc.com)

## Table of Content:

Information Assurance.....	3
Policy & Regulatory Compliance: .....	3
Certifications and Accreditation (C&A):.....	3
Technology Implementation & Integration: .....	3
Infrastructure Security: .....	3
Vulnerability Assessment: .....	3
Penetration Testing: .....	3
Security Program Development:.....	4
Security Training and Awareness: .....	4
Risk Assessment: .....	4
Certification and Accreditation in more detail.....	4
Methodology details and overview.....	4
Initiation Phase.....	5
Security Certification Phase.....	5
Security Accreditation Phase .....	5
Continuous Monitoring Phase.....	5
DITSCAP .....	6
Certification and Accreditation Support Overview .....	6
Definition .....	6
Verification .....	6
Validation.....	6
Post Accreditation.....	7
Technical Solutions for Security Risk Assessment .....	7
C&A Process Standard Operating Procedures (SOP).....	7
For More Information .....	9

## Information Assurance

Argosy has solid experience tailoring Information Security solutions to the federal and commercial customer. We provide the following Information and Security Assurance services to the public sector and the government:

### Policy & Regulatory Compliance:

Our Policy and Regulatory Compliance service can help you meet your regulatory requirement as well. We can assist you in meeting DITSCAP, HIPAA, ISO17799, FISMA, Sarbanes-Oxley, OMB, NIST, and other regulations.

### Certifications and Accreditation (C&A):

Our service activities can include any of the following:

- Developing & Conducting a security test and evaluation (ST&E) plan and test procedures
- Analyzing and reporting test results
- Developing and/or conducting a vulnerability assessment and developing a final vulnerability assessment report
- Conducting a risk assessment
- Developing a System Security Plan (SSP)
- Developing Continuity of Operations, Business Continuity / Disaster Recovery Plans
- Developing the certification and accreditation package

### Technology Implementation & Integration:

Our expertise in security technologies and our unbiased approach to technology selection, assures that your security technology investments provides the highest return on security investment at the same time that your valuable business assets are protected.

This service includes hands-on third-party systems selection, testing, integration, configuration, and installation. Some of the technologies that we have successfully deployed include: firewall, intrusion

detection systems (IDS), virtual private networks (VPN), public key infrastructure (PKI), encryption, strong authentication, content filtering, log consolidation, and other emerging technologies.

### Infrastructure Security:

Our consultants will review existing security controls in order to leverage existing strategies, recommend, and implement solutions by providing security in these areas:

- Network Immunization: Secure network design and architecture
- System Hardening: Secure operating system installation and configuration
- Secure Configuration and Deployment: Security Appliances, firewalls, VPNs, IDS/IPS, Anti-virus solutions
- Infrastructure Maintenance: Operational support

### Vulnerability Assessment:

Our vulnerability assessment service provides a thorough, hands-on security assessment to ensure that the security of your network and system is appropriate to your business and operational needs. The vulnerability assessment report includes analysis of findings along with a detailed action plan for improving your systems' and network's overall security posture.

### Penetration Testing:

Our consultants utilize the same tools and techniques used by hackers to identify and validate security vulnerabilities of your environment. We systematically analyze this data to determine the level of risk associated with these vulnerabilities and provide prioritized recommendations to help you mitigate risk to achieve your information security objectives. Argosy's penetration testing methodology will result in minimal or no impact on your network, systems, or business productivity.

### **Security Program Development:**

Argosy can assist you in developing and maintaining an organization-wide security program. With our Security Program Development service, we provide:

- Security Policy Development

Argosy can work with you to establish security processes that support business goals and objectives

- Incident Response:

We can assist you in the creation, implementation, and rollout of your incident response capability. We help you create policies and processes to ensure that security incidents are resolved effectively within the least amount of time.

### **Security Training and Awareness:**

Argosy can present training materials tailored towards specific audiences such as software developers, help-desk support, operations personnel, general staff and management. Our training can cover any security topics such as emails, passwords, viruses, computer misuse, and other security policy issues of importance to your organization.

### **Risk Assessment:**

Our risk assessment service enables your organization to estimate your security posture related to your business and information system infrastructure. We help you meet regulatory requirements that may require scheduled risk assessments to ensure that your organization remains compliant.

### **Certification and Accreditation in more detail**

Certification and Accreditation (C&A) is the enterprise-wide analysis of the technical and non-technical security governance, controls and security readiness of the IT infrastructure (assets). The deliverable from this analysis is a report detailing how well the assets comply with the applicable requirements, regulations and acceptable level of risk.

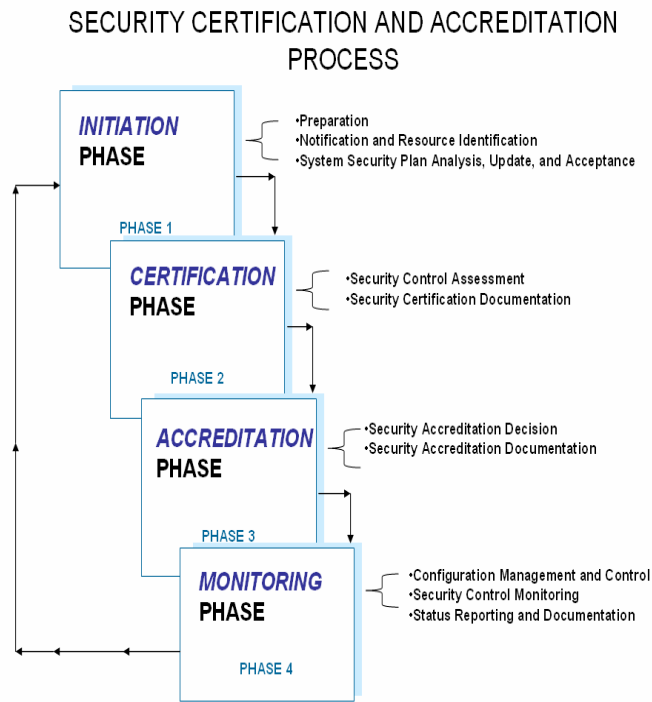
### **Methodology details and overview**

Argosy's methodology provides our clients with state-of-the-art/practice, low risk and cost effective approach to IT/IS Certification and Accreditation. Argosy's staff has the capabilities to assist you with all phases of your certification and accreditation efforts to comply with all DoD and any other government regulations and guidance. Argosy can provide C&A program planning, life cycle implementation, and compliance assessment support. The process of supporting a certification and accreditation project requires the coordination of many departments and other entities. If properly planned and performed, a C&A effort can result in a well-executed efficient project.

Argosy's methodology is in direct correlation with industry best practice and consistent with the National Institute of Standards and Technology (NIST) security certification and accreditation process guidance, (NIST Special Publication 800-37-Guide for the Security Certification and Accreditation of Federal Information Systems), which consists of the following distinct phases:

- Initiation Phase;
- Security Certification Phase;
- Security Accreditation Phase; and
- Continuous Monitoring Phase.

Exhibit-1 below provides a high-level view of the security certification and accreditation process including the tasks associated with each phase in the process:



**EXHIBIT 1 SECURITY CERTIFICATION AND ACCREDITATION PROCESS**

**Initiation Phase**

The Initiation Phase consists of three tasks: (i) preparation; (ii) notification and resource identification; and (iii) system security plan analysis, update, and acceptance. The purpose of this phase is to ensure that the authorizing official and senior agency information security officer are in agreement with the contents of the system security plan, including the system’s documented security requirements, before the certification agent begins the assessment of the security controls in the information system.

**Security Certification Phase**

The Security Certification Phase consists of two tasks: (i) security control assessment; and (ii) security certification documentation. The purpose of this phase is to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the

desired outcome with respect to meeting the security requirements for the system. This phase also addresses specific actions taken or planned to correct deficiencies in the security controls and to reduce or eliminate known vulnerabilities in the information system. Upon successful completion of this phase, the authorizing official will have the information needed from the security certification to determine the risk to agency operations, agency assets, or individuals—and thus, will be able to render an appropriate security accreditation decision for the information system.

**Security Accreditation Phase**

The Security Accreditation Phase consists of two tasks: (i) security accreditation decision; and (ii) security accreditation documentation. The purpose of this phase is to determine if the remaining known vulnerabilities in the information system (after the implementation of an agreed-upon set of security controls) pose an acceptable level of risk to agency operations, agency assets, or individuals. Upon successful completion of this phase, the information system owner will have: (i) authorization to operate the information system; (ii) an interim authorization to operate the information system under specific terms and conditions; or (iii) denial of authorization to operate the information system.

**Continuous Monitoring Phase**

The Continuous Monitoring Phase consists of three tasks: (i) configuration management and control; (ii) security control monitoring; and (iii) status reporting and documentation. The purpose of this phase is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the authorizing official when changes occur that may impact on the security of the system. The activities in this phase are performed continuously throughout the life cycle of the information system.

Completing a security accreditation ensures that an information system will be operated with appropriate management review, that there is ongoing monitoring

of security controls, and that reaccreditation occurs periodically in accordance with federal or agency policy and whenever there is a significant change to the system or its operational environment.

## **DITSCAP**

DITSCAP establishes a standard DoD-wide process to certify that a target Information System (IS) is safe to operate in its fielded environment and will maintain that posture throughout the system lifecycle. There are four phases: Definition, Verification, Validation, and Post Accreditation. Argosy has produced all the documentation required for the definition phase including the System Security Authorization Agreement (SSAA) and all its appendixes. These documents have in some cases been generated from scratch and in other cases updated to reflect changes to the system over time. Argosy has worked with the clients to identify and analyze vulnerabilities and verify that the security controls are in place. Argosy has conducted tests to validate that the system's security goals have been met and provided evidence to the DAA to assist in approving systems to operate in the DoD environment. We continue to work with our clients in monitoring changes to the environment to ensure that the security of the system is preserved and help conduct periodic compliance audits of both security management and configuration management. We are available to our clients to answer system security related questions.

### **Certification and Accreditation Support Overview**

Argosy understands that you are committed to upholding the highest standards of Information Assurance to protect and maintain the confidentiality of your IT information, as well as the defense of your information systems. In doing so, we will ensure that all Automated Information Systems (AISs) and Networks are in compliance with all needed policies, guidance, and standards.

Argosy will assist you and your mission to ensure the integrity, availability, confidentiality, non-repudiation

and authentication of all information technology automated information systems (AISs).

Argosy will perform certifications and accreditations of all your centrally managed AISs and networks; communicates security related IA issues or items of interest affecting the enterprise; and tests, verify and assures adequate security controls exist within the IT systems supporting your systems.

A typical Argosy Certification and Accreditation engagement may also include one or all of the following *facets*:

#### **Definition**

This effort defines the C&A level of effort, identifies the Designated Approving Authority (DAA) and the Certification Authority CA, and culminates with an agreement, by the program manager, the DAA, the CA, and the user representative, on the method for implementing the security requirements. That agreement is documented and describes the system mission, target environment, target architecture, security requirements, and applicable data access policies. The agreement describes the applicable set of planning and certification actions, resources, and documentation required for the C&A. The agreement is the vehicle that guides the implementation of requirements and the resulting C&A actions.

#### **Verification**

The objective of the verification effort is to verify the evolving system's compliance with the requirements agreed on in the agreement. This phase consists of activities that occur between the signing of the initial version of the agreement and the formal C&A of the system, such as continuing refinement of the agreement, system development or modification, certification analysis, and analysis of the certification results.

#### **Validation**

The objective of this step is to validate that the preceding work has produced an information system that operates in a specified computing environment with an acceptable level of residual risk. This phase

consists of process activities that occur after the system is integrated and culminates in the accreditation of the IT system, such as a review of the agreement, or an evaluation of the integrated IT system, certification, and accreditation.

### **Post Accreditation**

This phase contains process activities necessary to continue to operate and manage the system so that it will maintain an acceptable level of residual risk. Post-accreditation process activities include ongoing maintenance of the agreement, system operations, change management, and compliance validation.

### **Technical Solutions for Security Risk Assessment**

Risk assessment is the process of analyzing threats to, and vulnerabilities of, an AIS and network and the potential impact that the loss of information or capabilities of a system would have on national security. It appraises the operation of the system to determine if risks are being contained or reduced to an acceptable level. The resulting analysis is used as a basis for identifying appropriate and cost-effective security countermeasures.

Assessing risk is an ongoing activity, which ensures that new threats and vulnerabilities are identified and that appropriate security countermeasures are implemented. Methods should include a consideration of the major factors in risk management: the value of the AIS and network or application, threats, vulnerabilities, and the effectiveness of current and proposed safeguards.

Argosy has experience working with *RiskWatch* risk assessment management tools (some of which are designed specifically for the Healthcare enterprise). Riskwatch tools provides security risk assessment and compliance software that automates the risk management and site survey process for information systems, physical, facilities security, and the HIPAA Final Security Rule.

### **C&A Process Standard Operating Procedures (SOP)**

Argosy C&A steps define a process (Exhibit 2- Sop Certification and Accreditation Process Flow) that standardizes all activities leading to a successful accreditation. The principal purpose of that process is to protect and secure the entities comprising your information infrastructure. Standardizing the process will minimize risks associated with nonstandard security implementations across shared infrastructure and end systems. Argosy's process applies to all systems requiring C&A throughout their life-cycle. It is designed to be adaptable to any type of IT system and any computing environment and mission. It may be adapted to include existing system certifications, evaluated products, use new security technology or programs, and adjust to the applicable standards.

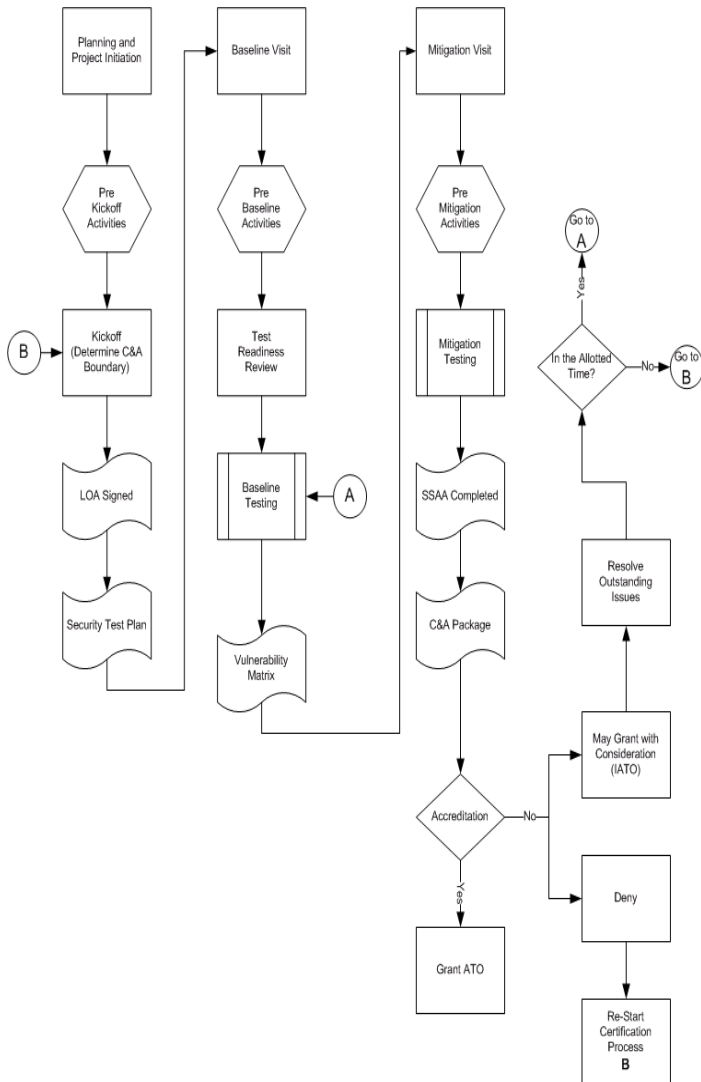


EXHIBIT-2 SOP CERTIFICATION AND ACCREDITATION PROCESS FLOW

## For More Information

*For more information contact:*

*Rob Montgomery*

*301.816.9373 x17*

[rob.montgomery@argoc.com](mailto:rob.montgomery@argoc.com)

