American Society of Military Comptrollers
Professional Development Institute 2017

"What the SOC?"

A Reporting Entity's Guide to Evaluating System and Organization Controls (SOC) 1 Reports

June 2017

Notice

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

Introductions

Geoff Weber
Partner, Federal Advisory Services
KPMG LLP

Stephen Camara
Managing Director, Federal Advisory Services
KPMG LLP

James Davila
Staff Accountant, Office of the Deputy Chief Financial Officer
Office of the Secretary of Defense

Tony Hullinger
Director, Office of Audit Readiness
Defense Finance and Accounting Service

Eric Engelbrektsson
Chief, Financial Policy Branch
Defense Logistics Agency

Level-Setting Concepts

It’s all about the relationship…

A trading partner

A service organization

A customer

Level-Setting Concepts

SOC 1 Report Basics…

– What are they?

– What are they used for?

– Who are the key players in their preparation and use?

– What do they contain?

– Why are they important?

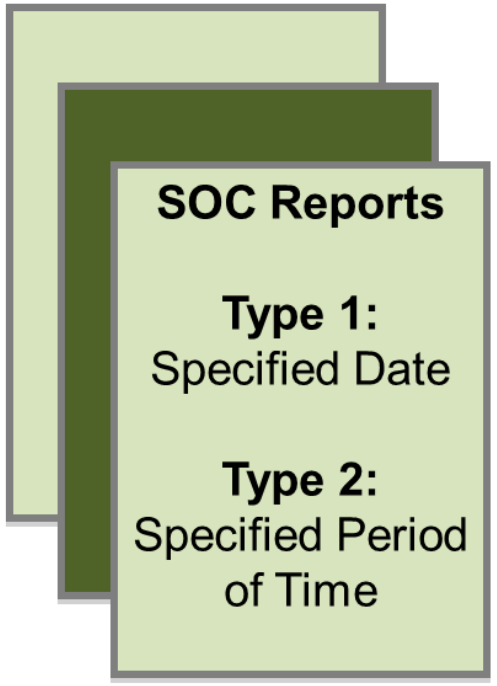
Level-Setting Concepts

SOC 1 reports…

- …provide important information about a service organization and its controls relative to user entities' internal control over financial reporting
- …contain sections prepared by an independent auditor (a.k.a., the 'service auditor') AND service organization
- …help a user entity and its auditors obtain an understanding of the service organization and, if properly scoped, support the user auditor's design of a control-based audit

SOC 1 Report Structure and Content

Section	SOC 1 Report Contents	Reponsibility
I.	Independent Service Auditor's Report	Service Auditor
II.	Management's Assertion	Service Organization
III.	Management's Description of the System	Service Organization
IV.	Control Objectives, Control Activities, and Test of Operating Effectiveness (Type 2 reports)	Shared
V.	Other Information Provided by the Service Organization	Service Organization



Panel Discussion

Steve Camara, Moderator

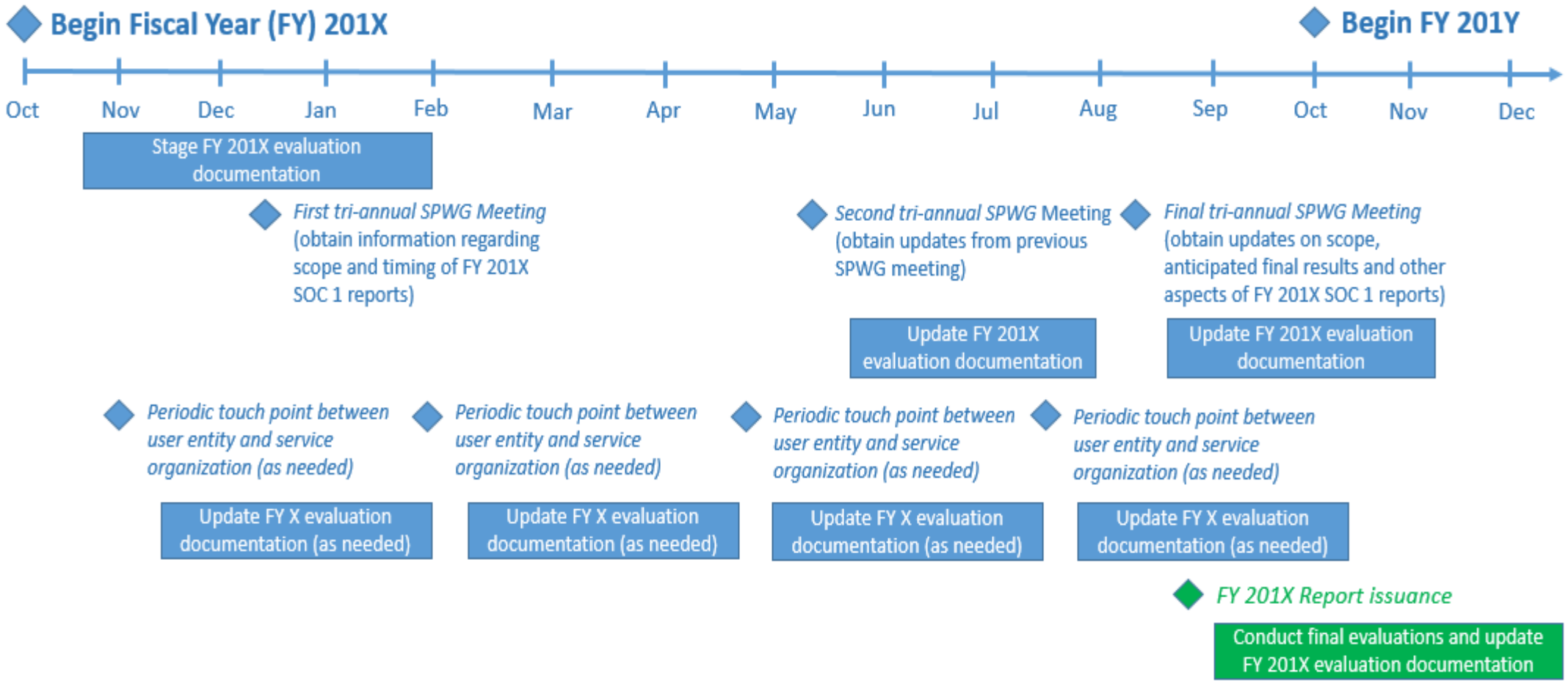
Discussion Topic 1

Question: What factors should I consider when determining whether my service organization's SOC 1 reports are properly scoped?

Discussion Topic 2

Question: What are some suggestions for establishing a robust, ongoing cycle of interaction between my organization, our financial statement auditors, and our service organizations?

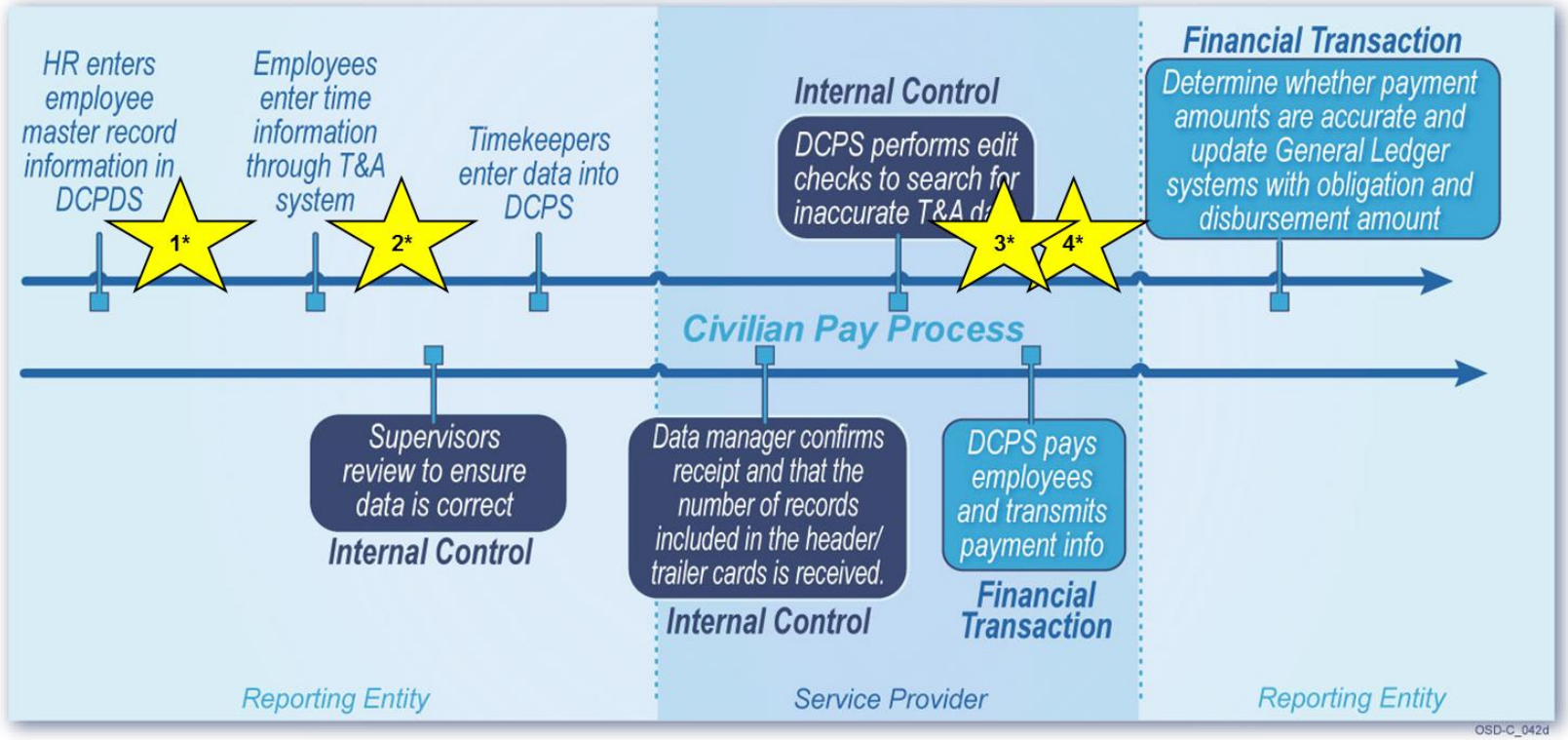
A Notional Timeline of Key Activities



Discussion Topic 3

Question: What are some key considerations and leading practices for me to consider when evaluating the results of my service organization's SOC 1 reports?

Family of SOC 1s – An Example



SSAE 16

1 – DMDC Defense Civilian Personnel Data System SOC 1
2- - Defense Agency Initiative (DAI) and Automated Time (ATAAPS) SOC 1
3 – DFAS Defense Civilian Payroll Service (DCPS) SOC 1
4 – DFAS Standardized Disbursing Service (ADS) SOC 1
5 – DFAS Financial Reporting SOC 1 (DDRS)
* - Systems hosted in a DISA Enterprise Services Directorate Data Center SOC 1

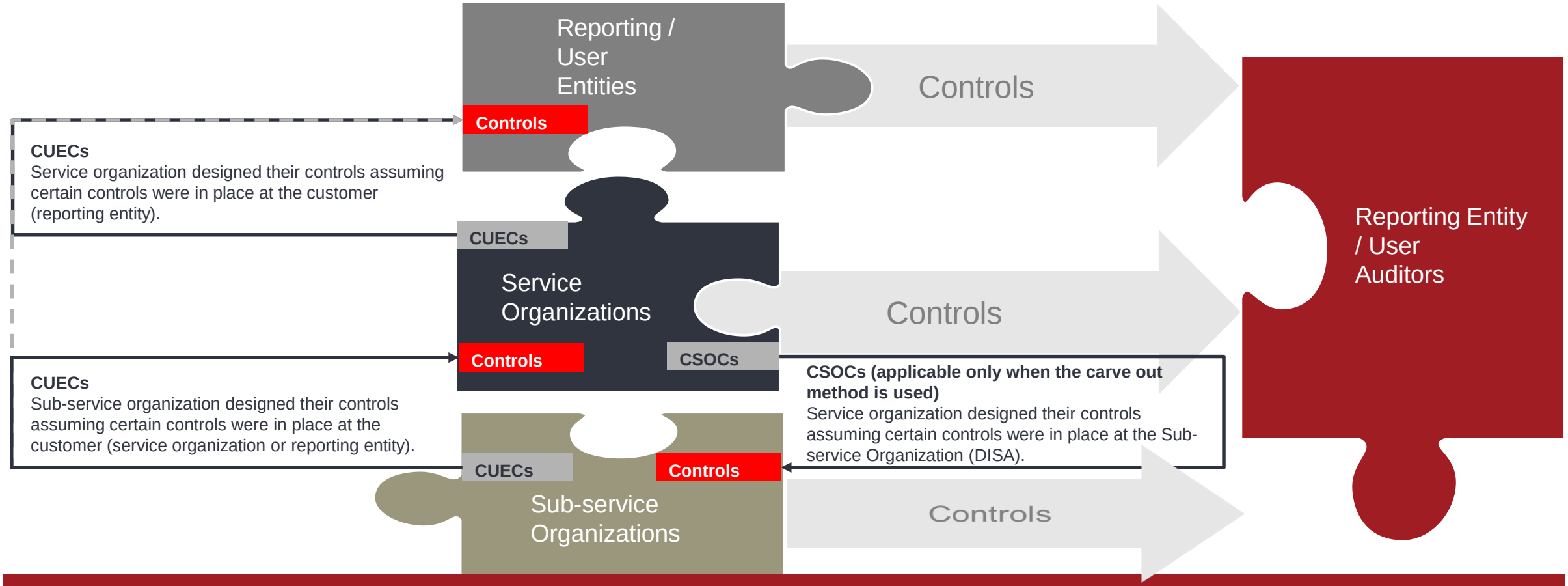
Discussion Topic 4

Question: What are subservice organizations and why is it important for service organizations to effectively monitor the subservice organization's key controls?

Discussion Topic 5

Question: What are complementary user entity controls (CUECs) and complementary subservice organization controls (CSOCs)? How do I tell the difference between them?

Connecting the Dots



Need to avoid conflicting / contradictory information in "related" SOC 1 reports and pointers to nowhere.

Discussion Topic 6

Question: What are the service organizations required to implement as part of the recently issued DCFO memos designed to improve reporting on controls at a service organization?

The 10 Commandments

Independent Public Accounting Firm feedback on improving SOC 1 reports resulted in 10 recommendations.

Deputy Chief Financial Officer Policy Memo Issued in February 2016

Identified Ten Required Changes to SOC 1 Reports

1. SOC 1 Reports to be Issued by August 15th of each year.
2. Nine Month Attestation Period (October 1 – June 30).
3. Bridge Letters to be Issued by October 8th of each year.
4. CUECs to be Aligned to Control Objectives
5. Describe Service Organization Controls in Place to Monitor Subservice Organizations and Identify Service Organization Controls in Place to Address Subservice Organization CUECs.
6. Establish an Interim Milestone of April 30th to Obtain Service Auditor Feedback.
7. Identify Key Inputs and Management's Rationale / Approach.
8. Identify Edit Checks and Management's Rationale / Approach.
9. Identify Interfaces and Management's Rationale / Approach.
10. Identify Outputs and Management's Rationale / Approach.

Improving SOC 1s Memo

Addressing New Standards

Input was solicited from IPAs performing financial statement audits and SOC 1 engagements.

Memo was sent to Service Organizations for comment and addresses the following key points:

1. Service Organizations to meet with their IPA(s) to establish an understanding of SSAE 18 impact by January 13, 2017.
2. Service Organization to validate the reliability of key output reports / data.
3. Service Organizations to document Complementary Subservice Organization Controls (CSOCs), their basis for assuming the CSOC is in place at the Subservice Organization, and the associated monitoring controls in place at the Service Organization.
4. Service Organizations to communicate of CSOCs to Subservice Organizations by January 23, 2017.
5. Provides a deadline for Subservice Organizations to inform Service Organizations that they do not plan to have controls in place to address the CSOCs.
6. Provides a deadline for Subservice Organizations to provide corrective plans to Service Organizations for those instances where remediation is needed to put controls in place to address the CSOCs.

SSAE 18 DCFO Memo

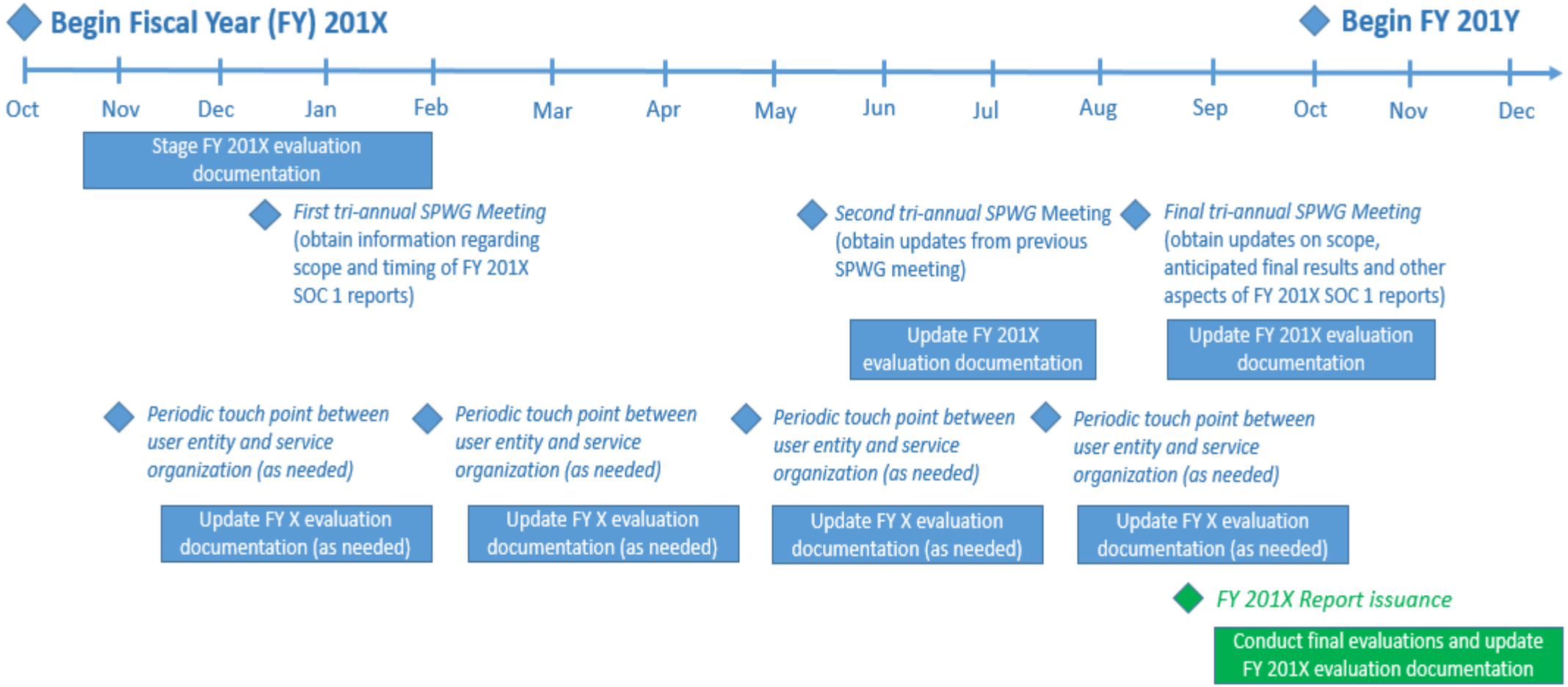
Discussion Topic 7

Question: When do service organizations typically issue SOC 1 reports and what are their typical periods of coverage (‘the reporting period’)? Why are these matters important to me?

Discussion Topic 8

Question: If SOC 1 reports are not typically available until mid-August, what should I do to manage time compression risk associated with receiving SOC 1 in mid-August and having to complete detailed evaluations in line with my auditors' SOC 1 report assessments?

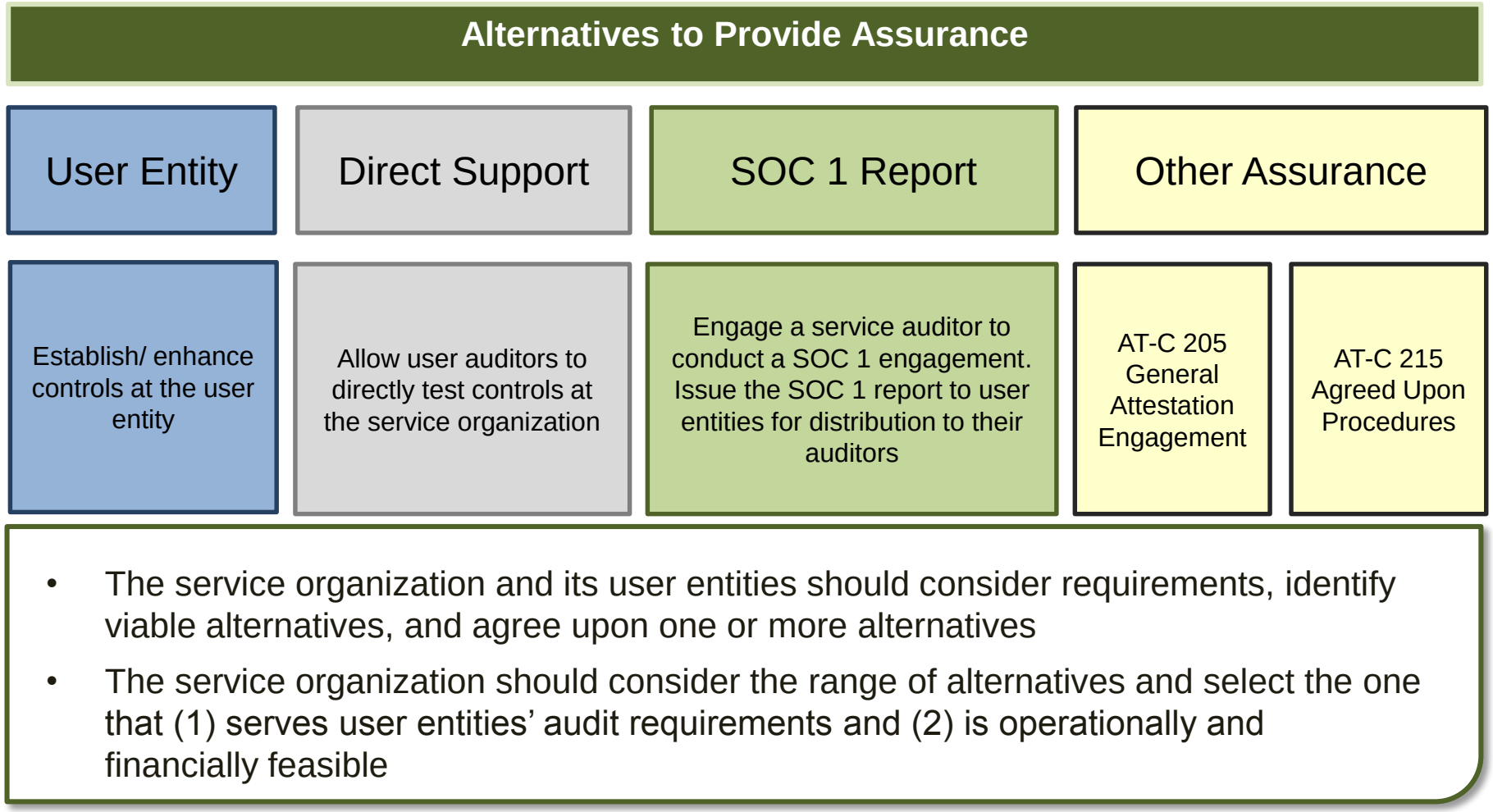
A Notional Timeline of Key Activities



Discussion Topic 9

Question: I have a service organization that does not have a SOC 1 report. What do I do?

Assurance Alternatives



Discussion Topic 10

Question: What are some of the factors that should be considered when determining whether an external entity is a service organization or just a vendor/trading partner?

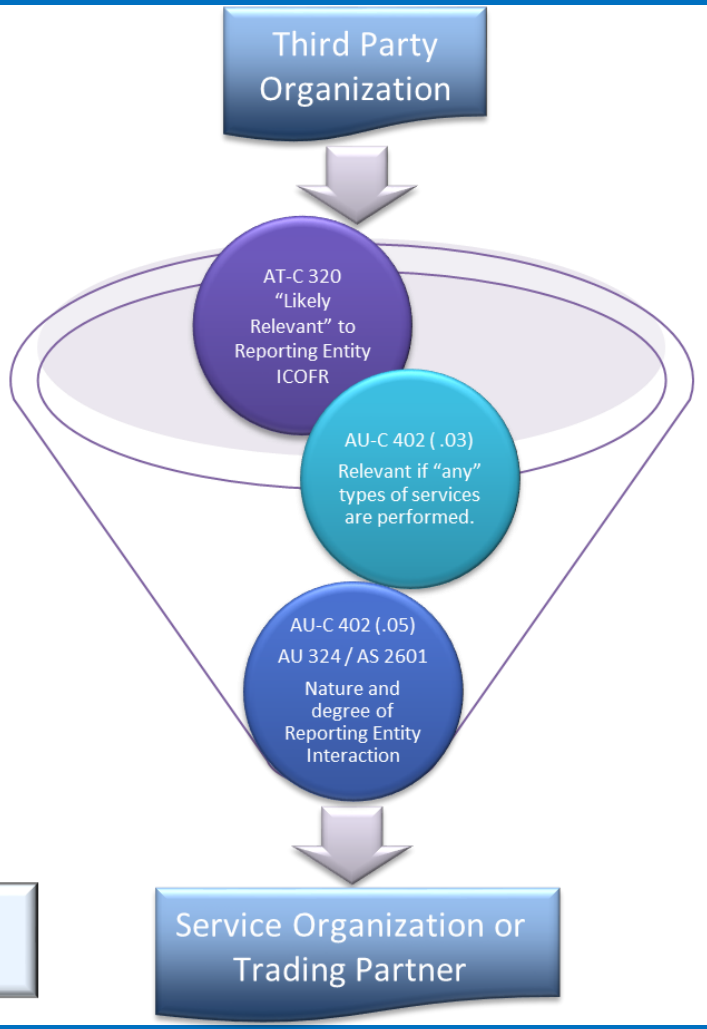
Factors to Consider

AT-C Section 320
Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting

AU-C Section 402
(*Audit Considerations Relating to an Entity Using a Service Organization)*

AS 2601
Consideration of an Entity's Use of a Service Organization

The auditing standards provide a framework for defining Service Organizations



Discussion Topic 11

Question: Can I leverage my component's Managers' Internal Control Program (MICP) (or other compliance efforts) to support my SOC 1 report evaluations? Can I use SOC 1 report evaluation results to support other agency compliance efforts?

Audience Questions/ Wrap Up