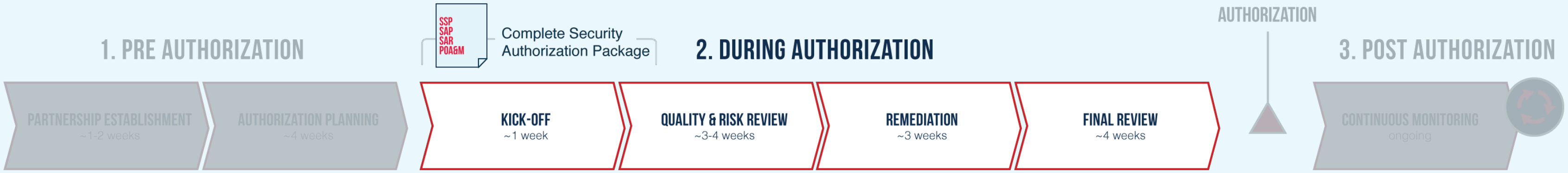
DURING AUTHORIZATION

Kick Off



AUTHORIZATION KICK-OFF

Kick-off meetings provide transparency into process, requirements and milestones for authorization among the Agency, CSP, and PMO

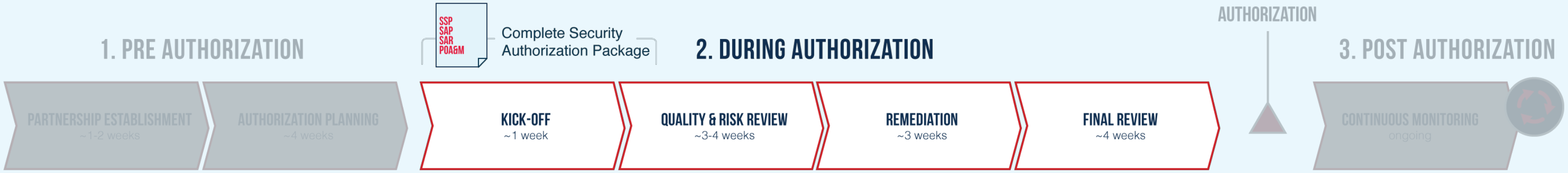
Best Practices

- Ensure the right people with the right authority are included in the meeting
- Create a kick-off agenda that structures and guides the conversation
- Instruct the CSP and 3PAO on which documents / materials to brief the Agency on prior to the kick-off
- Define roles and responsibilities for the process among the Agency, CSP, and 3PAO
- Clearly define and “showstoppers” for agency review up front
- Walk away from the meeting with clear understanding of action items and takeaways

PRO TIP Share agency-specific security requirements and concerns prior to the kick-off and gain consensus on the implementation of those controls

DURING AUTHORIZATION

Quality & Risk Review



1. PRE AUTHORIZATION

PARTNERSHIP ESTABLISHMENT
~1-2 weeks

AUTHORIZATION PLANNING
~4 weeks

SSP
SAP
SAR
POA&M

Complete Security
Authorization Package

2. DURING AUTHORIZATION

KICK-OFF
~1 week

QUALITY & RISK REVIEW
~3-4 weeks

REMEDIATION
~3 weeks

FINAL REVIEW
~4 weeks

AUTHORIZATION

3. POST AUTHORIZATION

CONTINUOUS MONITORING
ongoing

QUALITY & RISK REVIEW
Artifacts Required by FedRAMP

System Security Plan (SSP)		Security Assessment Plan (SAP)	Security Assessment Report (SAR)	Plan of Action and Milestones (POA&M)
Federal Information Processing Standard (FIPS) 199 Categorization	Control Implementation Summary (CIS) Workbook	Test Case Procedures	Risk Exposure Table	POA&M
Information Security Policies and Procedures	User Guide		Security Test Case Procedures/ Results Workbook	
Digital Identity Determination Plan	Privacy Threshold Analysis (PTA)/Privacy Impact Assessment (PIA)		Infrastructure, Database, and Web Application Scan	
Rules of Behavior (RoB)	Information System Contingency Plan (ISCP)	Penetration Test Plan and Methodology		
Configuration Management Plan (CMP)	Incident Response Plan (IRP)		Auxiliary Documents	
Separation of Duties Matrix	Laws and Regulations		Penetration Test Report	
Integrated Inventory Workbook	Continuous Monitoring Plan			

QUALITY & RISK REVIEW
Roles & Responsibilities

AGENCY

- Conduct review based on the approach determined in the authorization planning phase
- Determine plan for implementing customer procedures for addressing customer requirements
- Review the CSP's monthly scans submissions throughout the quality and review process
- When assessing the overall quality and risk of the authorization package, check for major issues or concerns in meeting Federal and Agency-specific requirements

CLOUD SERVICE PROVIDER

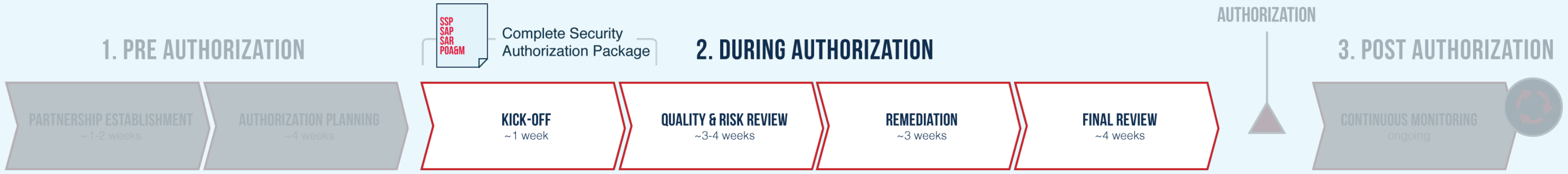
Participate in meetings with the Agency to address any questions arising from review

3PAO

Support CSP in meetings with Agency, as agreed to between CSP and 3PAO, to discuss Agency questions/concerns

DURING AUTHORIZATION

System Security Plan (SSP)

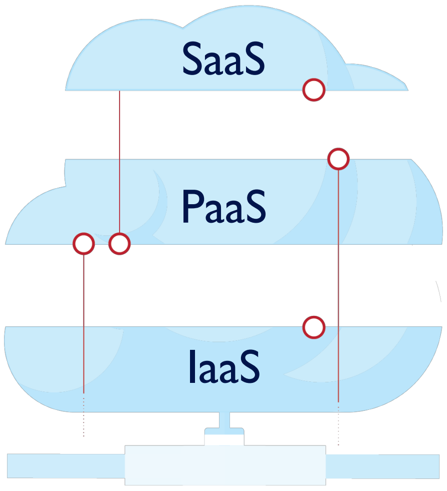


QUALITY & RISK REVIEW
Approach / System Security Plan (SSP) – Overview

What is a System Security Plan (SSP)?

- Provides an overview of the security requirements for the Cloud Service Offering
- Describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed, or stored by the system

SSP SECTION	WHAT'S IMPORTANT
All	Is it complete - is the entire template filled out?
Security Categorization (FIPS 199) [Section 2.2]	Is it appropriate for Agency data types?
Digital Identity Determination [Section 2.3]	Is it appropriate and accurate?
Cloud Service Model [Section 8.1]	Is it accurately represented for what the Agency is willing to authorize (SaaS, PaaS, IaaS)?
Cloud Deployment Model [Section 8.2]	Is it accurately represented for what the Agency is willing to authorize (Govt only, Public, Private, Hybrid)?
Leveraged Authorizations [Section 8.3]	Is it accurately addressed? The Agency needs to know what authorizations are being leveraged by the CSP, because the Agency must also authorize those services (entire stack must be authorized by each Agency). If there are services mentioned in the SSP that are not showing up as being leveraged or vice versa, then the Agency should question that.
System Description [Section 9]	Does it clearly describe the function(s) of the service and the narrative is not just marketing fluff?



THE STACK

QUALITY & RISK REVIEW
Approach / System Security Plan (SSP) – Overview

What is an Authorization Boundary?

All components of a cloud service to be authorized for operation by an Authorizing Official and excludes separately authorized systems, to which the cloud service is connected.

AUTHORIZATION BOUNDARY —WHAT'S IMPORTANT

Is it fully described and clearly illustrated?

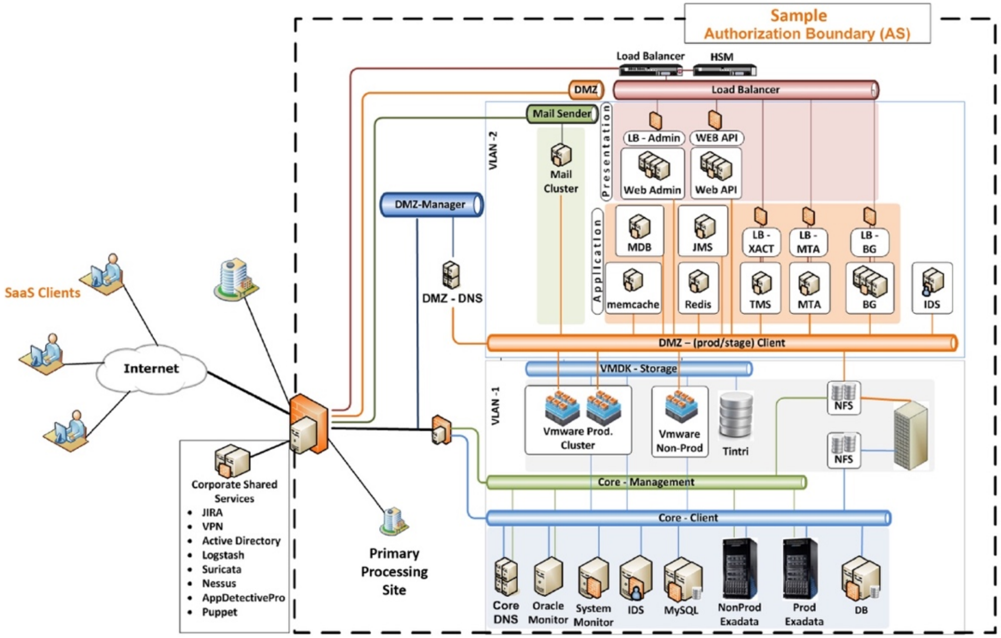
Does it include a clearly defined authorization boundary (typically a box around components)?

Does it define services wholly within the boundary and is it consistent with the system description?

Does it depict all major components or groups within the boundary?

Does it identify all interconnected systems?

Is it validated against the inventory?



QUALITY & RISK REVIEW
SSP – Authorization Boundary Red Flags

RED FLAG	WHAT IS THE CONCERN?
Boundary diagram is too simplistic	• Under-reporting of external service interconnections • Misrepresentation of system components (software applications and hardware); does not align with system inventory • CSP misunderstanding of what should be included in the boundary and Federal data protection considerations
Misrepresentation of leveraged service	• Lack of understanding of the CSP's boundary versus the boundary of the leveraged service
Overuse of corporate services	• Possible co-mingling of federal data with customer, commercial data • Additional external services that aren't reflected in the boundary
Interconnections between systems of differing security categorizations (e.g., concerns about transmission of data between high and low)	• Potential transfer of higher criticality data to a lower criticality service • Misunderstanding of the criticality of Federal data and adequate protection measures • Vetting of external services did not take into consideration Federal data processing/storage plans
Interconnections with cloud services that are not FedRAMP Authorized	• Agency should consider risk associated with using non-authorized services and should consider accepting risk for them or asking CSP to use a FedRAMP Authorized service

QUALITY & RISK REVIEW
Approach / System Security Plan (SSP) – Overview

WHAT IS A DATA FLOW?

Identifies anywhere Federal data is to be processed, stored, or transmitted; and how data comes into and out of the cloud service authorization boundary

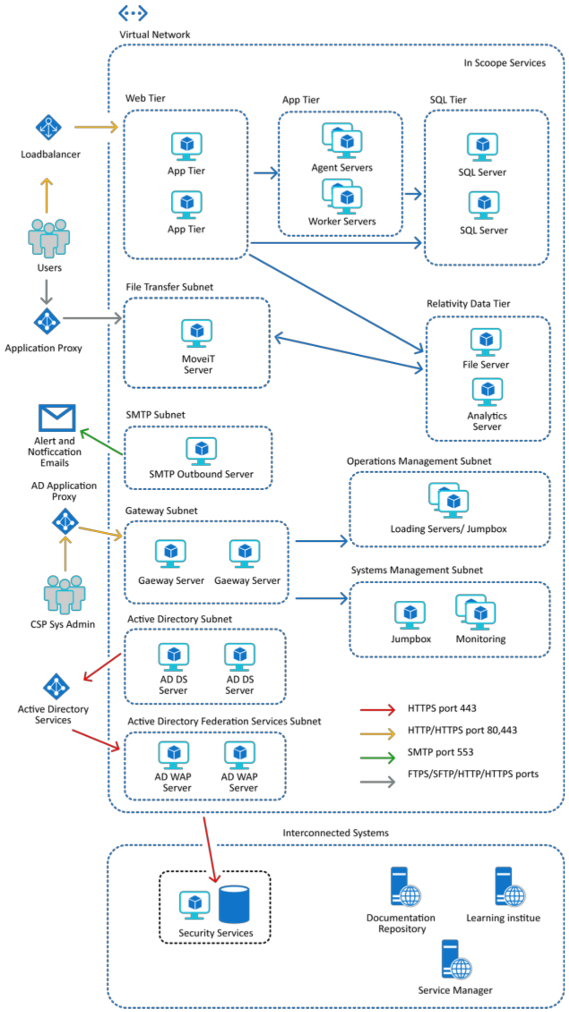
DATA FLOW - WHAT'S IMPORTANT

Is it fully described and clearly illustrated?

Does it delineate how data comes into and out of the system boundary, including ports, protocols, and services?

Does it identify data flows for privileged, non-privileged, and customers' access?

Does it identify an authentication mechanism to the system boundary?



QUALITY & RISK REVIEW
Approach / Anatomy of a Control

AC-17 Remote Access (L) (M) (H)

AC-17	Control Summary Information
Responsible Role:	
Parameter AC-1(a):	
Parameter AC-1(b)(1):	
Parameter AC-1(b)(2):	
Implementation Status (check all that apply): □ Implemented □ Partially implemented □ Planned □ Alternative implementation □ Not applicable	
Control Origination (check all that apply): □ Service Provider Corporate □ Service Provider System Specific □ Service Provider Hybrid (Corporate and System Specific) □ Configured by Customer (Customer System Specific) □ Provided by Customer (Customer System Specific) □ Shared (Service Provider and Customer Responsibility) □ Inherited from pre-existing FedRAMP Authorization	

Ensure the role is appropriate for the control

Describes organization-defined timeline, policy, or FedRAMP requirement associated with the control

Specifies the cloud services implementation status of the control requirements

Specifies who is/are responsible for performing the control

AC-17 What is the solution and how is it implemented?	
Part a	
Part b1	
Part b2	

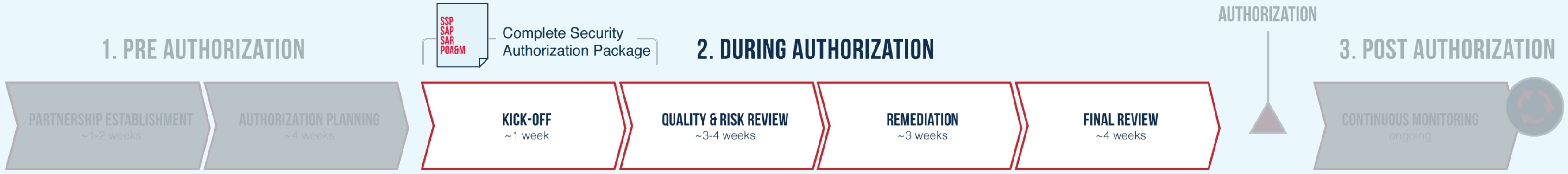
The what, when, who, and how of the control

QUALITY & RISK REVIEW
Approach / SSP – Security Control Red Flags

Control Section / Red Flag		What is the Concern?
Responsible Role	The same entity (ISSO) is performing many, most, if not all the controls	• CSP may not understand resources needed to fulfill the control • Raises concern about potential resource issue
Implementation Status	Status selected is incorrect or does not make sense	• CSP does not understand or know their implementation status • Erroneous selection(s) hastily made without thought/understanding of requirements. • SSP is not consistent actual implementation status per SAR; SSP not updated to address SAR findings
	N/A Controls inappropriately selected	• CSP is not planning to implement and control may not be tested as part of assessment • Erroneously used when the control is inherited
	Alternative Implementations inappropriately selected	• CSP may not understand the control • Sometimes used when there is no plan for meeting control
Control Origination	Unclear Customer Requirements	• Lack of understanding of required customer involvement
	Unclear System Inheritance	• Lack of understanding of what is being inherited • Sometimes overused; CSP erroneously assumes functions are being performed by leveraged service provider (IaaS/PaaS)
Solution Implementation Description	Vague Descriptions	• Lack of understanding of control or how the system meets the requirement • Descriptions developed hastily without thought/understanding of requirements
	Controls are inconsistent with SAR	• Documented process/procedures not consistent with how the CSP is actually performing efforts • Documented technical configuration differs from actual configuration

DURING AUTHORIZATION

Security Assessment



1. PRE AUTHORIZATION

PARTNERSHIP ESTABLISHMENT
~1-2 weeks

AUTHORIZATION PLANNING
~4 weeks

SSP
SAP
SAR
POA&M

Complete Security
Authorization Package

2. DURING AUTHORIZATION

KICK-OFF
~1 week

QUALITY & RISK REVIEW
~3-4 weeks

REMEDIATION
~3 weeks

FINAL REVIEW
~4 weeks

AUTHORIZATION

3. POST AUTHORIZATION

CONTINUOUS MONITORING
ongoing

QUALITY & RISK REVIEW
Approach / Assessment Overview

What is a Security Assessment?

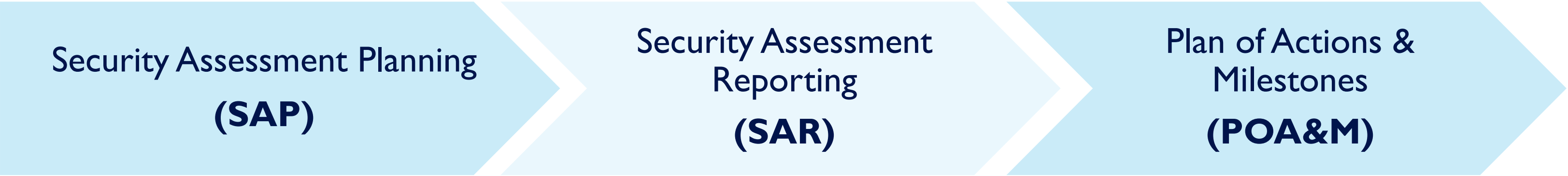
Performed to determine current security posture of a cloud service based on compliance with Federal requirements

Determine & identify residual risk based on level of compliance with Federal requirements

Determine adequacy of the mitigating controls and factors for residual risk

Provide specific recommendations on how to correct weaknesses or deficiencies in the controls

Key Security Assessment Phases



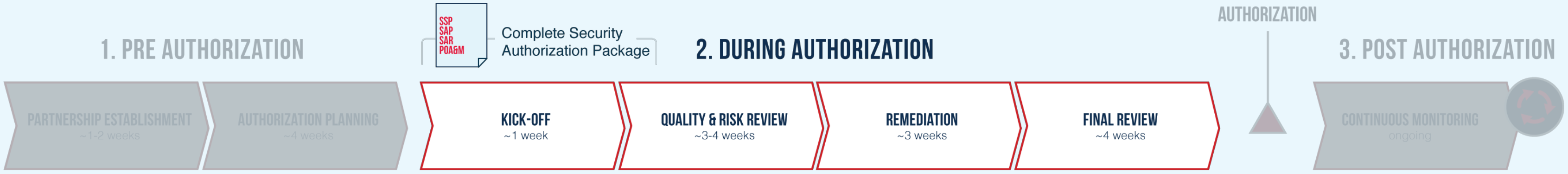
Security Assessment Planning **(SAP)**

Security Assessment Reporting **(SAR)**

Plan of Actions & Milestones **(POA&M)**

DURING AUTHORIZATION

Security Assessment Plan (SAP)



1. PRE AUTHORIZATION

PARTNERSHIP ESTABLISHMENT
~1-2 weeks

AUTHORIZATION PLANNING
~4 weeks

SSP
SAP
SAR
POA&M

Complete Security
Authorization Package

2. DURING AUTHORIZATION

KICK-OFF
~1 week

QUALITY & RISK REVIEW
~3-4 weeks

REMEDIATION
~3 weeks

FINAL REVIEW
~4 weeks

AUTHORIZATION

3. POST AUTHORIZATION

CONTINUOUS MONITORING
ongoing

QUALITY & RISK REVIEW
Approach / SAP

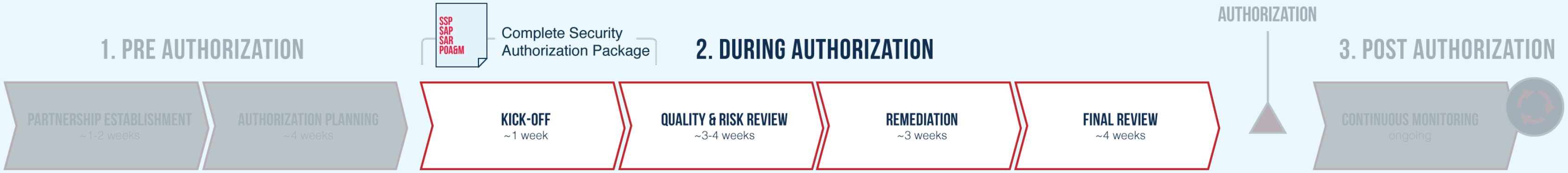
What is a Security Assessment Plan?

Describes the scope of the assessment; assessment procedures to be used to determine security control effectiveness; assessment environment, assessment team, and assessment roles and responsibilities.

SAP Section	What's Important
Scope [Section 2]	• Needs to include entire boundary and interconnections • Ensure assessor is using Integrated Inventory Workbook
Methodology [Section 4]	Ensure that if a sampling methodology is used, it is acceptable by the Agency. JAB Guidance: • FedRAMP recently published the Guide for Determining Eligibility and Requirements for the Use of Sampling for Vulnerability Scans • Any approach that uses sampling must be well-documented by the 3PAO, and approved in advance by the AO
Rules of Engagement [Section 6]	All roles and responsibilities have been identified for each participating party and agreed upon.
Test Case Procedures (Test Case Workbook) [Appendix A]	• All controls that are to be tested are included • Test procedures for covering alternative/unique implementation should be clearly articulated
Penetration Testing Plan and Methodology [Appendix B]	The plan clearly articulates how all attack vectors are going to be tested and consistent with FedRAMP Penetration Test Guidance.

DURING AUTHORIZATION

Security Assessment Report (SAR)



1. PRE AUTHORIZATION

PARTNERSHIP ESTABLISHMENT
~1-2 weeks

AUTHORIZATION PLANNING
~4 weeks

SSP
SAP
SAR
POA&M

Complete Security
Authorization Package

2. DURING AUTHORIZATION

KICK-OFF
~1 week

QUALITY & RISK REVIEW
~3-4 weeks

REMEDIATION
~3 weeks

FINAL REVIEW
~4 weeks

AUTHORIZATION

3. POST AUTHORIZATION

CONTINUOUS MONITORING
ongoing

QUALITY & RISK REVIEW
Approach / SAR

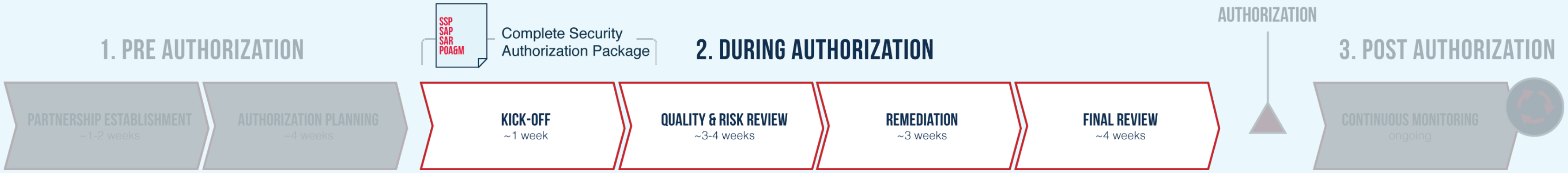
What is a Security Assessment Report?

Describes the assessment process/procedures and residual risks associated with the vulnerabilities identified during the security assessment of the cloud service.

SAR Section	What's Important
Scope [Section 1.4]	Consistent with the SAP.
Security Categorization [Section 2.1]	**Consistent with the SSP** and other documents.
Assessment Methodology [Section 3]	Testing should be performed within Agency acceptable time frame. • Scan and test case may not be older than 120 days prior to submission to Agency for review • Pen test must be within 1 year of SAR submission date to Agency, or as approved by the Agency AO • Agencies may seek waiver for timelines of testing if AO provides written approval in ATO letter and CSP attests that the architecture has not changed since testing
Assessment Deviations [Section 3.1.1]	Are within reasonable limits (i.e., testing schedule was adjusted, does not exclude parts of the system, etc.).
Risks Remaining Due to Operational Requirements [Section 5.3]	**Operationally Required (OR)** findings need to have solid mitigating factors and the Agency AO needs to accept risk for ORs.
Authorization Recommendation [Section 7]	The **3PAO's recommendation** should support what is presented in the SAR.
Appendices A - F	• The summary tables should be consistent with Risk Exposure table, Pen Test Report, and Test Case Workbook; and are adequately separated by type • 3PAO should provide scan and must witness or perform the scans • Unusual number of false positive, large number of Highs, or excessive number findings • Evidence files should be included with the package (screenshots, collected files, etc.)
Appendix J – Pen Test Report	Critical component of SAR. FedRAMP will not authorize without Pen Test Report.

DURING AUTHORIZATION

Penetration Testing



1. PRE AUTHORIZATION

PARTNERSHIP ESTABLISHMENT
~1-2 weeks

AUTHORIZATION PLANNING
~4 weeks

Complete Security Authorization Package

2. DURING AUTHORIZATION

KICK-OFF
~1 week

QUALITY & RISK REVIEW
~3-4 weeks

REMEDIATION
~3 weeks

FINAL REVIEW
~4 weeks

AUTHORIZATION

3. POST AUTHORIZATION

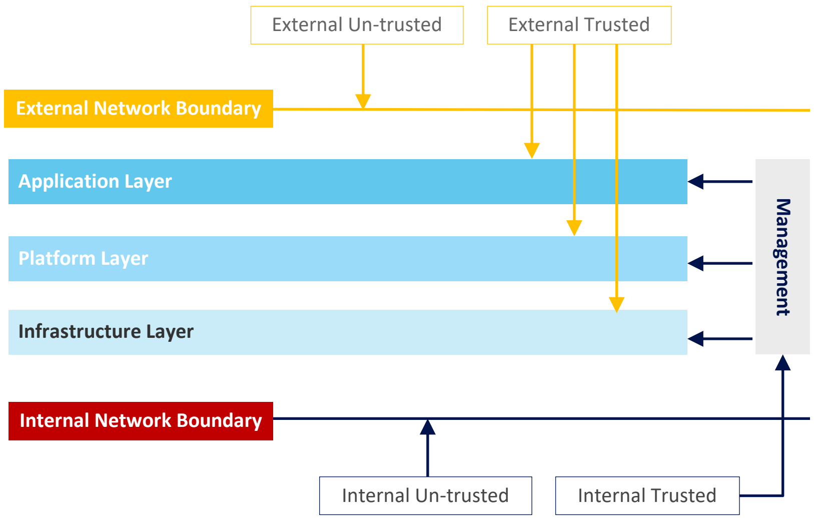
CONTINUOUS MONITORING
ongoing

QUALITY & RISK REVIEW
Approach / Penetration Testing Guidance Deep Dive

What is a Penetration Test?

An authorized simulated attack on a cloud service, performed to evaluate the security of the service. The test is performed to identify both weaknesses including the potential for unauthorized parties to gain access to the service's features and data.

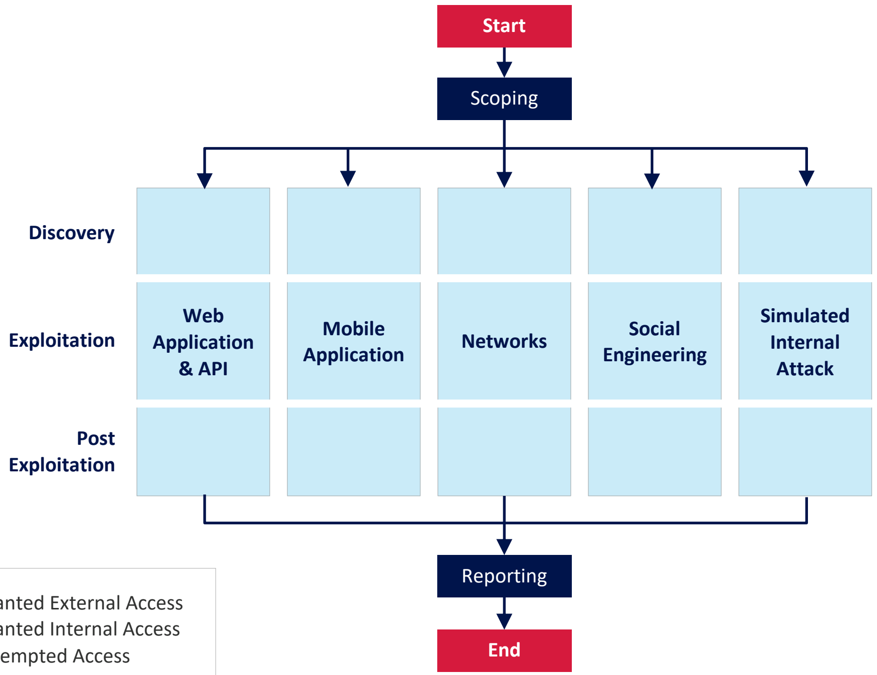
SAMPLE TARGET SYSTEM



LEGEND

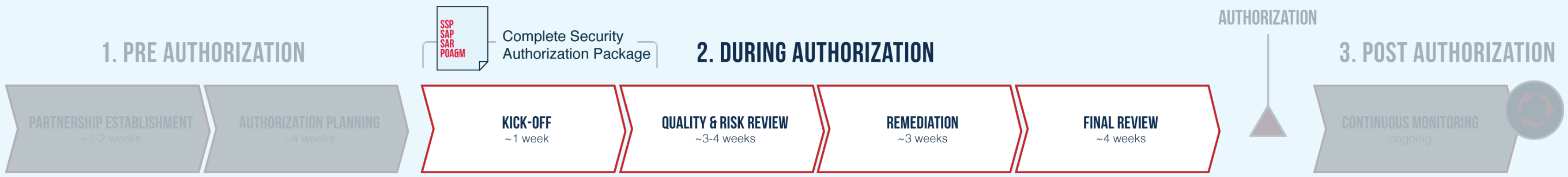
▬ Granted External Access
▬ Granted Internal Access
— Attempted Access

ELEMENTS OF A PENETRATION TEST



DURING AUTHORIZATION

Plan of Action and Milestones (POA&M)



QUALITY & RISK REVIEW
Approach / POA&M

What is a Plan of Action and Milestones?

A plan that describes specific measures to be taken to correct deficiencies found during a security assessment.

POA&M - What's Important	
Is the POA&M complete and is it consistent with the SAR?	
Was the FedRAMP POA&M Template Completion Guide followed?	
It should represent a snapshot in time.	
CSP is responsible for maintaining POA&M.	
All applicable columns should be filled out with enough detail to understand the remediation plan. (Bare minimum - at least an Original Detection Date, Adjusted Risk Rating, and Scheduled Completion Date).	
Remediation timeframes should be consistent with FedRAMP and/or Agency requirements. FedRAMP Remediation timeframes:	30 days – High 90 days – Moderate 180 days – Low
Operationally Required findings should be included in POA&M "Open" Tab.	

QUALITY & RISK REVIEW
Best Practices

Be aware of the Agency “hot button” issues to ensure requirements are adequately addressed

Obtain SSP and artifacts from the CSP as ready – Just-in-Time Approach – rather than reviewing the package all at once

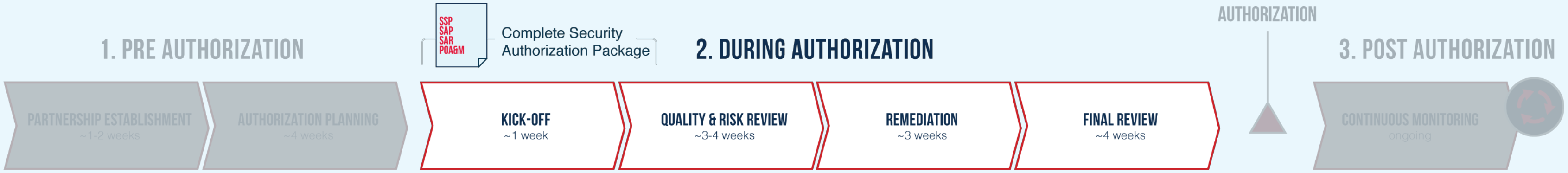
Ensure all deliverables are completed by the CSP / 3PAO before issuing an ATO

IF YOU SEE SOMETHING – SAY SOMETHING. Do not be afraid of asking questions about things that do not seem quite right.

- In coordination with the CSP, establish a plan and cadence for the review effort (e.g. scheduling, syncs, expectations, deliverables, etc.)
- Make sure you have the right resources dedicated to the review effort
- Request CSP to do their own quality reviews to ensure the package is complete and addresses all requirements
- Encourage the CSP to hire a 3PAO consultant to help with documentation
- Make sure the CSP has responded to **ALL** the requirements and answered the intent of the requirements
- Engage the FedRAMP PMO Agency Team for guidance and assistance

DURING AUTHORIZATION

Remediation



REMEDIATION
Roles & Responsibilities

AGENCY

- Assemble and provide comments/questions for authorization package to CSP
- Conduct meetings with CSP and 3PAO to discuss concerns, expectations, and to agree on next steps
- Coordinate with CSP on timeline for remediation efforts
- Reach out to FedRAMP as needed for guidance and assistance

CLOUD SERVICE PROVIDER

- Participate in meetings with Agency to discuss any concerns about package / technical security concerns
- Establish schedule for remediation activities with concurrence from Agency and 3PAO
- Perform remediation efforts per SAR and Agency concerns / questions
- Update SSP and / or other artifacts to address concerns; providing both a track-changes version and "clean" version, as agreed upon with Agency
- Coordinate with the 3PAO for remediation testing

3PAO

- Support CSP in meetings with Agency, as agreed to between CSP and 3PAO, to discuss Agency questions / concerns
- Perform remediation testing
- Develop final SAR and supporting material

REMEDIATION
Best Practices

Remediation of insufficiencies, weaknesses, and vulnerabilities occurs throughout authorization.

Review updated submissions to verify remediation was completed as expected and agreed to by the stakeholders, including the SSP and attachments, SAP, SAR, and POA&M.

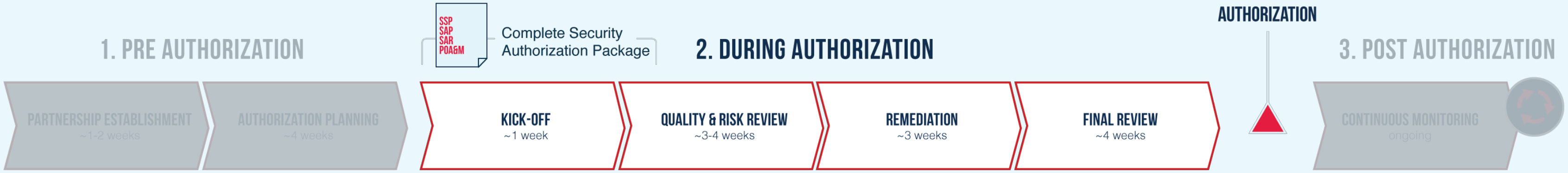
Maintain constant communications throughout the remediation process to ensure solutions are addressing Agency reviewer concerns.

Don’t hesitate to reach out to the FedRAMP PMO if you encounter challenges.

- The question of when / how to make a decision to require remediation is based on actual risk and Agency-specific policies and business mission.
  - Some risks require immediate remediation due to negative impact on the overall risk posture
  - Incomplete testing / assessment
  - Large number of “high” impact risk findings
  - Findings related to boundary protections, authentication, vulnerability management, access controls
  - Some risks may be remediated as part of Continuous Monitoring following authorization
- The Agency review of remediation work can happen on a Just-in-Time or on a Linear basis depending on Agency reviewer, CSP, and 3PAO preferences.
- At the end of the remediation phase, have an in-person remediation close-out meeting to review all changes, address questions in real time, and obtain approval.

DURING AUTHORIZATION

Final Review and Authorization



SSP
SAP
SAR
POA&M

Complete Security Authorization Package

1. PRE AUTHORIZATION

PARTNERSHIP ESTABLISHMENT ~1-2 weeks

AUTHORIZATION PLANNING ~4 weeks

2. DURING AUTHORIZATION

KICK-OFF ~1 week

QUALITY & RISK REVIEW ~3-4 weeks

REMEDIATION ~3 weeks

FINAL REVIEW ~4 weeks

AUTHORIZATION

3. POST AUTHORIZATION

CONTINUOUS MONITORING ongoing

FINAL REVIEW AND AUTHORIZATION

Roles & Responsibilities

AGENCY

- Conduct final review of authorization package
- Reach out to FedRAMP as needed for guidance and assistance
- Prepare and facilitate AO signature of Final Authorization Package
- Upload / submit signed ATO to FedRAMP secure repository

CLOUD SERVICE PROVIDER

- Participate in meetings with Agency to discuss any concerns about package / technical security concerns
- Coordinate with Agency on upload of Final Authorization Package to FedRAMP secure repository

3PAO

- Support CSP in meetings with Agency, as agreed to between CSP and 3PAO, to discuss Agency questions / concerns
- Upload Final Assessment material to FedRAMP secure repository

FINAL REVIEW AND AUTHORIZATION
Best Practices

Ensure all required remediation has been successfully completed and documented. CSPs should submit both "redlined" and final versions of documentation for Agency review / approval.

Refer to the FedRAMP Initial Authorization Package Checklist to ensure completeness of package.

Each Agency / AO makes the final decision based on a determination that the risk posture of the system is at an "acceptable" level for the Agency's use of the service.

Ensure upload of FedRAMP authorization package and signed ATO letter to FedRAMP secure repository.

- Document completed authorization package review per Agency policies and procedures (e.g., Agency-specific checklist, briefing, review report, etc.).
- Make sure the i's are dotted and the t's are crossed and a complete, high-quality authorization package is submitted for FedRAMP review, if applicable.
- Factors that can impact an Agency / AO risk determination
  - Types / numbers of residual risks
  - Agency policies and risk appetite factor
  - Business and mission needs