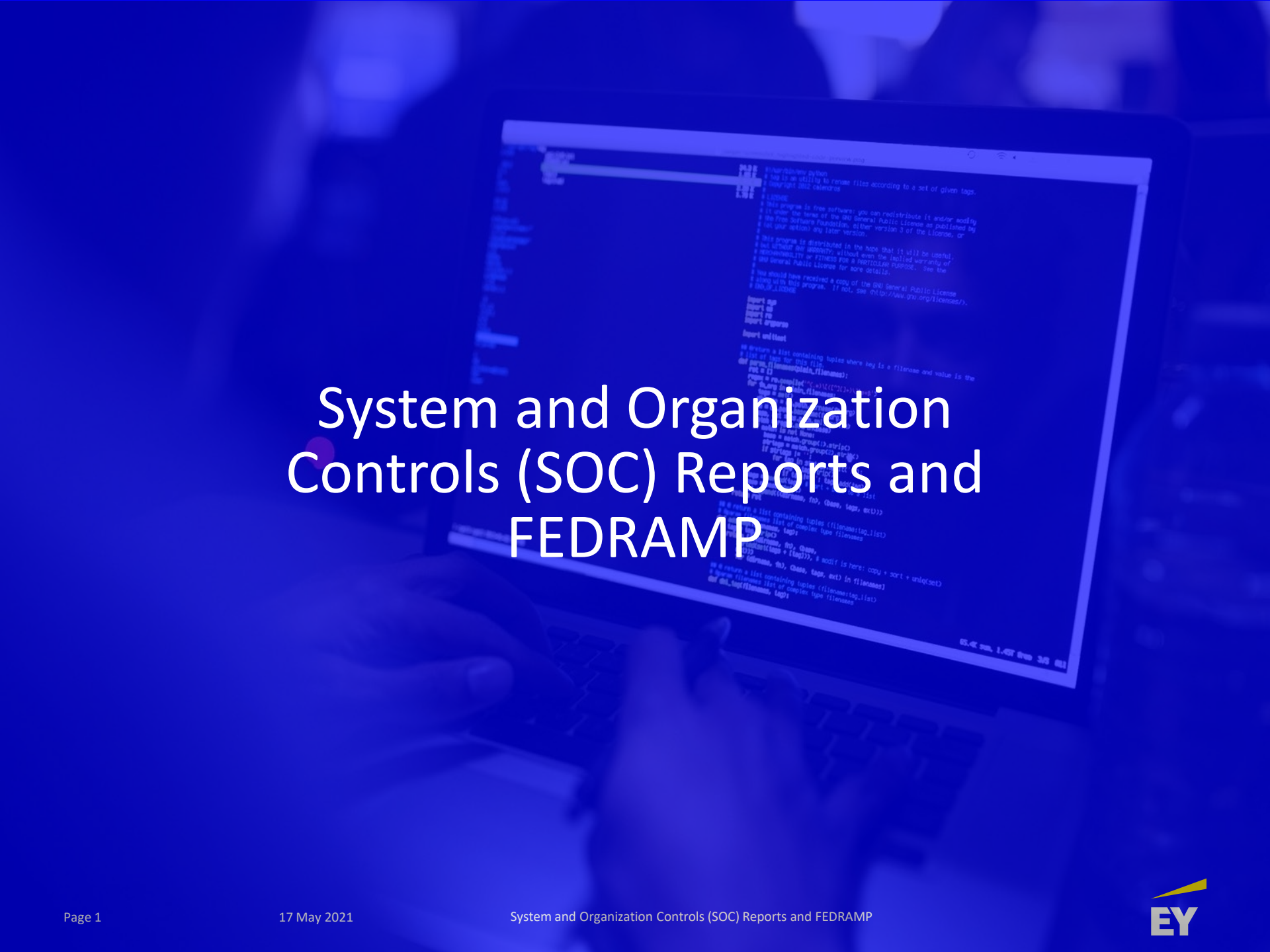


System and Organization Controls (SOC) Reports and FEDRAMP

FedRamp versus SOC reports (At a Glance)

- **System and Organization Control Report**

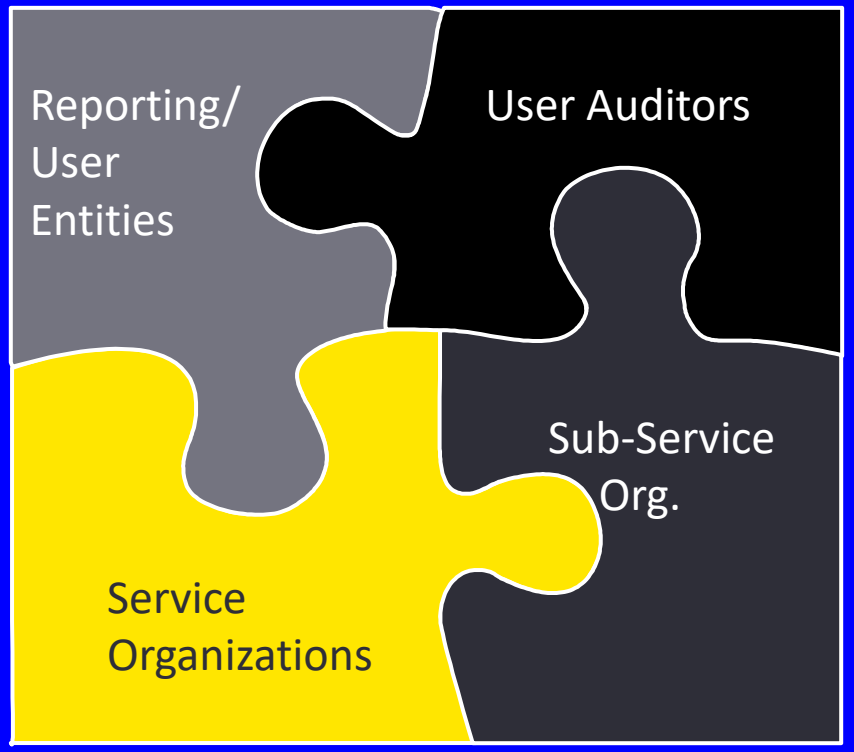
- Purpose: To provide Auditor to Auditor communication on the implementation of controls at a service organization based on specified criteria:
  - SOC 1: Internal Control over Financial Reporting
  - SOC 2: Trusted Service Criteria (TSC)
  - SOC 3: TSC for General Use
- Authoritative Body: AICPA
- Usage during a FSA: Utilized by Auditors to place reliance on the work of other auditors without performing their own testing
- Reporting Standard: SSAE 18 issued by AICPA and used across Federal and Commercial Industry

- **FedRamp 3PAO Report**

- Purpose: To provide a security assessment report (SAR) to federal authorizing officials for IT security authorization decisions on cloud service providers based on the type of data stored there are 3 levels of requirements:
  - FedRamp Low: Limited adverse effects on an agency's operations
  - FedRamp Moderate: serious adverse effects…
  - FedRamp High: severe or catastrophic adverse effect…
- Authoritative Body: FedRamp Program Office
- Usage during a FSA: As part of management oversight controls of 3rd party organizations, can not directly rely on testing performed.
- Reporting Standard: 3PAO Obligation and Performance standards

What is a Systems and Organizations Controls (SOC) Report?

- SOC reports are designed to assist service organizations in communicating the design and operating effectiveness of internal controls over financial reporting relevant to users of the report.
- SOC reports provide assurance and help customers/partners understand the possible risks involved in working with the evaluated organization.
- SOC reports are evaluated by an independent auditor of a user organization.



Three Types of SOC Reports

System and Organization Controls *(SOC)* reports are intended to provide user organizations with *reasonable assurance* that controls within the service organization are *accurately described, properly designed, and operating effectively* based on the overall operating environment.

SOC 1

Processes and controls at service organization relevant to providing:

- Entities internal control over financial reporting (ICFR)

Intended Audience:

- Accounting/Internal Audit
- Business unit management

- Full description of service organization's processes and controls
- Type 1: Assessment of design of controls at a point of time
- Type 2: Assessment of design of controls and their operating effectiveness for a period of time

SOC 2

Processes and controls at service organization relevant to providing:

- Information on controls related to security, availability, confidentiality, process integrity and/or privacy at a service organization to support vendor risk management needs

Intended Audience:

- Business unit management
- Vendor risk management
- Accounting/Internal Audit
- Chief information security officer
- Business continuity plan

- Full description of service organization's processes and controls
- Type 1: Assessment of design of controls at a point of time
- Type 2: Assessment of design of controls and their operating effectiveness for a period of time

SOC 3

- To provide interested parties with an IPA's opinion about controls at the service organization that may affect user entities' security, availability, processing integrity, confidentiality, or privacy.

Introduction to FedRAMP

FedRAMP (Federal Risk and Authorization Management Program):

- FedRAMP is an assessment for 3rd Party cloud computing service providers that are contracted to provide their services to Government Agencies.
- The Cloud Service provider must have the FedRAMP assessment complete by a 3rd Party Assessment Organization (3PAO).
- A government-wide initiative to provide joint authorization services
  - FedRAMP PMO in GSA
  - Unified government-wide risk management
  - Agencies would leverage FedRAMP authorizations (when applicable)
- Agencies retain their responsibility and authority to ensure use of systems that meet their security needs
- FedRAMP would provide an optional service to agencies

FedRAMP Governance Model