

TSP Audit Report

SSAE 16, SOC 1, SOC 2 Checklist



FOR FINANCIAL INSTITUTIONS



TSP Audit Report SSAE 16, SOC 1, SOC 2 Checklist

- I. **Report Opinion** - The opinion on the report should be read first to determine if any exceptions were noted. If exceptions and/or a qualification was made, the significance of these items should be considered when assessing overall risk. In addition to exceptions, the service reporting period should be defined in the report.
- II. **Management Assertion Letter** – A Management Representation Letter should exist for the TSP as well as for any subcontractors used by the primary TSP when the “inclusive method” was used. The date of the Management Representation Letter should coincide with the date on the Audit Report.
- III. **Use of Subcontractors** – The use of subcontractors and the services they provide should be described in the Report. If subcontractors are used, a disclosure should be made as to whether they have been “carved out” where the primary TSP disclaims any controls of the Subcontractor. If a subcontractor is used and the “inclusive method” used, then a separate Management Representation Letter as defined in II above should exist for each subcontractor.
- IV. **Control Environment** – The control environment should be reviewed to understand the ethics and risk management practices in place for the TSP. The control environment typically includes the following sections:



- a. Integrity and Ethical Values
- b. Organizational Structure
- c. Clear Assignment of Authority and Responsibility
- d. Security Awareness

- V. **Exceptions and Management Responses** – Exceptions related to the design and/or operating effectiveness of the system evaluated will be noted in the Report and detailed in a separate section where Management Responses should be provided. Exceptions should be reviewed to determine:
 - a. Whether Management Responses have been provided
 - b. If the same exceptions were noted in a previous year
 - c. How significant the exceptions are



- VI. **User Entity/Compensating Controls** – The Processing of transactions and the controls over processing are frequently designed with the assumption that certain controls would be placed in operation by user entities. A process should be in place to ensure your organization has established these controls and tests them periodically.
- VII. **Testing of Controls** – The results of testing should be reviewed for overall sufficiency if a Type II review was performed. The review should determine whether:
- Key processes described in the report were tested
 - The scope and depth of IT controls designed and tested is sufficient
 - If a SOC 2 was performed, that the appropriate trust principles were included

