ControlCase
Compliance as a Service

SSAE 18 & new SOC approach to compliance

Moderator Name: Patricio Garcia

Managing Partner ControlCase Attestation Services

Agenda

1. SSAE 18 overview
2. SOC 2 +
3. 2017 Trust Services Criteria

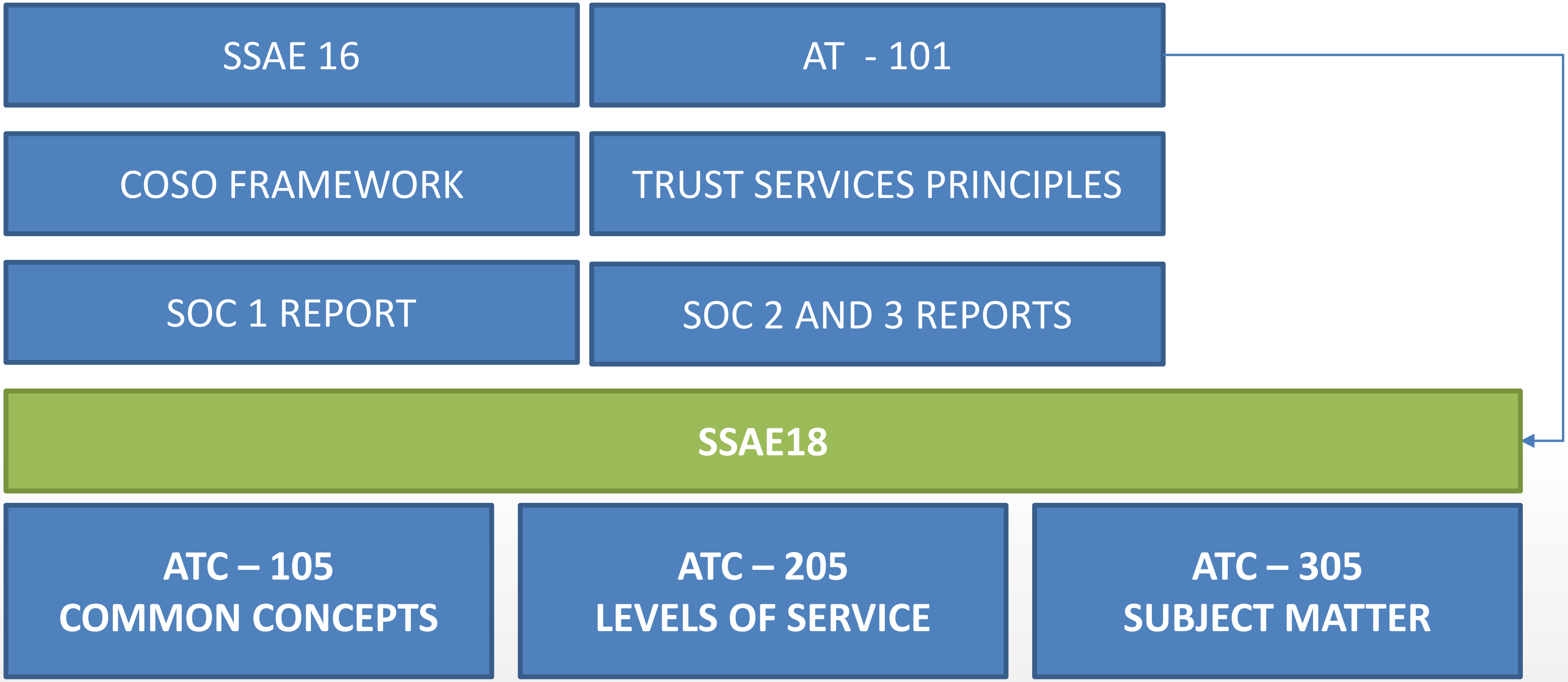
ControlCase
Compliance as a Service

SSAE 18 Overview

- SSAE 18 is the short name for Statement on Standards for Attestation Engagements No. 18.
- Establishes requirements and provide application guidance to auditors for performing and reporting on examination, review, and agreed-upon procedures engagements, including Service Organization Controls (SOC) attestations.
- SSAE 18 completely replaces SSAE 16 and many other SSAEs into a combined standard.
- SSAE 18 is NOT a certification. Neither was SSAE 16 or SAS 70 that preceded it.

ControlCase
Compliance as a Service

TRANSITION – EFFECTIVE MAY 2017



SSAE 16

AT - 101

COSO FRAMEWORK

TRUST SERVICES PRINCIPLES

SOC 1 REPORT

SOC 2 AND 3 REPORTS

SSAE18

ATC – 105
COMMON CONCEPTS

ATC – 205
LEVELS OF SERVICE

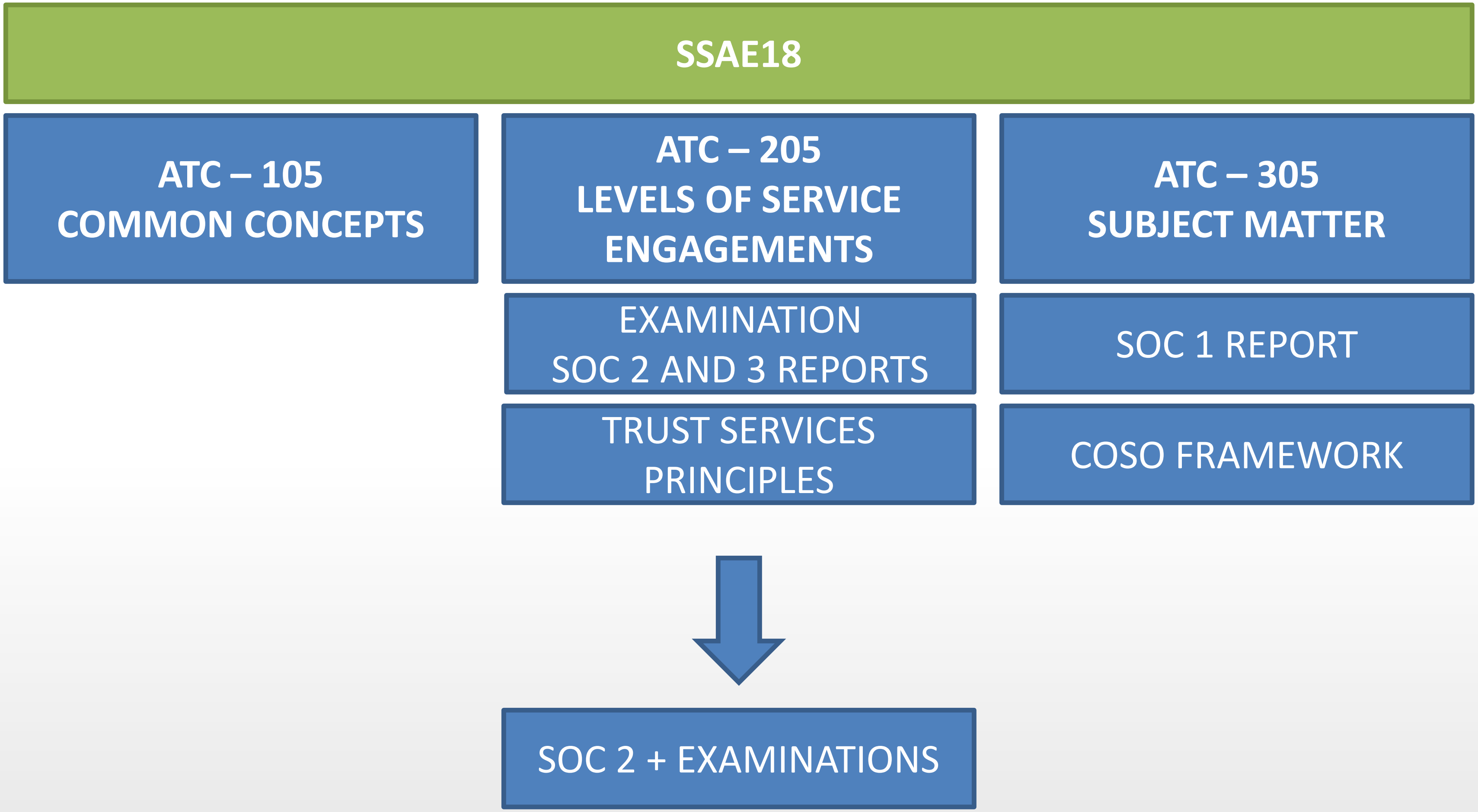
ATC – 305
SUBJECT MATTER

Statement on Standards for Attestation Engagements

- 100 Common Concepts
  - 105 Concepts Common to All Attestation Engagements
- 200 Levels of Service
  - Examination Engagements –reasonable assurance
  - Review Engagements – Limited assurance
  - Agreed-Upon Procedures Engagements
- 300 Subject Matter
  - Prospective Financial Information
  - Reporting on Pro Forma Financial Information
  - Compliance Attestation
  - Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC1)
  - Management Discussion and Analysis.

ControlCase
Compliance as a Service

APPROACH TO COMPLIANCE



SSAE18

ATC – 105
COMMON CONCEPTS

ATC – 205
LEVELS OF SERVICE ENGAGEMENTS

EXAMINATION
SOC 2 AND 3 REPORTS

TRUST SERVICES PRINCIPLES

ATC – 305
SUBJECT MATTER

SOC 1 REPORT

COSO FRAMEWORK

SOC 2 + EXAMINATIONS

System and Organization Controls

EXAMINATION

- **SOC 2® - SOC for Service Organizations: Trust Services Criteria**
- **In accordance with SSAE 18 - AT-C section 205**

SUBJECT MATTER

- **SOC 1 Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting (ICFR)**
- **In accordance with SSAE 18 - AT-C section 320**

KEY CHANGES RELATED TO SOC AUDITS

- THIRD PARTY AND VENDOR MANAGEMENT
  - IDENTIFY ALL SUBSERVICE ORGANIZATIONS USED IN PROVIDING IN-SCOPE SERVICES
  - INCLUDE A DESCRIPTION OF ANY SUBSERVICE ORGANIZATION CONTROLS - RELIES ON TO PROVIDE THE PRIMARY SERVICE TO ITS CUSTOMERS
- RISK ASSESSMENT
  - ORGANIZATION KEY INTERNAL RISKS
- TRUST SERVICES PRINCIPLES ALIGNED WITH THE COSO INTERNAL CONTROL FRAMEWORK.

KEY CHANGES RELATED TO SOC REPORTS

- MONITORING CONTROLS
  - SERVICE ORGANIZATION TO IMPLEMENT CONTROLS TO MONITOR THE EFECTIVENESS OF RELEVANT CONTROLS AT THE SERVICE ORGANIZATION
  - SERVICE AUDITOR TO REPORT ON THE SERVICE ORGANIZATION IMPLEMENTED TO MONITOR THE RELEVANT CONTROLS AT THE SUBSERVICE ORGANIZATION
    - **Reviewing SOC reports of the subservice organization's system**
    - Periodic discussion with subservice organization personnel
    - Regular site visits
    - Testing controls at the subservice organization
    - Monitoring external communications
    - Reviewing and reconciling reports.

ControlCase
Compliance as a Service

SOC 2 +

- A SOC 2 report, mapped to other Framework, may be crafted to reduce the number of customized reporting requests and be distributed to meet many requests by customers and other stakeholders.

EI3PA
EXPERIAN

MICROSOFT SUPPLIER DATA PROTECTION REQUIREMENTS

EI3PA CONTROLS MAPPED TO THE TSP

SOC 2 Type I or II PRIVACY PRINCIPLE PLUS ADDITIONAL MICROSOFT REQUIREMENTS

- SOC for Cybersecurity – **Cybersecurity Risk Management Program assessmenT**
  - Nature of operations, nature of information at risk, program objectives
  - Inherent risk, incident management, governance, risk management process

SOC 2 + CSA STAR

SOC 2® CSA STAR Attestation – Level Two (Third Party Assessment)

CLOUD SECURITY ALLIANCE

STAR Attestation builds on the key strengths of SOC 2 :

- Is a mature attest standard (it serves as the standard for SOC 2 and SOC 3 reporting) .
- Provides for robust reporting on the service provider's description of its system and on the service provider's controls, including a description of the service auditor's tests of controls.
- Evaluation over a period of time rather than a point in time
- Recognition with an AICPA Logo

ControlCase
Compliance as a Service

TSC alignment to COSO

1. Emphasis on the Board of Directors and TOP Management commitment to integrity, ethical values and oversight related to entity's internal control.
2. Additional Information required to confirm personnel competence
3. Information and communication requests security training to technical and non-technical system users
4. Risk Assessment not only related to IT, Development and Security operations. It should include in-scope service processing and operations.
5. Control Activities linked directly to the risk assessment process
6. Assess asset management effectiveness
7. Physical and access controls section provides additional guidance on different requirements (e.g. protection of encryption keys)
8. Change Management incorporates detailed requirements for detection, vulnerability management and incident management
9. **Risk Mitigation**
   1. The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
   2. The entity assesses and manages risks associated with vendors and business partners.