ASSESSMENT & AUTHORIZATION

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:
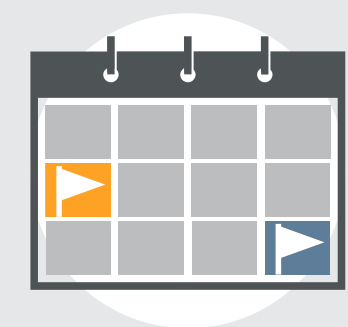
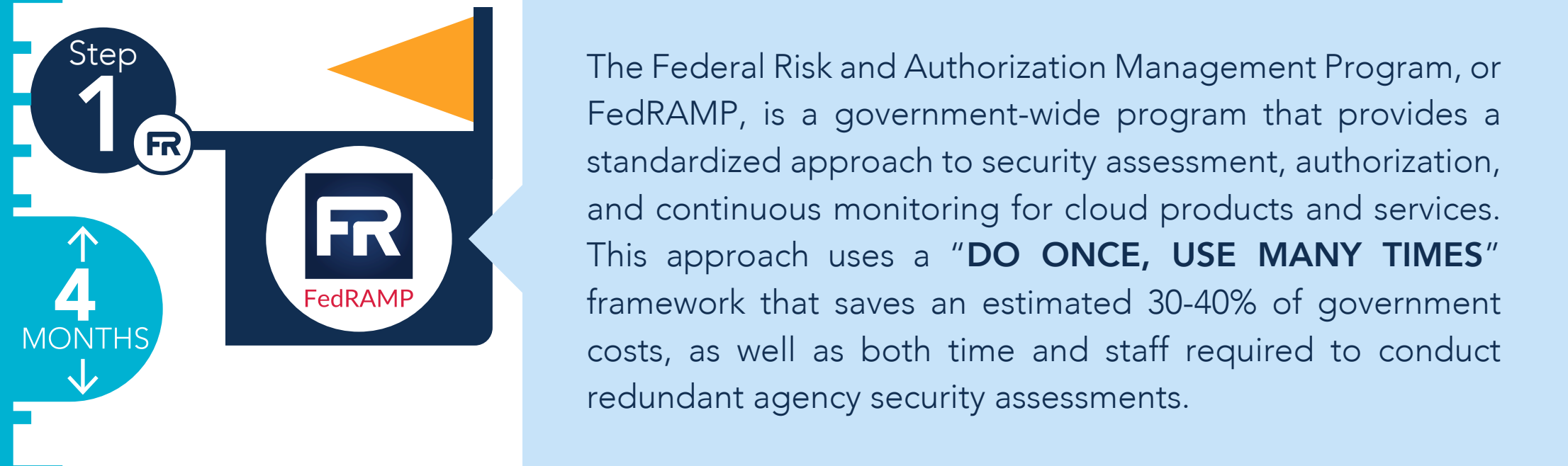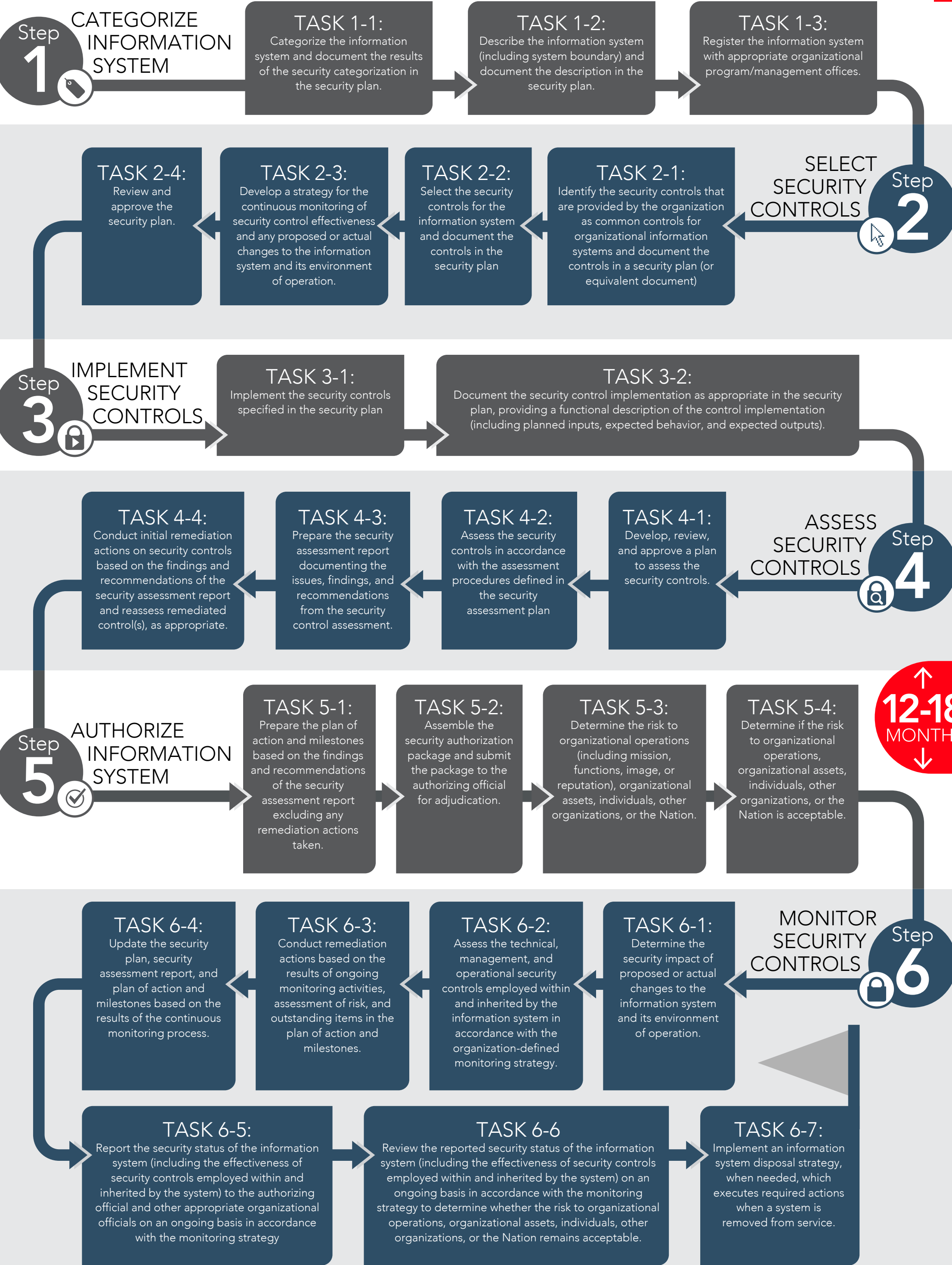| System Security Plan	Security Assessment Report	POA&Ms (Plan of Action and Milestones)

There are 2 ways to achieve A&A

"The Hard Way"
Complete the formal A&A/Certification and Accreditation (C&A) process

Step 1 — CATEGORIZE INFORMATION SYSTEM

TASK 1-1: Categorize the information system and document the results of the security categorization in the security plan.

TASK 1-2: Describe the information system (including system boundary) and document the description in the security plan.

TASK 1-3: Register the information system with appropriate organizational program/management offices.

Step 2 — SELECT SECURITY CONTROLS

TASK 2-1: Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document)

TASK 2-2: Select the security controls for the information system and document the controls in the security plan

TASK 2-3: Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation.

TASK 2-4: Review and approve the security plan.

Step 3 — IMPLEMENT SECURITY CONTROLS

TASK 3-1: Implement the security controls specified in the security plan

TASK 3-2: Document the security control implementation as appropriate in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).

Step 4 — ASSESS SECURITY CONTROLS

TASK 4-1: Develop, review, and approve a plan to assess the security controls

TASK 4-2: Assess the security controls in accordance with the assessment procedures defined in the security assessment plan

TASK 4-3: Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.

TASK 4-4: Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.

Step 5 — AUTHORIZE INFORMATION SYSTEM

TASK 5-1: Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.

TASK 5-2: Assemble the security authorization package and submit the package to the authorizing official for adjudication.

TASK 5-3: Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.

TASK 5-4: Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.

12-18 MONTHS

Step 6 — MONITOR SECURITY CONTROLS

TASK 6-1: Determine the security impact of proposed or actual changes to the information system and its environment of operation.

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 6-3: Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the plan of action and milestones.

TASK 6-4: Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.

TASK 6-5: Report the security status of the information 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.

TASK 6-6: Review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.

TASK 6-7: Implement an information system disposal strategy, when needed, which executes required actions when a system is removed from service.

1901 group + FedRAMP

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.

"The Easy Way"
Leverage a FedRAMP System

Step 1 — FedRAMP — 4 MONTHS

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:

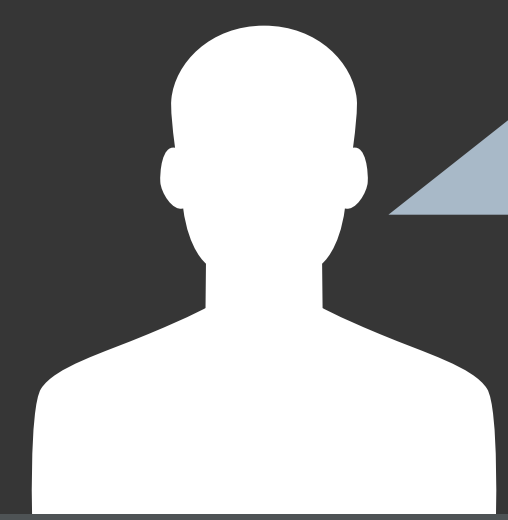| System Specific Controls	Hybrid Controls	Common Controls

Benefits

- 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

DO ONCE, USE MANY TIMES

$70 MILLION per year in cost avoidance as a result of FedRAMP authorization re-use

> 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

SOURCES:
- www.fedramp.gov
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf