# DEFENSE SECURITY SERVICE (DSS) ASSESSMENT AND AUTHORIZATION PROCESS MANUAL (DAAPM) AUTOMATION

**Ignyte Assurance Platform: Operationalizes every step of the DSS DAAPM workflow to assist cleared contractors on obtaining their ATO faster**

## OVERVIEW

The U.S. government's policy requires safeguards for assuring the confidentiality, availability, and integrity of classified information required by a contract. The Defense Security Service (DSS) Assessment and Authorization Process Manual (DAAPM) is designed to be used by cleared contractors participating in the National Industrial Security Program. Federal agencies like intelligence communities, DoD, and Special Access Programs (SAP) are adhering to the Assessment and Autorotation (A&A) by adopting common guidelines.

DAAPM transitions DSS A&A processes to the Risk Management Framework (RMF) availed to cleared contractors by DoD 5220.22, National Industrial Security Program Operating Manual (NISPOM). NIPSOM is responsible for recommending restrictions, requirements, and security measures for preventing unauthorized disclosure of confidential information. NIPSON authorizes U.S. Government Executive Branch Departments and Agencies to disclose data to their contractors. DAAPM uses NIST 800-37, Risk Management Framework for Information Systems and Organizations, and NIST SP 800-53, version 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations, to implement RMF processes.

RMF has more focus on holistic strategic processes for managing system risks and on procedures meant for developing trust across the Federal government. Implementing RMF has benefits like structured, disciplined, repeatable, and flexible processes in managing risks impacting system operations. Cleared contractors with access to classified information under DSS must follow DAAPM guidelines to implement RMF and obtain ATO. Ignyte Assurance Platform allows cleared contractors to automate RMF processes and to acquire ATO through the DSS.

## OUR SOLUTION

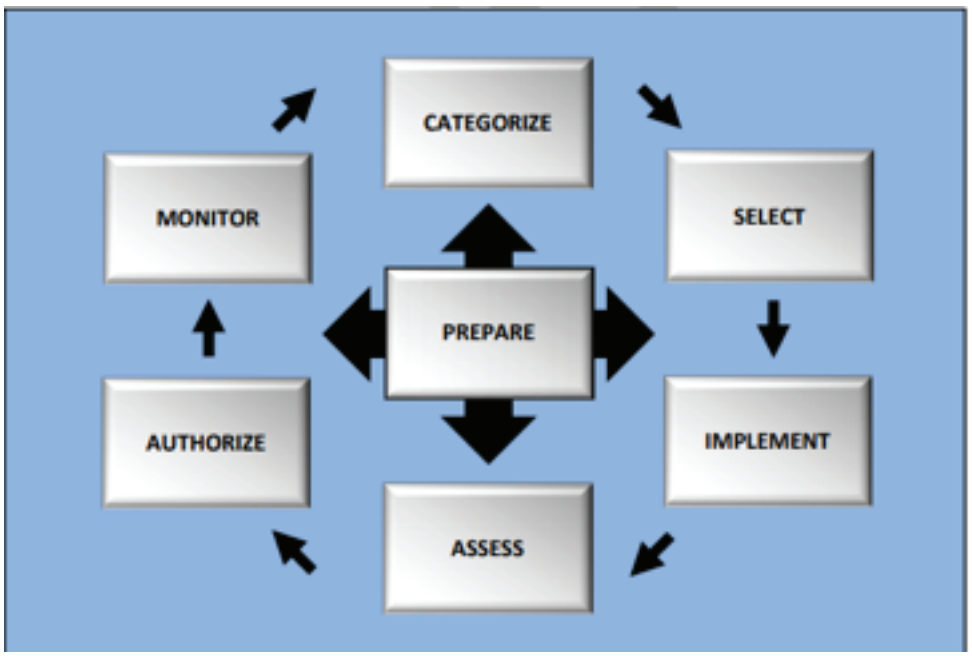
Ignyte Assurance Platform ensures DSS, DAAPM, and NISPOM compliance through automated analysis capabilities that allow it to automatically map RMF regulations to the control sets.

The solution is meant for:

- DoD contractors and subcontractors
- Companies handling classified information

Also, the Ignyte Assurance Platform enables businesses to focus on the nine risk management steps stipulated in the NIST 800-300 publication. This not only enables organizations to create adequate risk management strategies, but it also assists them to comply with all the necessary regulatory compliance needs. The steps are as highlighted below:

- System Categorization
- Select Applicable Security
- Controls
- Implement Controls
- Assess Controls
- Authorize
- Continuous Monitoring




The platform automates RMF workflow end to end in the above six steps allowing organizations to fully complete risk assessment processes. The platform automates documentation (System Security Plan, Plan of Action & Milestones, Security Assessment Report) needed for ATO for DSS/DAAPM system.

## OUR APPROACH

Ignyte engineers have vast experience handling Federal space containing complex regulations, standards like NIST SP 800-30, NIST 800-60 and NIST 800-53 to adhere to, and networks. This knowledge ensures your business complies with complex regulations. Our process observes NIST 800-30 (Guide for Conducting Risk Assessments), NIST 800-60 (Guide for Mapping Type of Information and Information Systems to Security Categories) and NIST 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations).

Our approach entails:

i. **Prepare:** This was added in NIST SP 800-37 Rev 2 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. It involves preparing an organization to manage risks through conducting critical activities at organization, mission, information systems, and business process levels.
ii. **System categorization:** This step informs processes for managing organizational risks by identifying adverse impacts to organizational operations, assets and other organizations to preserve confidentiality, availability, and integrity of information processes and organizational systems. This ensures system categorization based on business and mission objectives of the organization. Ignyte Assurance Platform has inbuilt 800-60 for registering system/application such that it populates security controls during control operator categorization.
iii. **Selecting security/privacy controls:** This stage involves documenting the necessary controls for securing information systems commensurate with organizational operations and assets, other organizations, and individuals. Allocating security and privacy requirements to environments in which the system operates determines system-specific controls, common, and hybrid during the control selection process. The platform automates the process and allows custom tailoring of the controls.
iv. **Implement security/privacy controls:** This step involves implementing and documenting organizational security and privacy controls in baseline configuration and details specific to control implementation. Control implementation is consistent with organizational enterprise architecture and related security and privacy architectures. They serve as a resource for guiding control allocation to system or system components.
v. **Assess security/privacy controls:** This involves determining if selected controls are implemented correctly and operate as intended, producing desired outcomes concerning organization system privacy and security requirements.
vi. **Authorize:** This ensures organizational accountability through requiring senior executives to determine acceptability of supply chain, privacy, and security to assets and operations, other organizations depending on the system operation, and common controls. Authorization packages include security plans, reports for assessing privacy and security, action plans and milestones, executive summaries which Ignyte Assurance Platform automate for documenting required ATO. Organizations maintain change control depending on the update of the authorization package. Providing timely updates to plans, assessment reports, and action plans and milestones continually supports near real-time risk management concepts, and it can be used to reauthorize if needed.
vii. **Continuous monitoring:** Maintains ongoing situational awareness regarding information systems and organizational security and privacy posture to support risk management decisions.

Ignyte firmly believes that meeting complex regulatory and industry standards is a continuous process. The process requires a business to allocate financial and human resources to ensure that it is always compliant in an environment where new security requirements emerge every day. As such, Ignyte provides security-centric guidance to ensure our clients access advanced security. This saves the need for investing in expensive cybersecurity teams and internal controls. We guide your organization in continuous assessments, risk monitoring, and security improvement processes.

## OUR BENEFITS

- **Reduced compliance burdens:** Ignyte Compliance Management and Oversight model provides powerful workflow features and integrates all platform modules and third-party applications. This is to automate processes related to compliance.
- **Executive Insight:** Ignyte provides real-time dashboards and reports designed to provide compliance insights at the executive level. They consist of granular metrics for compliance and audit professionals. We also provide resources for NIST compliance requirements to guide you during the compliance process.
- **Track Ongoing Compliance:** We mitigate all risks and potential compliance violations within your organization. Changes in your organization's internal environment will trigger alerts ensuring you are up to date with ongoing compliance
- **Tailored solution:** Our approach is independent of any vendors allowing us to offer our customers in-depth services and recommendations customized to ensure you achieve the desired ROI.

## WHY IGNYTE?

Are you a business struggling to develop an effective risk management strategy/program? Ignyte professionals have the necessary expertise needed to prepare your enterprise to prevent security incidents. We provide solutions where your business faces contract termination or stop work order due to noncompliance. Contact our experts for free compliance consultations

### Get Started Now!

Give us a call to setup a demo today at https://ignyteplatform.com/request-a-demo/

REQUEST A DEMO

### ABOUT IGNYTE ASSURANCE PLATFORM

Ignyte Assurance Platform™ is a leader in collaborative security and integrated GRC solutions for global corporations. For corporate risk and compliance officers who depend heavily on the protection of their resources, Ignyte is the ultimate translation engine for simplifying compliance across regulations, standards and guidelines. The Ignyte platform is used by leading corporations in diverse industries; such as, Healthcare, Defense, and Technology. Ignyte is headquartered in Miamisburg, Ohio and can be reached at **www.ignyteplatform.com**. PH: **1.833.IGNYTE1 or (937) 789-4216**