











Assessment and Authorization (A&A) is required by the Federal Information Security Management Act (FISMA) of 2002, which requires that all Information Technology (IT) systems and applications supporting Federal agencies must go through a formal A&A, also known as Certification and Accreditation (C&A) process before being put into production and use.

System Authorizations require time, energy, and money to manage:

System Security Plan



Security Assessment Report

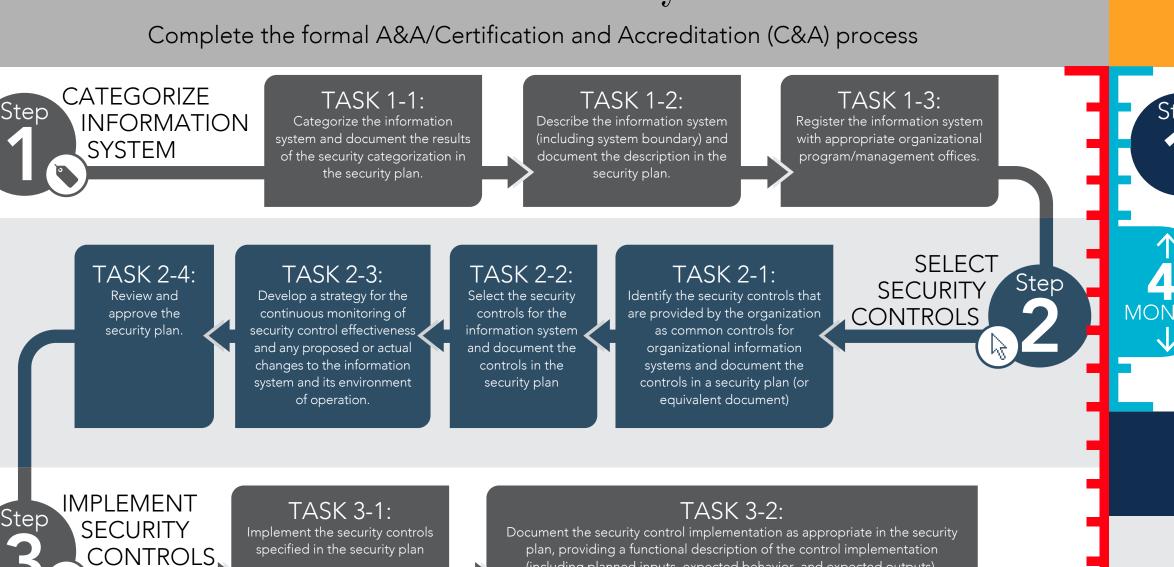


POA&Ms (Plan of Action and Milestones)



There are 2 ways to achieve A&A

"The Hard Way"



TASK 4-2:

Assess the security

controls in accordance

with the assessment

the security

assessment plan

TASK 6-2:

Assess the technical,

management, and

operational security

controls employed within

and inherited by the

information system in

accordance with the

organization-defined monitoring strategy.

TASK 6-6

Review the reported security status of the information

employed within and inherited by the system) on an

ongoing basis in accordance with the monitoring

strategy to determine whether the risk to organizationa

operations, organizational assets, individuals, other

organizations, or the Nation remains acceptable.

system (including the effectiveness of security controls

TASK 5-2:

Assemble the

ecurity authorization

the package to the

(including planned inputs, expected behavior, and expected outputs).

TASK 4-1:

Develop, review,

and approve a plan

to assess the

security controls

TASK 5-3:

Determine the risk to

organizational operations

functions, image, or

organizations, or the Nation

TASK 6-1:

Determine the

security impact of

changes to the

information system and its environment

of operation.

proposed or actual

ASSESS

MONTHS

SECURITY

CONTROLS

TASK 5-4:

Determine if the risk

to organizational

organizational assets

MONITOR

CONTROLS

TASK 6-7:

system disposal strategy,

when needed, which

executes required actions

removed from service.

SECURITY Step

"The Easy Way"

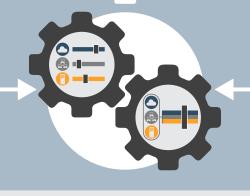
Leverage a FedRAMP System

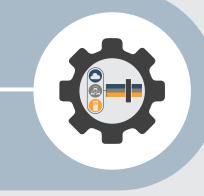
The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "DO ONCE, USE MANY TIMES" framework that saves an estimated 30-40% of government costs, as well as both time and staff required to conduct redundant agency security assessments.

How?

Streamline assessment by leveraging authorized system security plans and their:







System Specific Controls

Hybrid Controls

Benefits

Common Controls



Increase re-use of existing security assessments across agencies



Save significant cost, time, and resources



Improve real-time security visibility



Provide a uniform approach to risk-based management



Enhance transparency between government and Cloud Service Providers (CSPs)



Improve the trustworthiness, reliability, consistency, and quality of the Federal security authorization process

per year in cost avoidance as a result of FedRAMP authorization re-use

DO ONCE,

USE MANY TIMES



TASK 4-4:

Conduct initial remediation

actions on security controls

based on the findings and

control(s), as appropriate

INFORMATION

TASK 6-4:

Update the security

plan, security

monitoring process.

TASK 6-5:

system (including the effectiveness of

security controls employed within and

inherited by the system) to the authorizing

official and other appropriate organizational

officials on an ongoing basis in accordance

with the monitoring strategy

Report the security status of the information

AUTHORIZE

SYSTEM

TASK 4-3:

Prepare the security

assessment report

documenting the

from the security

TASK 5-1:

Prepare the plan of

action and milestones

based on the findings

TASK 6-3:

Conduct remediation

actions based on the

monitoring activities,

assessment of risk, and

outstanding items in the

plan of action and



1901 Group's In³Sight™ Platform has received FedRAMP Moderate authorization from the U.S. Government that enables the confidence in security for Federal agencies to trustingly utilize monitoring and managed services. This certifies that 1901 Group has passed the Federal Risk Management Process defining standards as a cloud service provider.

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

By leveraging 1901 Group's FedRAMP authorized product (In³Sight™), we were able to concisely map IT security controls to NIST standards which expedited issuance of an essential Authority To Operate (ATO) resulting in substantial time savings and cost savings.

- FEDERAL AGENCY PROGRAM MANAGER