

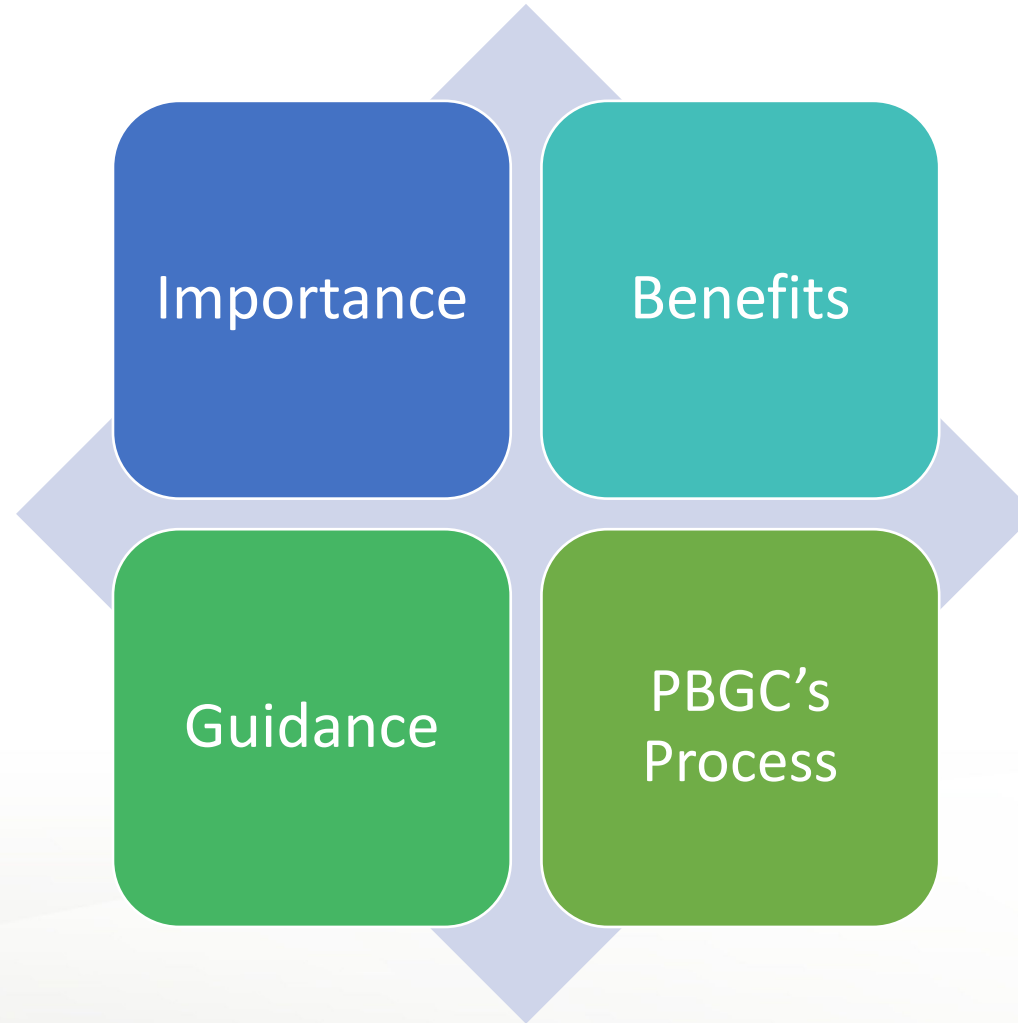


# Building a Consistent and Repeatable Assessment Process – PBGC’s Journey

*Presented by: Sue Schultz-Searcy, CISA, Assessment and Authorization Division Manager (AAD),  
ECD*

*David Woodson, Assessment Program Lead, ECD*

*5/23/2023 – not for attribution*



# Assessment Program Benefits

Identify security and privacy risks

Manage and mitigate risks

Protect sensitive information

Ensure compliance

Prevent Incidents

Optimize resources

Support Audits

Promotes Collaboration



# Guidance to Support Federal Assessment Program

NIST (SP) 800-53

NIST 800-53A

NIST (SP) 800-39

# PBGC's Assessment Program

1. Supports the PBGC's enterprise-wide continuous monitoring strategy.
2. Facilitates the assessment of Enterprise Common Controls, Core Controls, and selected system specific controls.
3. Is documented in the Assessment Program Plan (Runbook) developed by the Enterprise Cybersecurity Department.

The Runbook outlines the assessment process, including:

- Identifying the relevant controls
- Assessment techniques
- Data collection methods
- Analysis
- Reporting
- Roles & Responsibilities
- Templates
- And is updated at least annually or as necessary to reflect evolving practices related to security and privacy requirements.

# Roles and Responsibilities

- Authorizing Officials (AO)
- Common Control Providers (CCP)
- Information Security Officer (ISO)
- Information System Security Manager (ISSM)
- Information System Security & Privacy Officers (ISSPO)
- Security Control Assessors (SCA)

# Roles and Responsibilities cont. - Security Control Assessors

- Security Control Assessors (SCA) are responsible for conducting security and privacy control assessments while applying a standard methodology to evaluate the effectiveness of the controls.
- The role of the SCA is designated as a significant security role at PBGC which requires them to complete annual role-based training.
- New SCAs are subject to a Quality Assurance Process.
- A weekly meeting has also been established to convey program updates and to provide assessment statuses to management.

# Roles and Responsibilities cont. - Security Control Assessors





Security Control Assessor Level	Qualification & Responsibilities	Education, Certifications & KSAs (Based on NICE SP-RSK-002, OPM DCWF Code 612)	Experience	GS Level Equivalent	Key Metrics
<b>SCA Level I</b>	<p>require moderate information system security knowledge and skills to perform the following responsibilities:</p> <p>Perform information systems assessment and authorization (A&amp;A) as defined in applicable ICDs and guidance.</p> <p>Perform the processes involved in developing and implementing security related directives and guidance for Information Assurance, Information Technology, and Information Management.</p> <p>Utilize risk management strategies for information technology solutions.</p> <p>Understand emerging technologies and their implementation within Government system and network environments.</p> <p>Possess knowledge of information technology concepts used in the evaluation of security performance and integrity of state-of-the-art applications, communications systems, hardware, software, satellite control systems, and</p>	<p>Bachelor's Degree</p> <p>SSCP, CCNA-Security, GSEC, Security+, CISA, GCIH, GCED, CISSP, CASP</p> <p>K001 – Knowledge of computer networking concepts and protocols, and network security methodologies.</p> <p>K0002 – Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).</p> <p>K0003 – Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.</p> <p>K0004 – Knowledge of cybersecurity and privacy principles.</p> <p>K0005 – Knowledge of cyber threats and vulnerabilities.</p> <p>K0006 – Knowledge of specific operational impacts of cybersecurity lapses.</p> <p>K0007 – Knowledge of authentication, authorization, and access control methods.</p> <p>K0008 – Knowledge of applicable business processes and operations of customer organizations.</p> <p>K0009 – Knowledge of application vulnerabilities.</p> <p>K0010 – Knowledge of communication methods, principles, and concepts that support the network infrastructure.</p>	0-3 years	GS-7	<p>SCA Should be able to do 20+ controls per month</p> <p>Works with some guidance without and writes reports with no more than 1 round of review and peer review is required.</p>



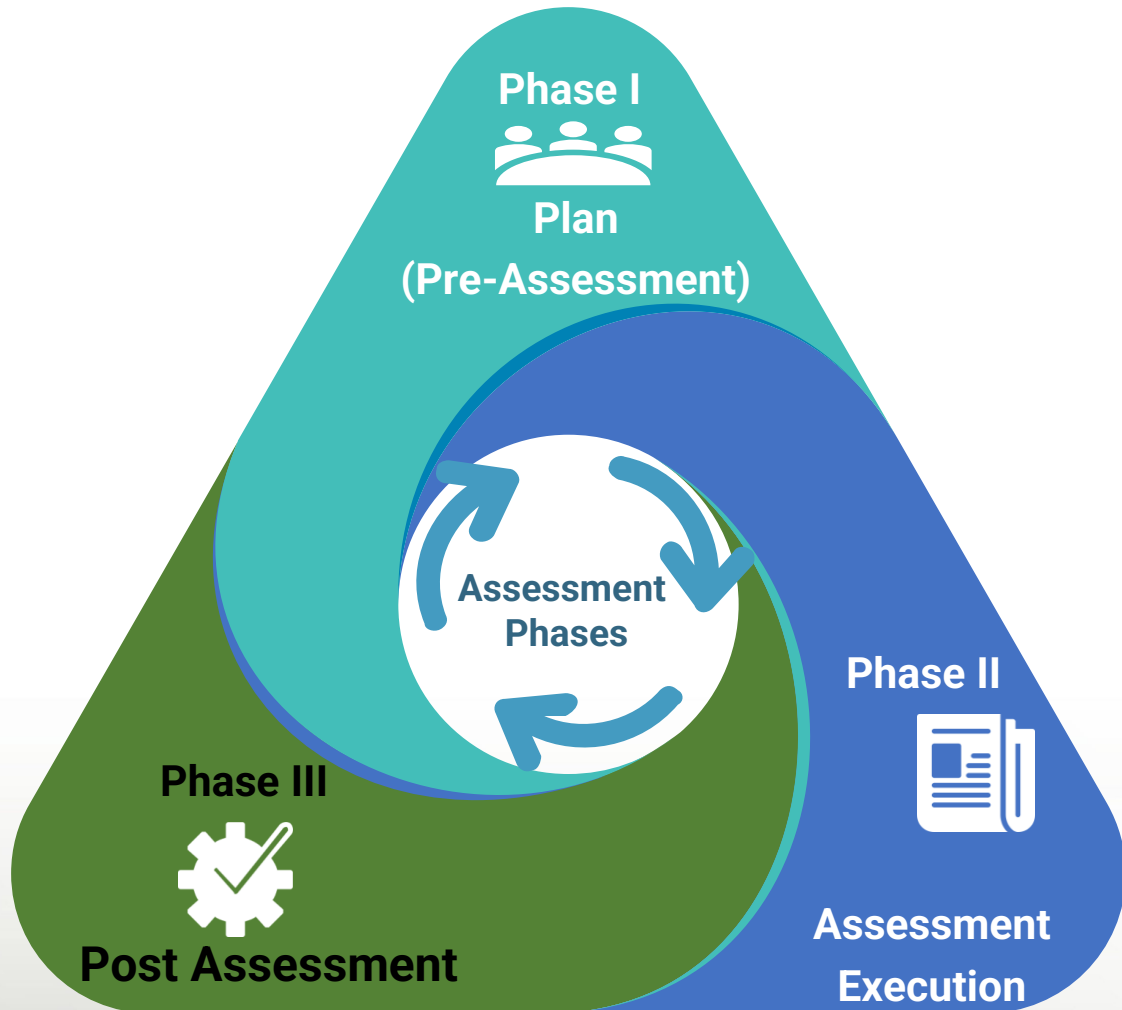
# Roles and Responsibilities cont. – RACI Chart

## Assessment Roles and Responsibilities (Defined & Communicated)

Tasks \ Roles	Phase I		Phase II					Phase III	
	Plan & Prepare Assessment (SSP)	Pre-Assessment (Impl. Statements & Artifacts)	Assess Controls	Review Artifacts, DIS & Impl. Statements	Draft IRR	Conduct Interviews	Draft Assessment Report	Upload Results to CSAM & ECM SharePoint	Generate and deliver SAR, Summary Analysis
ISSM	I	I		I					I
ISO	A	A				I			I
ISSPO	C	C				I			I
AO	C	C							I
CCP	R	R	I	I	I	I			I
SCA			R	R	R	R	R	R	R

 Responsible, 
  Accountable, 
  Consulted, 
  Informed

# Assessment Phases



## I - Plan (Pre-Assessment)

- Purpose & Scope
- Roles & Responsibilities
- Control Assessment Procedures

## II - Assessment Execution

- SCA Reviews Controls in CSAM
- SCA Reviews Artifacts
- SCA Prepares the method for examining, interviewing, and or testing control requirements

## III - Post-Assessment

- SCA document results in CSAM
- Assessment program team leads generates Security Assessment Report (SAR) and sends out a summary email to control PoCs
- Issue Resolution Log (IRL)
- Performance Metrics

1. Assessment Template
2. Assessor Review Checklist
3. Issue Resolution Report Template
4. Lessons-Learned Record

# Assessment Template

Assessor Name *Choose an item.:*

Date: *Click or tap to enter a date.*

NIST Control Number:		Total # DIS:	
<b>Implementation Statement:</b>			
Text here			
<b>DIS Requirement:</b>			
Text here			
<b>Assessment Findings:</b>			
Text here			
<b>Assessment Result:</b>		Choose an item.	
<b>Methods &amp; Objectives:</b>			
Text here			

# Assessment Template Alternative

1.  Export to Excel

2.

DIS Number	Implementation Statement	Determine If Statement	Finding	Methods & Objectives:	Assessment Result	Assessor	Assessment Date

# Assessors Review Checklist

		Peer reviewed by:			Choose an item.
Check Parameter	Yes	No	NA	Comments	
1) Does the Implementation Statement address the Determine If Statement (DIS) requirements? (It is important that the implementation statement supports the DIS)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
2) Have all artifacts been uploaded to CSAM? (Documents, Screen Shots, Drawings, etc.)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
3) Are the assessors results clearly documented? And if the result is 'other than satisfied', are the corrective recommendations/actions clearly documented? (This is important so that the CCP can understand the findings and know what needs to be done to correct them so the control result can be moved to 'satisfied'?)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
4) Are there spelling errors? If so, correct them.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
5) Are there grammatical errors? If so, correct them.	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
6) Are all workpapers uploaded to SharePoint?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

# Issue Resolution Report Template

Issue ID #	Date Identified	SCA	Control POC/SMEs	Control/ DIS	Issue Description / Interview Questions / Recommendation	Targeted Resolution Date	Status (New, In-Progress, Closed)	ITIOD Response/SCA Comments

# Lessons-Learned Log

Assessment Program Lessons-Learned											
No.	CM Focus Area	Identified Fiscal Year - Quarter	Lesson Learned	Source	Resolve			Action(s) Taken / Planned	People	Process	Technology
					Y	P	N				



- Continue to evaluate the assessment program for enhanced quality and efficiencies.
  - Assessment Program Evaluation
  - CSAM automation
  - CSAM Integrated Project Team (IPT)
- See what other automation efforts might help to improve the assessment process.
  - Open Security Controls Assessment Language (OSCAL)

