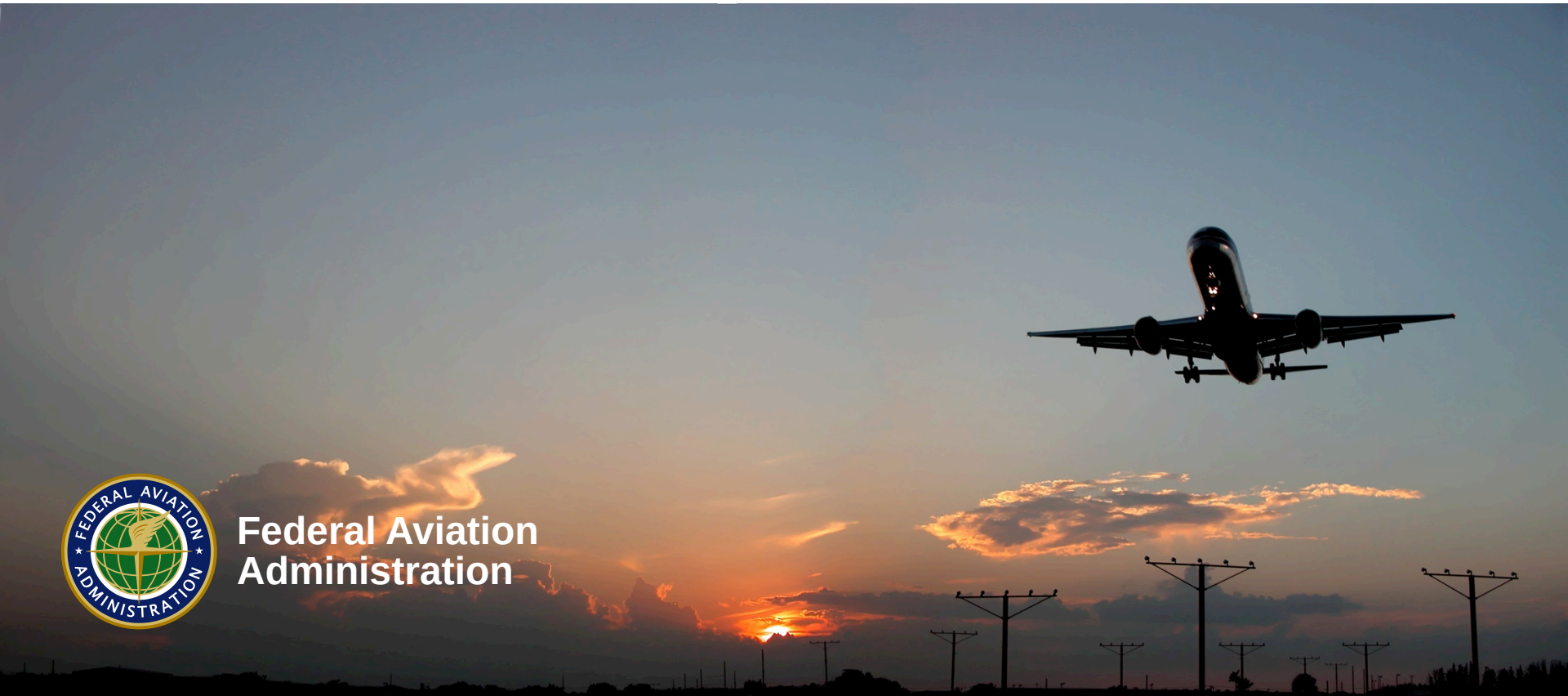
2020 FAA Cybersecurity Awareness Symposium

Securing the Aviation Ecosystem | "Cyber Hygiene"

Program Control and Governance (PC&G): Information Assurance

Date: October 20, 2020



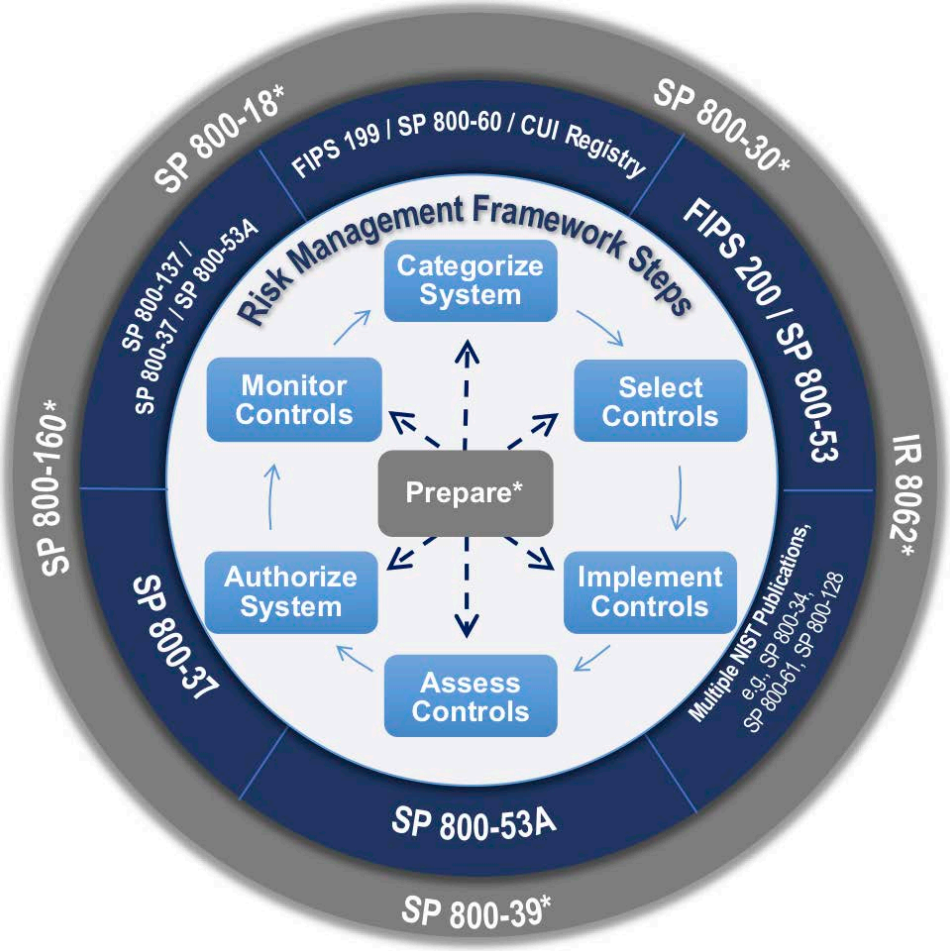
What is Authorization?

- **Per National Institute of Standards and Technology (NIST) 800-37 R2 (Appendix F, p 139):**

"Authorization is the process by which a senior management official, the authorizing official, reviews security and privacy information describing the current security and privacy posture of information systems or common controls that are inherited by systems. The authorizing official uses this information to determine if the mission/business risk of operating a system or providing common controls is acceptable – and if it is, explicitly accepts the risk."

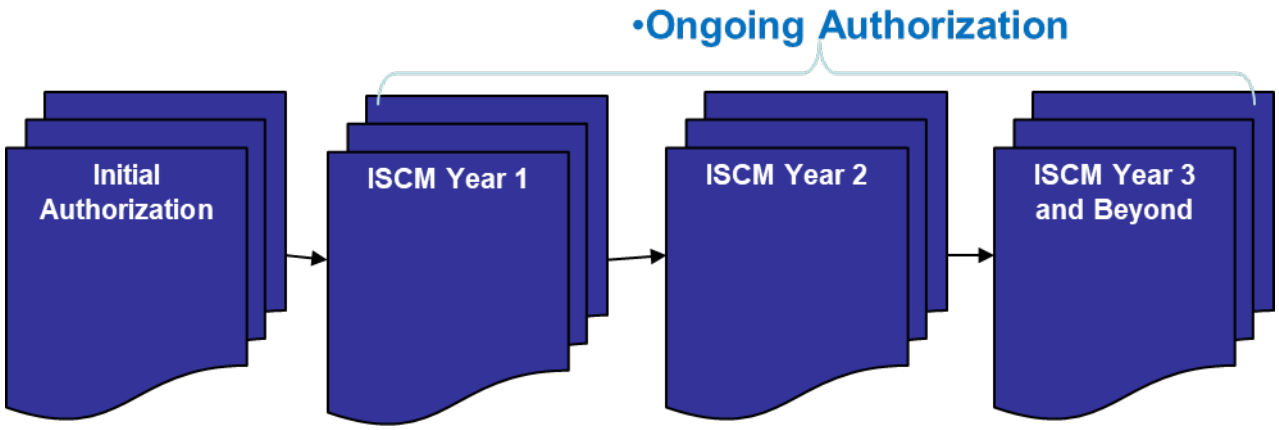
NIST Risk Management Framework (RMF)

- **The Air Traffic Organization (ATO) Authorization Process follows the NIST RMF**
- **Steps 1 – 5 are performed to establish the <u>Initial</u> system Authorization to Operate**
- **Step 6 (Monitor Controls) is performed to maintain <u>Ongoing</u> Authorization via Information Security Continuous Monitoring**

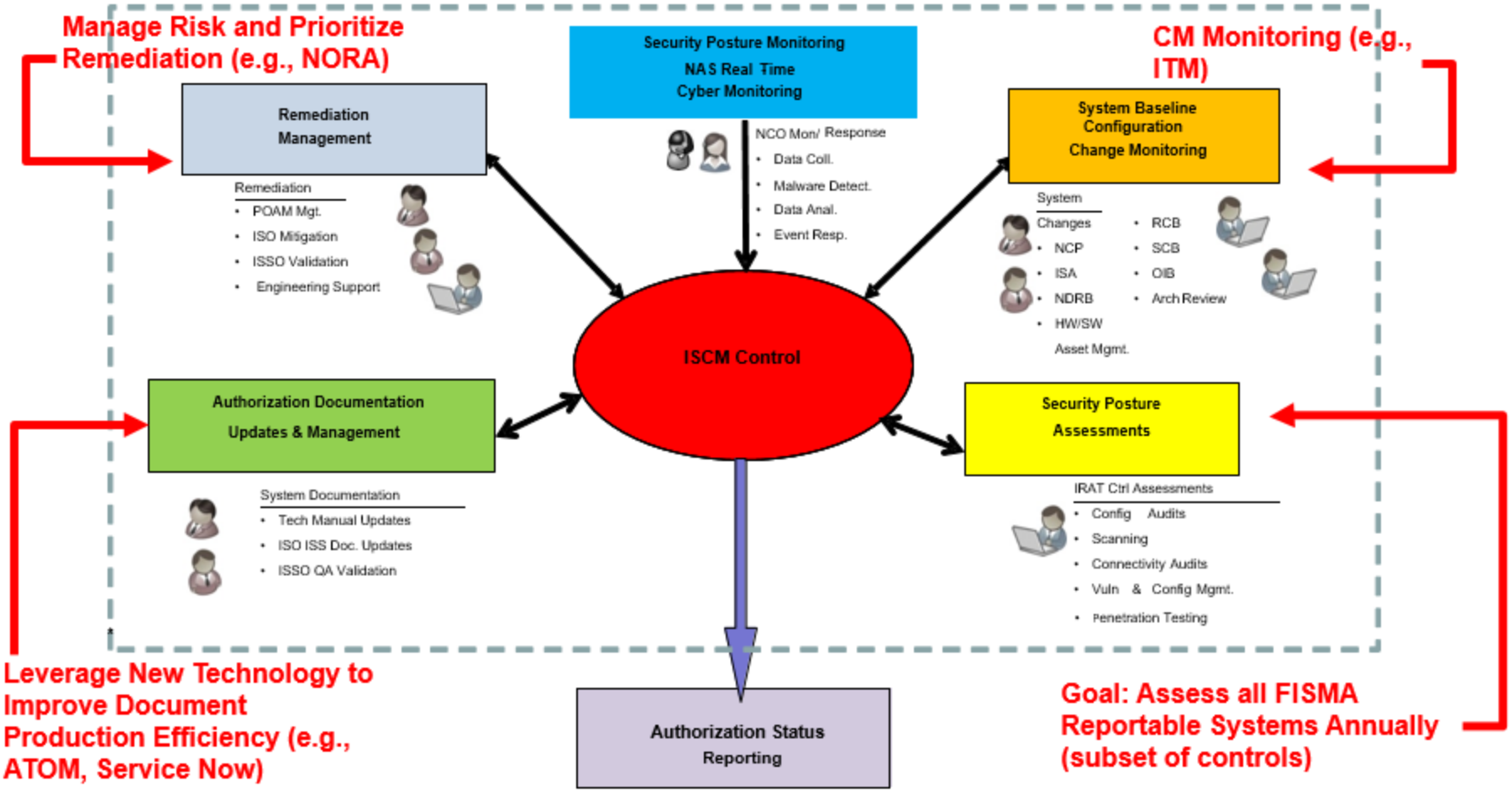


Initial & Ongoing Authorization

- **New systems complete an initial authorization**
  - Based on the **full set** of ATO Tailored NIST 800-53 (as amended) security controls
- **After initial authorization, systems complete annual continuous monitoring assessments as part of Information Security Continuous Monitoring (ISCM)**
  - Based on a subset of security controls (e.g., core controls, open Plans of Action and Milestones (POAMs), OIG/GAO/DHS findings/alerts, other controls as required)
  - Ongoing Authorization requires Authorizing Official (AO**)** signature at least once every 3 years or Authorization expires

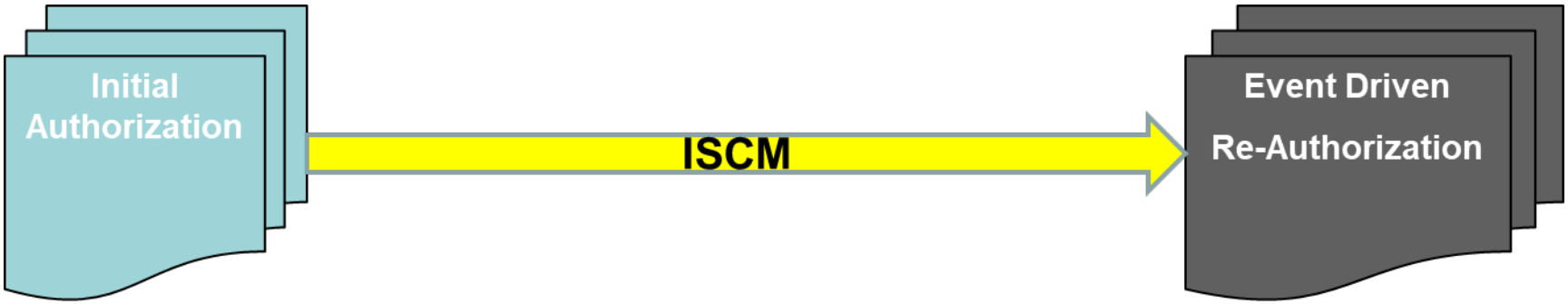


ATO ISCM Process Overview



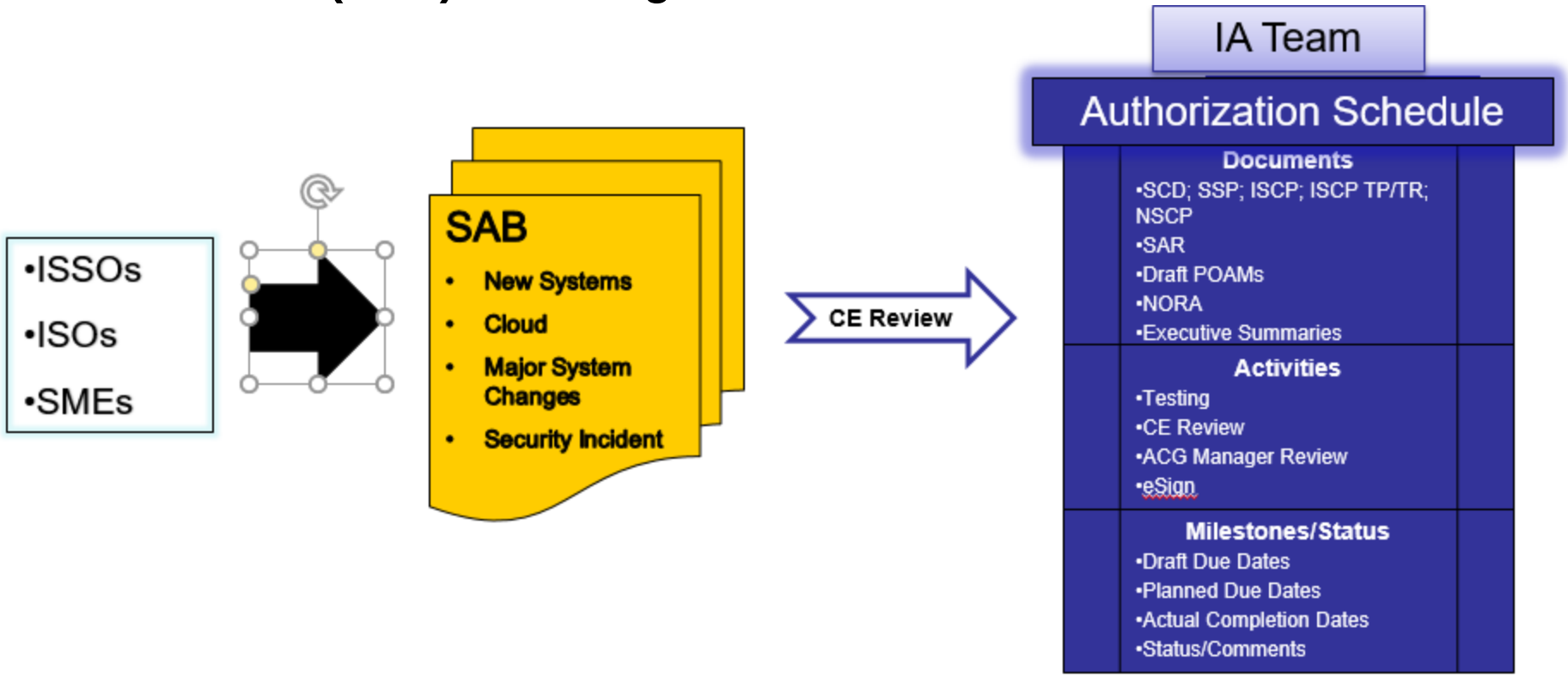
Re-Authorization Criteria

- **System Re-Authorization is event driven, not time driven**
- **If during ISCM an event occurs that significantly changes or brings into question the overall security posture of the system, a full system Re-Authorization may be required**
- **Events driving Re-Authorization include:**
  - New threat/vulnerability/impact information
  - An increased number of findings/weaknesses/ deficiencies from the ISCM Program
  - New mission/business requirements
  - A change in the authorizing official
  - A significant Change in risk assessment findings
  - Significant changes to the information system, common controls, or the environment of operation
  - Organizational thresholds being exceeded
- **At Re-Authorization, an assessment of <u>all</u> requirements is conducted**



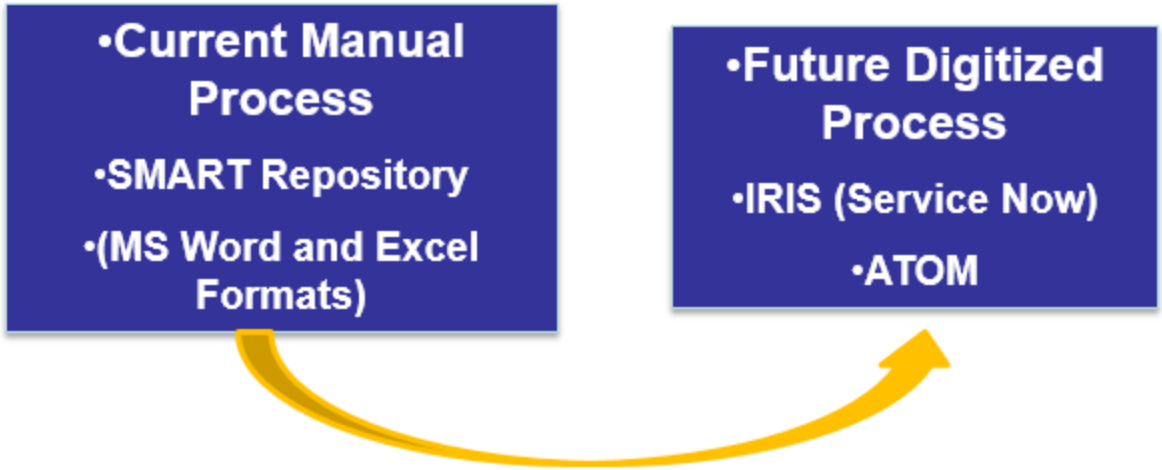
Getting On “The Schedule”

- **Systems need to get on the Authorization and ISCM Schedule for initial and ongoing authorization**
- **Targeted time line from submission of System Characterization Document (SCD) to AO signature = 6 months**



Complete Authorization Documents

- **Information System Owners (ISOs)/Information System Security Officers (ISSOs) develop/update system authorization documents per the schedule (SCD, SSP, NSCP, ISCP/ISCP Test Plan)**
  - Based on current year document templates (on ATO Information System Security (ISS) Website)



Scheduling Security Assessments

- **The Independent Risk Assessment and Test Team (IRAT) coordinates assessment and testing activities through the ISSO**
- **Testing "Windows" are documented on the schedule**
  - Actual test dates are set within the Window
  - Not all systems are testable, therefore, other assessment methods are used:
    - Examination
    - Interview
    - Observation/Demonstration

IRAT TEST DATE (30 days after SCD Submission & 14 days after SSP - 14day range to test)			
Start	End	Scan Date	Scan Confirmed
09/30/19	10/14/19	10/08/19	Confirmed

- **SSP <u>must</u> be completed prior to finalizing the SAR**

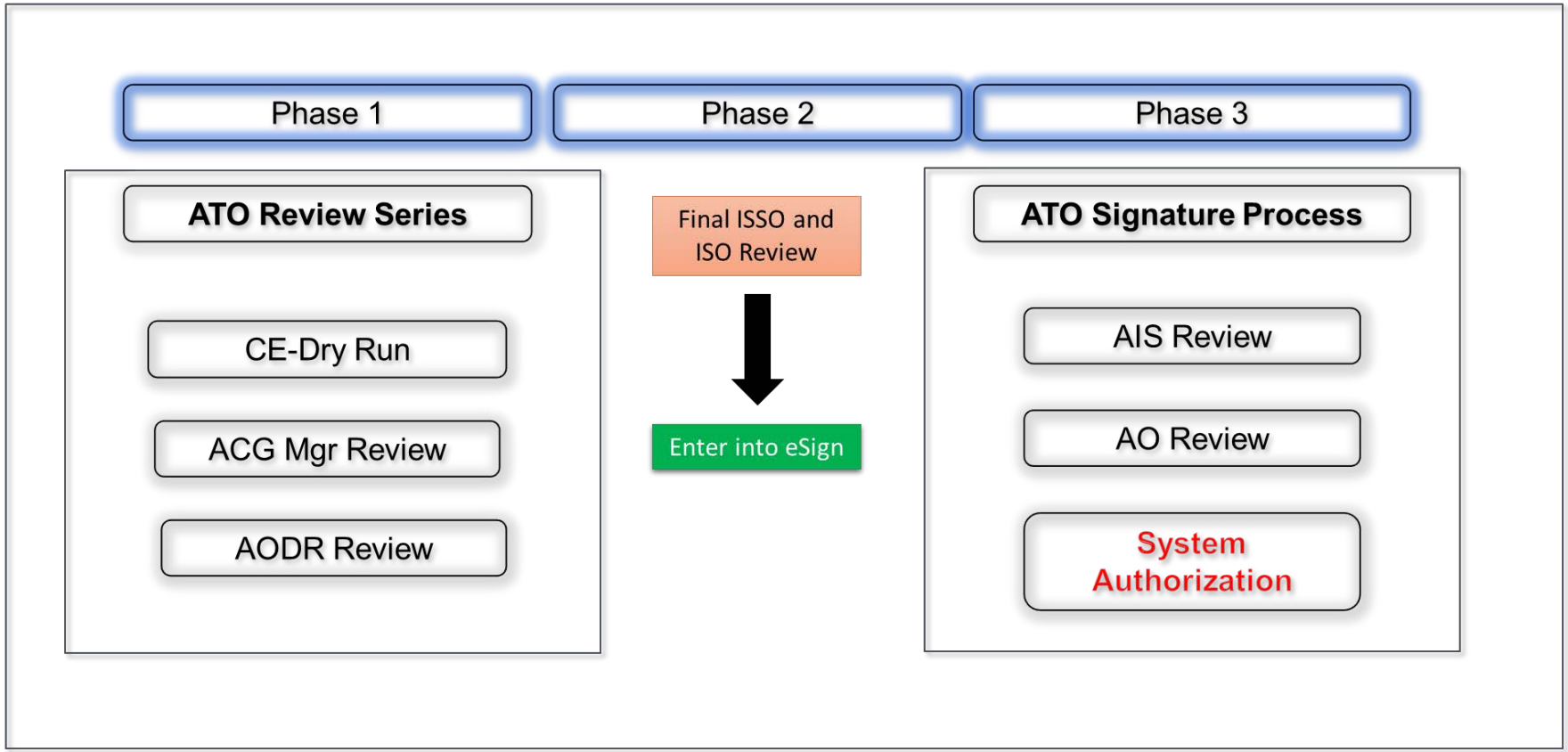
SAR and Draft POAMs

SAR (60 days after test, SCD & SSP must be complete)		Draft POAMs sent to ISSOs	
SAR Final Due	SAR Final Actual	POAM Draft Due	POAM Draft Received
01/10/20	01/06/20	01/18/20	01/07/20

- **The PC&G - IA Team develops the draft POAMs after receiving the SAR from the IRAT**
- **Draft POAMs are sent to ISSOs for finalization by the ISOs**
- **ISOs have 90 days to finalize their POAMs**
  - In that time they work on: cost, schedule, remediation plan
  - Checkpoints are built-in at T-minus 60, 45 (escalation point if necessary) & 30 days in order to allow sufficient time to address issues that may be delaying POAM completion
- **Completion of SAR and draft POAMs trigger the POAM review process**

POAM Final Due	POAM Final Act	Total POAM	Finalized POAM	Remaining POAM	% POAM Finaliz
7/19/20		86	82	4	95%

Authorization Package Review/Signature



Post Authorization

- **After AO signature, the IA Team does the following:**
  - Uploads signed Executive Summary to:
    - Security Management and Assessment Reporting Tool (SMART)
    - Cyber Security Assessment and Management (CSAM)
- **Updates new ATO expiration date in the following:**
  - SMART
  - CSAM
  - Master Schedule
- **Updates authorization statistics**
- **ISO and ISSOs continue to remediate POAMs per the planned completion dates**